SIEMENS

Application example • 01/2016

Basics of Setting up an Industrial Wireless LAN

SCALANCE W

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

Warranty and liability

Note

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

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Application Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change of the burden of proof to your detriment.

Any form of duplication or distribution of these Application Examples or excerpts hereof is prohibited without the expressed consent of the Siemens AG.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.industry.siemens.com.

Table of contents

Preface

Objective of the document

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

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

Core contents of this document

This document deals with the following key issues:

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

Topics not covered in this application

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

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

Reference to Automation and Drives Service & Support

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

http://support.automation.siemens.com/WW/view/en/22681042

1 Radio Waves as Basis of a Shared Medium Network

1.1 Overview of radio standards

At present, there are a number of different technologies available for setting up radio networks, such as, Bluetooth, GPRS und UMTS for cellular telephone networks, RFID tags for identification and goods tracking, etc. (see also chapter 3)

Within the framework of this document, we focus on WLANs in the strict sense, i.e. radio networks which follow the IEEE 802.11 standard (see chapter 2). "IWLANs" ("Industrial WLANs") refers to WLANs, which are "hardened" by special measures, i.e. made ready for requirements and utilization in industrial environments.

1.2 Introduction to radio networks

1.2.1 Comparison between radio waves and cables

The use of cables and lines for communication has certain advantages since an exclusive medium is available: The transmission characteristics of this medium are well defined and constant (provided that cables, routers or similar components are not replaced) and it is distinctly recognizable at any time which nodes are connected to a local area network (abbrev. LAN) and which ones 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. Eventually, the use of wire-bound methods for the communication with freely moving nodes is only feasible in exceptional cases. Radio links additionally enable bridging zones of sections, for which cabling would otherwise be difficult (streets, waters).

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

1.2.2 Complexity of the radio field

Radio waves propagate through space, are diffracted, reflected at obstacles or attenuated when passing through and thus generate a complex radio field which even changes when the obstacles move. It is obvious 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 characteristics for the individual nodes of the radio network, depending on their position. In addition, it is practically impossible to discover a “silent listener” in a radio network.

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

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 what the CSMA (Carrier Sense Multiple Access) is for. This procedure requires a check from each station whether the medium is free before transmitting. Only then can the data be sent.

However, if this check occurs from two stations at the same time, it may happen that both detect the medium as free and send data at the same time. A collision occurs and the data becomes unusable. A wireless transmitting station cannot determine a signal collision itself. The dedicated signal covers the signals of other stations and collisions cannot be distinguished from interferences.

In order to avoid these non-recognizable collisions as best as possible, the CA (Collision Avoidance) system is additionally used. If the occupied medium is now free, a station ready to transmit, will not start straight away with the data transmission but it will wait for a randomly determined 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 fields of application

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

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

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

1.4 The physics of radio waves

1.4.1 Propagation

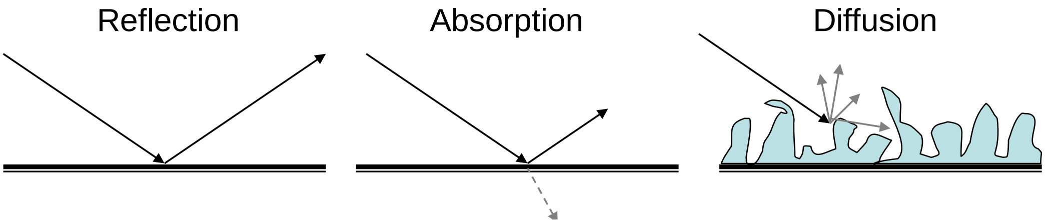
Unlike signals in a line, radio signals propagate three-dimensionally in space as electromagnetic waves.

Obstacles and objects influence the propagation of radio waves, effects such as reflection, 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 a rest is finally let 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 the radio waves:

- On the one hand, radio waves (unlike incoherent light) can amplify or even extinguish one another (so 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 the double signal strength, but it will possibly not detect any signal at all.
- On the other hand, the propagation properties of the waves depend on their wavelength, i.e. high-frequency radio waves behave differently than low-frequency radio waves. In particular, radio waves of long wavelength (i.e. low-frequency) can be “diffracted” around objects. Similar to sound or water waves, it is then possible to receive signals even in the “shadow” of a radio source.

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

Frequency sensitivity of the properties of radio waves

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

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

1.4.2 Faults

Each object that is spatially located within a radio network can disturb this network if it sends signals on the frequency used by the transmitters. In contrast to lines, which can be shielded relatively easily and reliably, radio networks are susceptible to interferences by any device in their proximity which, intermittently or continuously, can radiate on strictly limited channels or emit broadband radiation.

These devices include devices 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 the achievable data rate of a radio transmitter depend, among other things, on the frequency used.

Range

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

With the SIMATIC NET Selection Tool (see chapter 9.6) the range can be determined in dependence of several parameters, such as frequency and transmission power.

Data rate

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

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

[1] The theoretically attainable gross data rate (in bit/s) is proportional to the band width. 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 depends – even if the connections are optimal – not only on the quantity of the user data. Depending on the protocol, there will be a smaller or larger overhead for the handling of the radio communication and interconnected devices such as access points, routers, etc. also cause delays which develop when the signals are relayed.

The achievable net data rate is thus influenced in multiple ways by the design and the parameterization of the actually existing radio network.

1.4.4 Frequencies, frequency spacings and channels

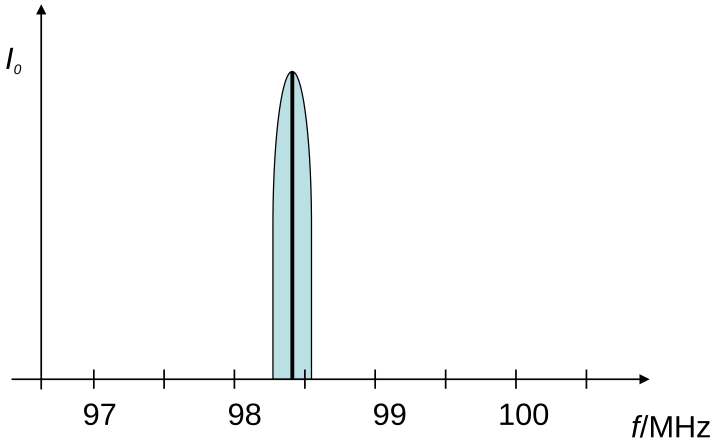
Only one node can transmit on each radio frequency at any time. If several stations send simultaneously on the same frequency, none of the two can be received; this case is referred to as a “collision”.

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

Frequencies and required spectrum

Strictly speaking, the statement that a transmitter emits on exactly one frequency is not correct: this would only be the case for 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 to each other that is proportional to the data rate used: This is referred to as the “band width” of the transmitter.[2]

Figure 1-2



The example shown in the above figure 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 band width is exaggerated; in reality 40 kHz are sufficient for an FM signal.

[2] The transmission capacity is generally colloquially referred to as “bandwidth”.

Bands and channels

To keep the clarity, the radio spectrum, i.e. the entire frequency range of the radio communication, is divided into individual “bands”. The different bands differ in the radio characteristics (transmission range, susceptibility to interferences, possible data rate, 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 13 channels with center frequency between 2.412 GHz and 2.472 GHz, the distance between the neighboring channels is 5 MHz each. Theoretically, thirteen transmitters can use the band simultaneously.[4]

1.5 Antennae

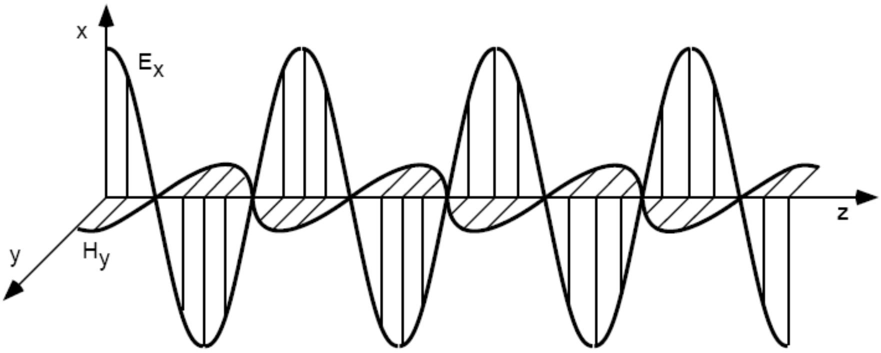
Task

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

Electromagnetic waves

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

Figure 1-3



[3] "Industrial, Scientific and Medical"; also see glossary.
[4] However, since the frequency ranges of transmitters of neighboring channels overlap, there are only three channels that are mutually interference-free (see also chapter 2.4.12.4.1).

1.5.1 Characteristics of an antenna

Impedance

Impedance refers to a frequency-dependent resistor. For the IWLAN components (antenna, cable) this resistor has 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.

Polarization

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

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

Table 1-1

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

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

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

1.5.2 Omnidirectional and directional antennae

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

Antenna gain

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

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

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

Antenna diagrams

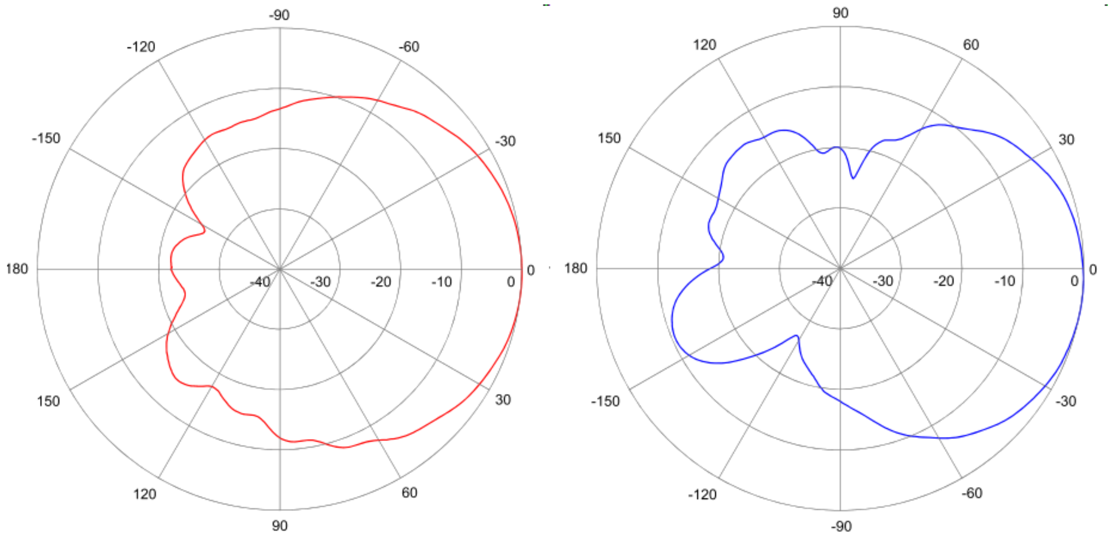
An antenna describes the directional characteristic of an antenna in which the direction-independent antenna gain is measured. Normally, the representation of the directional diagram occurs in polar coordinates.

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

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

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

Figure 1-4

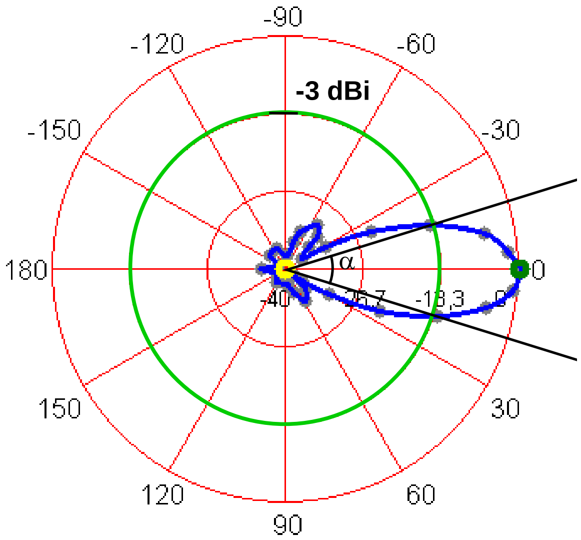


[5] Since the antenna gain is measured in logarithms, 6 dBi correspond to 4 times the power, 9 dBi 8 times the power etc..

Aperture angle

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

Figure 1-5



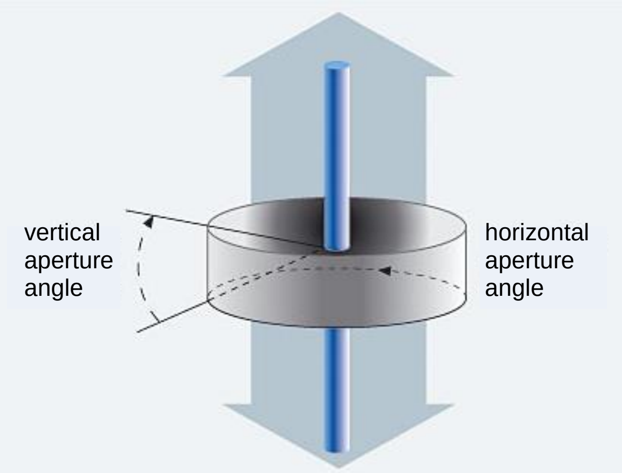
The horizontal and vertical aperture angles of an antenna usually differ depending on the geometry.

Omnidirectional antennae

Omnidirectional antennae always have the form of a rod or a straight wire. The term is misleading in so far as the radiation intensity is not isotropic, i.e. not equal in all directions. The radio field of the antenna reaches the maximum intensity on a plane, at a right angle to the antenna axis (compare Figure 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 radial symmetrical; this means that the field intensity is identical in all directions when viewed from the top along the antenna axis. In this case, the “horizontal aperture angle” is 360°.

Figure 1-6

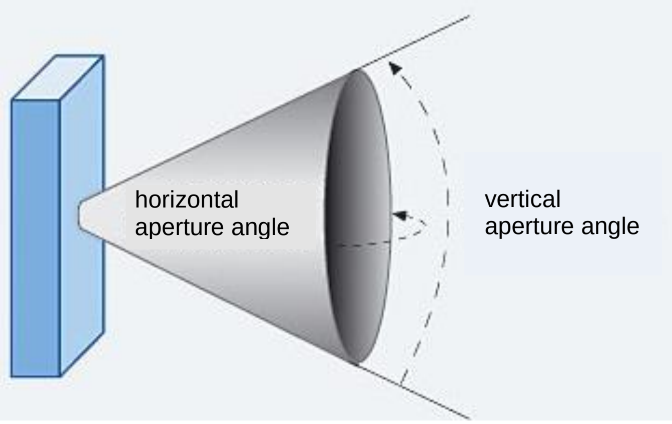


Directional antennae

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

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

Figure 1-7



In the maximum field intensity direction the transmission range of a directional antenna is typically ten times as large as the range of an omnidirectional antenna.

Antennae for SCALANCE W devices

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

Leaky wave cable

Leaky wave cables for which the developing radio field is limited to the direct proximity of the conductor, are alternatives to conventional antennae.

The fields of application of such leaky wave cables are moving nodes which move 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 leaky wave 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.

In order to be able to specify the possible range, the Fresnel zone was defined. The Fresnel zone describes certain spatial areas between transmitter and receiver antenna and therefore characterizes the signal propagation. For the calculation of the free space loss, the following is required

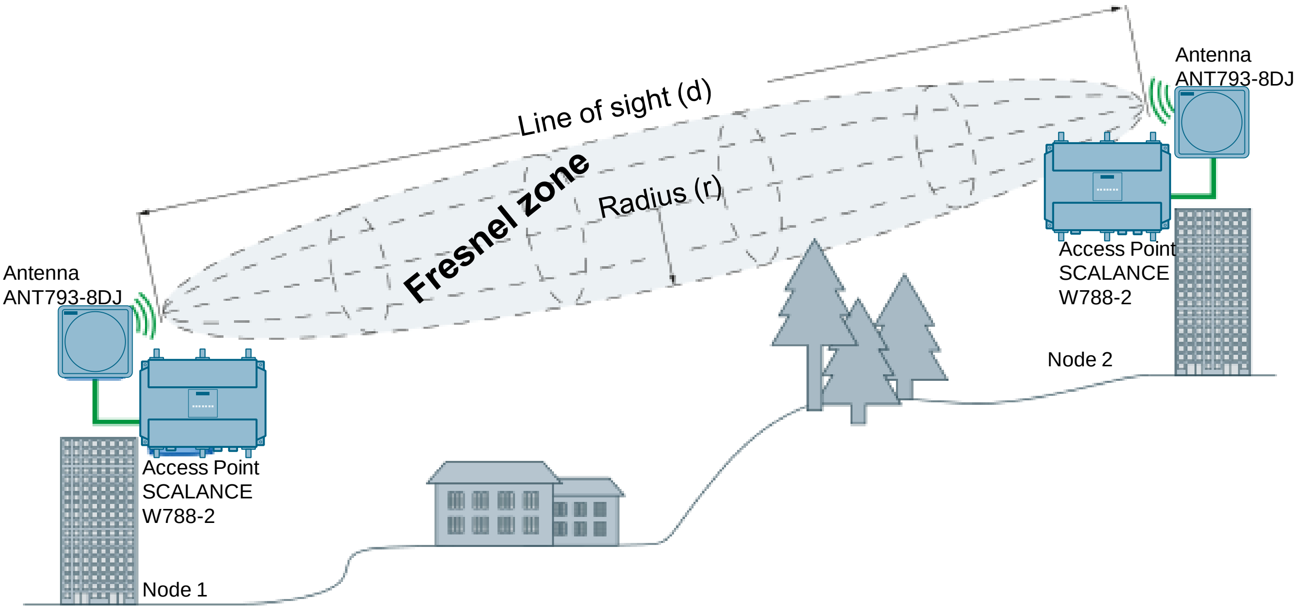
1. direct line-of-sight connection between the transmission path of transmitter and receiver and
2. that there is another area around this line-of-sight contact that must also be free of obstacles.

It is subdivided in several orders. The first order[6] is the most significant one, since this is where the main part of the signal energy is transmitted.

The above mentioned conditions for the application of the free space loss are fulfilled, if the first Fresnel zone is free of obstacles.

The Fresnel zone is in the shape of an ovoid and is irrespective of the frequency of the radio waves and the distance between transmitter and receiver. The diameter of these zones becomes smaller with increasing frequency, and it becomes larger with increasing distance between transmitter and receiver station.

Figure 1-8



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

1.6 Modulation and multiplex method

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

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

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

1.7 Requirements for radio communication in the industrial environment

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

Data volumes

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

Transmission speed and latency

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

Fail-safety and reliability

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

Additional interferences in the industrial area

Office and home environments are usually characterized by a low degree of interference from objects which are not part of the radio network. However, naturally, the industrial environment exhibits some very intensive interference which is unfavorable for the propagation of electromagnetic waves. Metal parts or other signal sources, such as RFID can be found almost everywhere, which can disturb or interrupt the transmission.
The metal areas, e.g. reflecting radio waves can course loss of packages or even obliterate the radio signal.

2 The IEEE 802.11 WLAN Standard

2.1 The network standards of the IEEE 802 series

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

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

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

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

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

Table 2-1

Standard	Definition area
802.11a	Communication
802.11ac	Communication
802.11ad	Communication
802.11b	Communication
802.11e	Quality of service (see chapter 2.3.1)
802.11g	Communication
802.11h	Communication (reduce interference)
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)

[7] See also http://www.ieee.org/portal/site,

2.2 Communication standard of the IEEE 802.11

The original 802.11 standard[8] (today often referred to as "802.11 legacy" for reasons of clarity) defines the connection of the network nodes via radio in the frequency band at 2.4 GHz.

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

The standard was improved by the extensions "b", "a", "g", "h" and "n", which were put on the market in this order.

Concerning the frequency bands used (2.4 GHz and 5 GHz), the different standards vary regarding the simultaneously usable channels and the maximum data rate.

The transmission capacities were increased by more complex and more 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 currently common 801.11 standards.

Table 2-2

	802.11a/h	**802.11b**	**802.11g**	**802.11n**	**802.11 ac**	**802.11 ad**
Frequency band	5 GHz	2.4 GHz:	2.4 GHz:	2.4 GHz and 5 GHz	5 GHz	60 GHz
Max. gross data rate	54 Mbit/s	11 Mbit/s	54 Mbit/s	600 Mbit/s	7 Gbit/s	7 Gbit/s
Modulation and multiplex method*)	OFDM	DSSS	OFDM	MIMO and OFDM	MIMO and OFDM	

*) on the individual modulation methods, see chapter 1.6

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

As a matter of principle, an 802.11a device cannot communicate with an 802.11b/g device, since they are transmitting on different frequency bands. However, the "b", "n" and "g" versions of the standards are compatible to one another.

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

2.2.1 IEEE 802.11a

Description

The IEEE 802.11a standard was approved in 1999. It uses the 5 GHz frequency band and the Orthogonal Frequency Division Multiplexing (OFDM) modulation method and the SISO technology. A maximum gross data rate of 54 Mbps can be attained.

This frequency band is mainly used by the military for radar in air and marine traffic. WLAN tends to be used as second rate user.

In order to prevent interferences between WLAN and the 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.

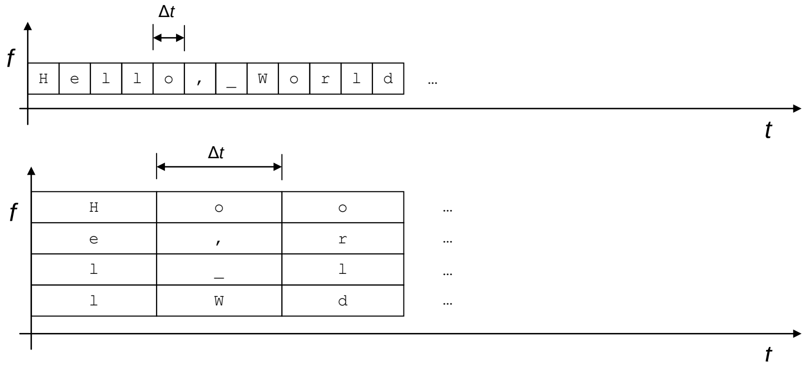
Orthogonal Frequency Division Multiplexing (OFDM) modulation method

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

The massive parallel data transmission drastically reduces the data rate over each *individual* channel, i.e. there is much more time available for transmitting the individual bits. Consequently, OFDM connections are significantly less susceptible to short-term noise or occurring echoes. Even in case of considerable path differences, there is a high probability that a received echo is still associated to the same bit as the one currently transmitted via the "direct path".[9] The reduced transmission rate additionally ensures that the duration of short-term noise peaks is mostly shorter than the transmission of a bit.

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

Figure 2-1



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

[9] In other words: The runtime difference remains lower than the duration of the transmission of one bit.

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

2.2.2 IEEE 802.11b

Description

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

"Direct Sequence Spread Spectrum" (DSSS) modulation method

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

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

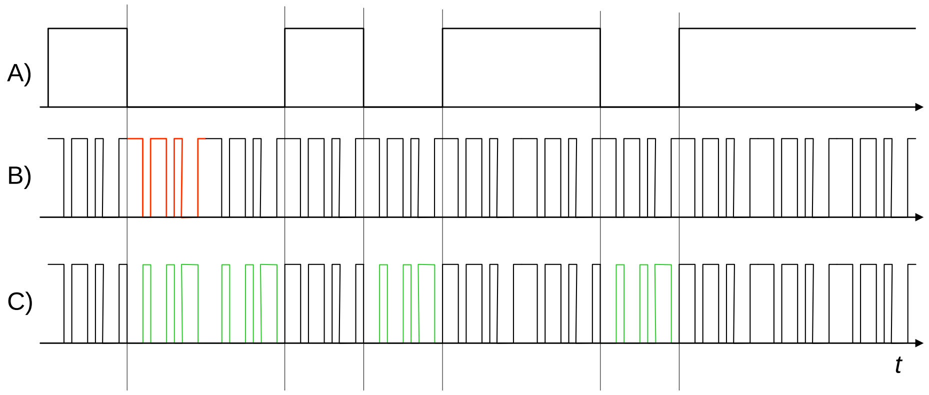
This has several effects:

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

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

[10] This is of course a simplified representation and strictly speaking it is not an addition or subtraction but XOR operations of data with its keys.

Figure 2-2



The above figure illustrates the function of DSSS.

A) The user data signal,

B) The “chips” used for encryption. This is only a short sequence (red) that is continuously repeated. The bit string of the “chips” changes much faster than in the user data.

C) The encrypted signal is identical to the chips as long as the user data signal is “1” (black sections); otherwise, it is created by inverting the chips (green).

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

2.2.3 IEEE 28.29g

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 the SISO technology and can therefore reach a maximum data rate of 54 Mbps. This standard is downward compatible to IEEE 802.11b. If both standards are used in a network, the DSSS modulation method with the respectively lower data transmission rate is used.

OFDM modulation method

See chapter 2.2.1

2.2.4 IEEE 802.11n

Description

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

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

Diversity systems

Diversity is a technology to increase the transmission security in a radio system. The principle is to transmit and receive the information in one radio channel several times (redundantly). The basis of all diversity systems is to transmit the signals via several parallel paths that are independent from each other. The separation can be in terms of time, via the frequency or in terms of space.

Spatial separation is mainly used in today’s radio systems.

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

What information is to be evaluated by what antenna, is decided by test measurements that are carried out during the establishment of the connection. The antenna that receives the data with the best signal-to-noise ratio will be used for further data transmission. The signal of the other antenna is ignored. Concretely used are therefore only the data of one transmission path.

Multiple Input / Multiple Output systems

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

A MIMO system differs from diversity systems by not only using one channel for redundant signal transmission, but several parallel subchannels. These additional data channels make it possible to transfer different data with the same antennae irrespective from each other on the same frequency band and at the same time, so called multiplexing (“spatial multiplexing”).
The technology requires the transmitter as well as the receiver to be equipped with a minimum of two and a maximum of four antennae.

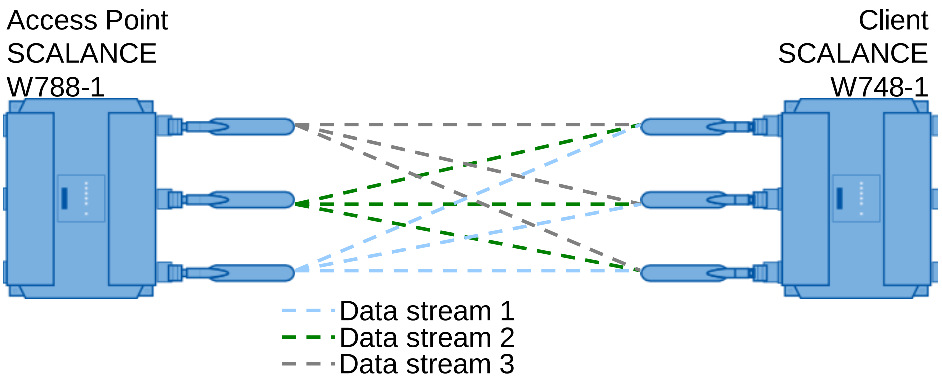
Beamforming enables the transmitter and the receiver to block out interferences in the channel and therefore establish a secure and high-quality connection.

The principle is to combine the signals of the individual antennae elements via adjustable phase shifters and enhancement factors. This results in “beamforming”, which can be electronically adjusted via so called intelligent antenna (smart antennae).

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

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

Figure 2-3



Shortened guard interval

The guard interval prevents that different transmissions are mixed. After the lapse of the transmission time there is an intermission (guard interval) between the two transferred OFDM symbols before the next transmission starts.

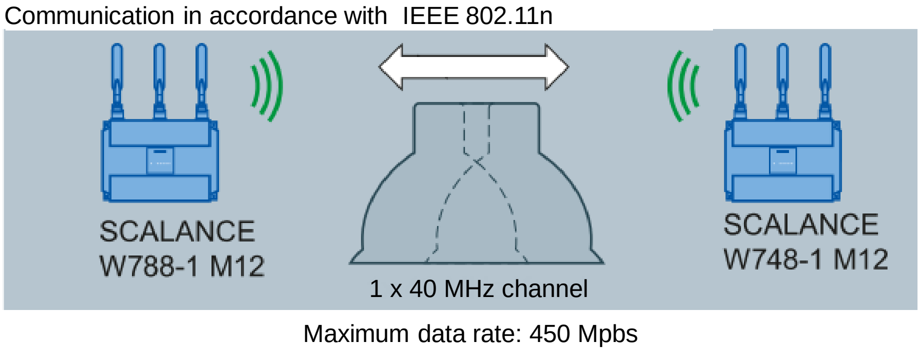
The guard interval of IEEE 802.11a/b/g is 800 ns. IEEE 802.11n can use the shortened guard interval of 400 ns.

Channel bonding

Channel bonding is the summary of several channels, in order to achieve a higher data throughput.

For IEEE 802.11n data can be transmitted via two directly neighboring channels. The two 20 MHz channels are combined to one channel with 40 MHz. This makes it possible to double the channel band width 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 the compatibility between IEEE 802.11n and IEEE 802.11a/b/g devices.

Figure 2-4


Communication in accordance with IEEE 802.11n
SCALANCE
W788-1 M12
1 x 40 MHz channel
SCALANCE
W748-1 M12
Maximum data rate: 450 Mpbs

Frame aggregation

For IEEE 802.11n it is possible to combine individual data packets to one larger data packet (frame aggregation).
This method minimizes the packet overhead, the wait times between the data packets are shortened and the data throughput is thus increased.
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 of the SCALANCE W devices (IEEE 802.11n) displays the available data transmission speeds for the WLAN 802.11n mode. They can be combined and selected as desired. Only the selected data transmission speeds are then used by the access point for the communication with the clients.

2.2.5 IEEE 802.11ac

Description

IEEE 802.11ac is a radio network standard that was approved in November 2013 for a 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 Gbps are possible. Data transmission is only in the 5 GHz band.

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

In terms of technology this standard does not bring any essential changes to the predecessor IEEE 802.11n. The higher transmission rate is mainly achieved through wider channels (up to 160 MHz), up to eight simultaneously used transmission and receive units, a high-quality modulation as well as multi-user MIMO.

OFDM modulation method

See chapter 2.2.1

2.2.6 IEEE 802.11ad

A new standard for wireless gigabit has existed since 2012. This is a specification according to IEEE 802.11ad for a wireless connection between digital video systems in the gigabit range. High data rates are achieved by the change of the frequency range to the 60 GHz band and the optimization of the access protocol.

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

2.2.7 Transmission range and special antennae

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

By using directional antennae this value can be increased to a multiple of 100m. Depending on the country of use, line of sight and the Fresnel zone (see chapter 1.5.3) even distances of several kilometers can be covered.

2.3 Other IEEE 802.1x standards

In the course of time a number of further standards were 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: Adaptation 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.

Furthermore, IEEE 802.1 standards exist that are important for operating 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. a specific connection quality is guaranteed if this standard is complied with.

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

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

WMM

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

2.3.2 IEEE 802.11h and the 5 GHz band

IEEE 802.11h

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

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

DFS (Dynamic Frequency Selection)

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

TPC (Transmit Power Control)

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

2.4 Channel distribution in the IEEE 802.11 standard

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

2.4.1 The 2.4 GHz band

The frequency bank is a frequency section that can be used license free in practically all nations at 2.4 GHz.[11] Since it is relatively economical to produce transmitters and receivers, the 2.4 GHz technology is very popular and not only used for WLAN but also for numerous other applications.

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

To exclude that the transmitters in the WLAN disturb each other, it is required that they keep at least this distance from each other. This reduces the number of frequencies that can be used independently of one another in practical operation to three: Usually only the channels 1, 7 and 13 (the so called “non-overlapping channels”) are simultaneously used for 802.11 networks.

With the 802.11n standard an expansion of the band width 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, it is required that many channels that are independent of one another, i.e. non-overlapping channels, are used. In this case, it may be advisable to switch to the 5 GHz band of the 802.11a/h/n standard, which offers a larger number of non-overlapping channels.

[11] Updated lists with country approvals for the individual SCALANCE W products can be found at http://www.siemens.com/radio approvals.

[12] Details of the permitted channels are different in every country. The topic is discussed in detail in chapter 7.

2.4.2 The 5 GHz band

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

Generally 5 GHz waves are “harder”, i.e. the propagation behavior is similar to that of light beams: There is less diffraction around objects, the absorption is higher and the penetration depth lower than for 2.4 GHz waves. Generally, the practically achievable transmission range is a little less than in the 2.4 GHz band.

Compared with the 2.4 GHz band the 5 GHz band is clearly less “busy”, and there are only few interference sources in this range. Military radar and satellite tracking systems are exceptions, their operators naturally react rather sensitively towards system interferences from a WLAN.

To harmonize the operation of 5 GHz WLANs with these systems the IEEE standard 802.11h (see chapter 2.3.2) was created.

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

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

Connection security and interference by other devices:

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

In any case the optimal configuration of illumination, frequency band and antennae must be clarified by a radio field analysis prior to setting up the system.

Size

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

Licensing

2.4 GHz as well as 5 GHz networks can be operated without license in most states. In chapter 7 the issue country approvals is described in more detail.

3 Alternative Radio Technologies to IWLAN

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

3.1 Bluetooth

“Bluetooth” is the name for the IEEE 802.15.1 standard which describes the networking of small devices via short distances. Its main area of application is the application of cable connections between office devices such as PDAs, 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, hence it collides 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 with a lower power in order to save their batteries; this is why typical ranges are below 10 m.). The data is transmitted with a speed of up to 24 Mbit/s.

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

Note To obtain further information on this topic, please use the following URL: https://www.bluetooth.org

3.2 Wireless HART

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

WirelessHART also uses the ISM frequency band (2.4 GHz with maximal 250 Kbit/s) and automatically builds meshed networks whose extend can be considerably larger than the nominal radio range of an individual node (approx. 200 m). The network organizes itself by evaluating all connection information from the WirelessHART Gateway (IE/WSN-PA Link), in order to automatically provide redundant paths with this information. This can achieve a very high availability of the communication connection, since bad connections or the failure of individual nodes can be bridged. Furthermore, the availability of the entire network via the operation of two redundant gateways can be significantly increased.

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

The main application area of WirelessHART here is the regular transmission of lower, non-time critical data volumes in large distances (typically between approx. 15 seconds and several hours) over relatively large distances (such as, for example, in process industry. Due to the lower energy consumption of WirelessHART devices, long battery runtimes 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 at sufficient illumination of the meshed network, it automatically “mends” the failure of intermediate stations.

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

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

http://www.siemens.com/wirelesshart

http://www.hartcomm.org/

3.2.1 Zigbee

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

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

The Zigbee standard is under the control of the Zigbee alliance , which also provides further information on this topic.

Note To obtain further information on this topic, please use the following URL: http://www.zigbee.org/

3.2.2 WiMAX

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

Different than the WLAN standards, WiMAX can also bridge bigger distances so that remote and rural regions can also be supplied with broadband. Due to this property WiMAX is seen as an alternative to the landline DSL.

The theoretical range is 50 km with a transmission speed of up to 75 Mbps. However, in reality this value is well below.

Note To obtain further information on this topic, please use 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

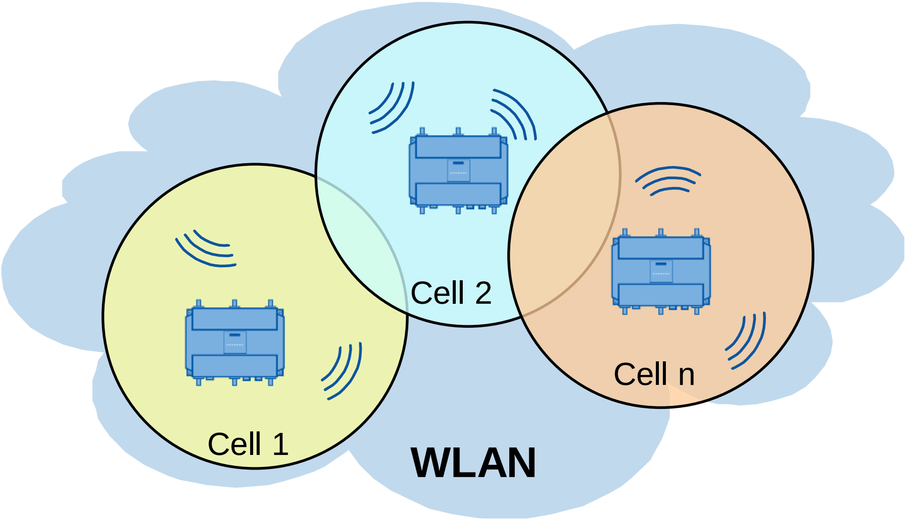
As we have seen in section 1.4.3, the range of radio transmitters is limited in practical operation. Generally, the area you want to cover by a LAN will be too large to be reliably “illuminated” by one single transmitter.

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

Structuring radio networks by radio cells

Furthermore, it is more economic to divide the WLAN into individual cells since only one station can send on each channel at any time. If several cells are available, an active transmitter can be located in *each* cell and the actual data throughput increases. Additionally, due to the short distances, only comparably small transmission power is necessary. The following figure shows the division of the WLAN into several cells.

Figure 4-1



Note To obtain further information on this topic, please use the following URL: http://www.siemens.com/iwlan

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

The use of “access points” is required to control the communication in a cell or to connect several radio cells with 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 radio cell or if the communication occurs only within one cell, the access point can be used to coordinate the communication within this cell.

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

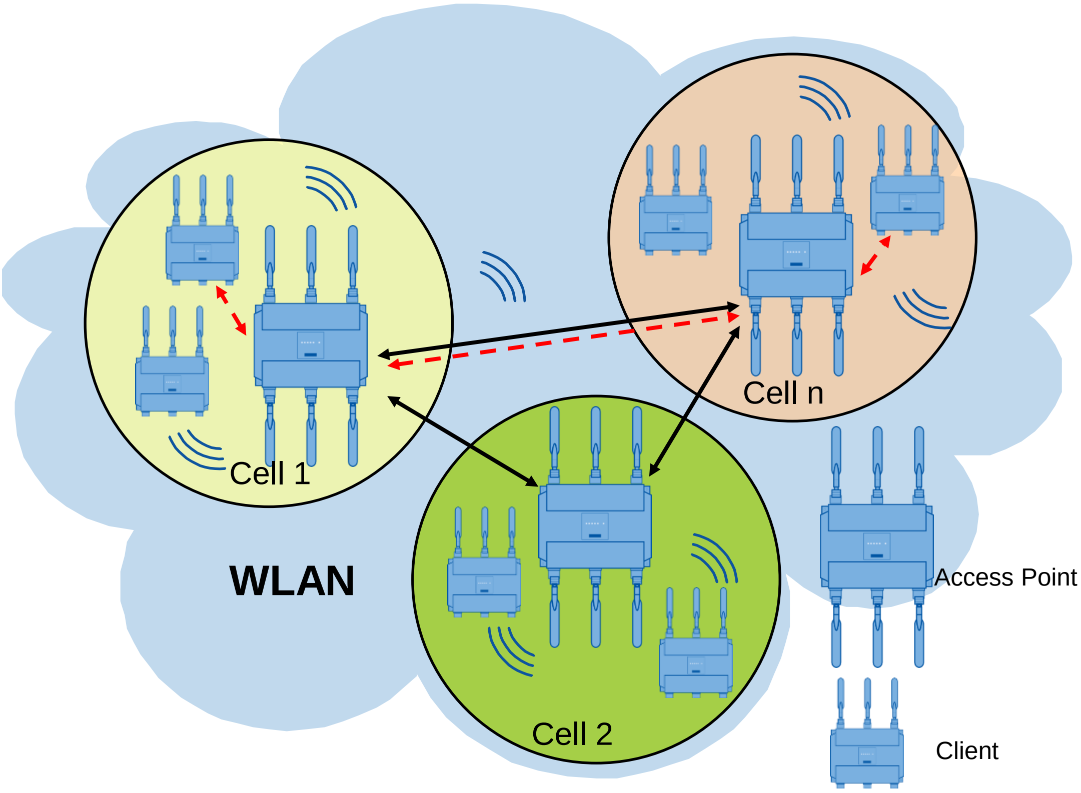
Access points as a “backbone” of the communication

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

The term “backbone” indicates in this case the combination of the different radio 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 radio cells (yellow, red, green) with a number of clients and one respective access point. The red arrows follow the communication path between a client of the yellow cell and a client of the red cell.

4.2 The roaming method

Motion of clients between the radio cells: Roaming

If a WLAN spans a larger area, the radio field of one access point (radio cell) is usually not enough. Several radio cells are required to illuminate the area in terms of radio technology. If the radio areas of the access points overlap only a very little bit, the clients should be permitted to freely move, without an interruption of the network connection. Not only within their own radio cells but also transboundary into other radio cells.

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

For the roaming process it is necessary that the individual radio cells overlap each other and that the bordering radio cells communicate on different channels with each other. If all radio cells would use the same channel, a client located in the overlapping area would permanently have faulty reception. (See section 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 100 ms occurs. This time is necessary to

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

If this time is tolerated by all communication nodes, communication continues undisturbed.

If very fast update times are required, e.g. for PROFINET I/O communication, access points and client modules have to be used that support the iPCF proprietary process (see section 4.6.1) for fast roaming and deterministic data traffic.

4.3 Infrastructure networks

The operation of WLANs with the aid of coordinating access points is referred to as “infrastructure mode”.

The following sections show several examples of infrastructure network topologies.

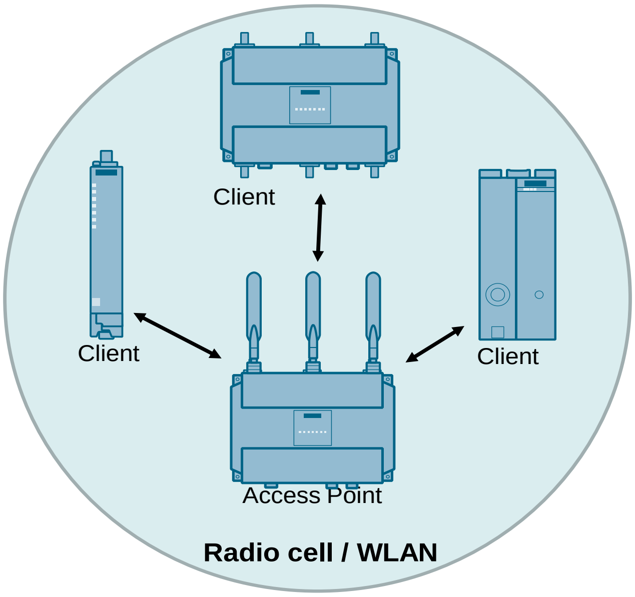
4.3.1 Standalone networks

Description

Standalone networks consist of a number of clients which are all located in the radio cell of one single access point. The function of the access point is limited to the coordination of the client communication to each other.

Illustration

Figure 4-3



The above figure shows such a standalone network. It includes an access point which coordinates the data communication of the other bus nodes and via which the entire traffic is directed. The access point determines the “SSID” (“Service Set Identifier”) of the network, in other words, its “name”.

It is not necessary that all network nodes of a standalone network have direct contact to each other.

The maximum expansion of such a network is limited by the condition that all clients have to be located within the range of the access point (red circle).

4.3.2 Mixed networks

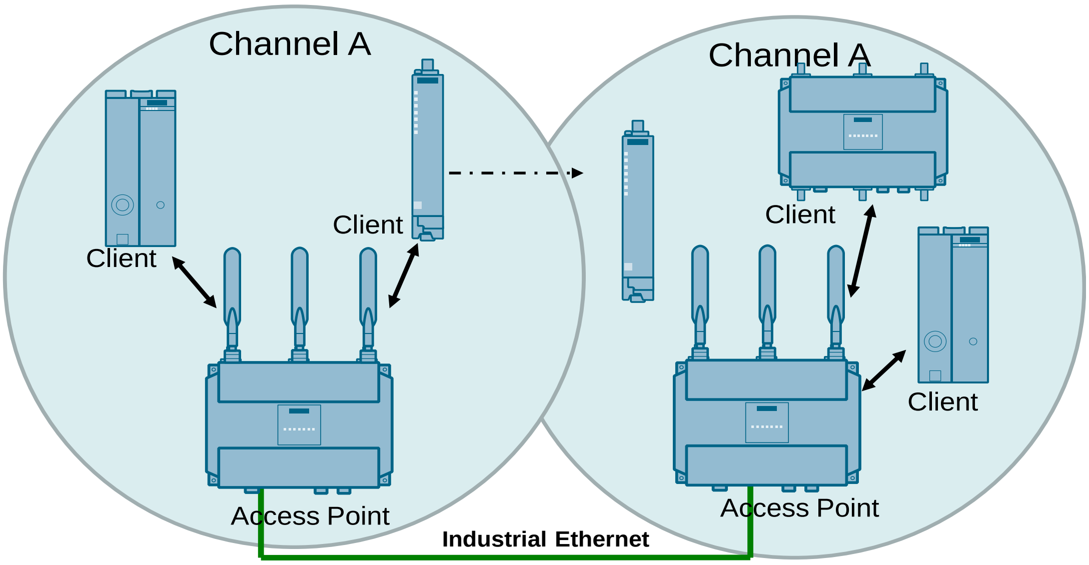
Description

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

Several access points can be connected to the cable-based network. This means that the access points generate several radio cells. If these cells cover a specific area completely, the clients located in this area can move from radio cell to radio cell (so-called “roaming”, see chapter 4.2).

Illustration

Figure 4-4



A number of access points are connected by a wire-bound Ethernet line. (Any other stationary nodes can also be connected to the Ethernet segment.) Several nodes connected via WLAN (clients) are located within the radio field covered by the access points (red circles above).

Mixed networks allow roaming, i.e. the change of a mobile node from one radio cell to a neighboring cell (see above, dotted arrow).

WLANs set up as described above, can theoretically reach any size. Interferences with reception may occur within the overlapping range of the radio cells since the access points operate on the same frequency.

4.3.3 Multi-channel configuration

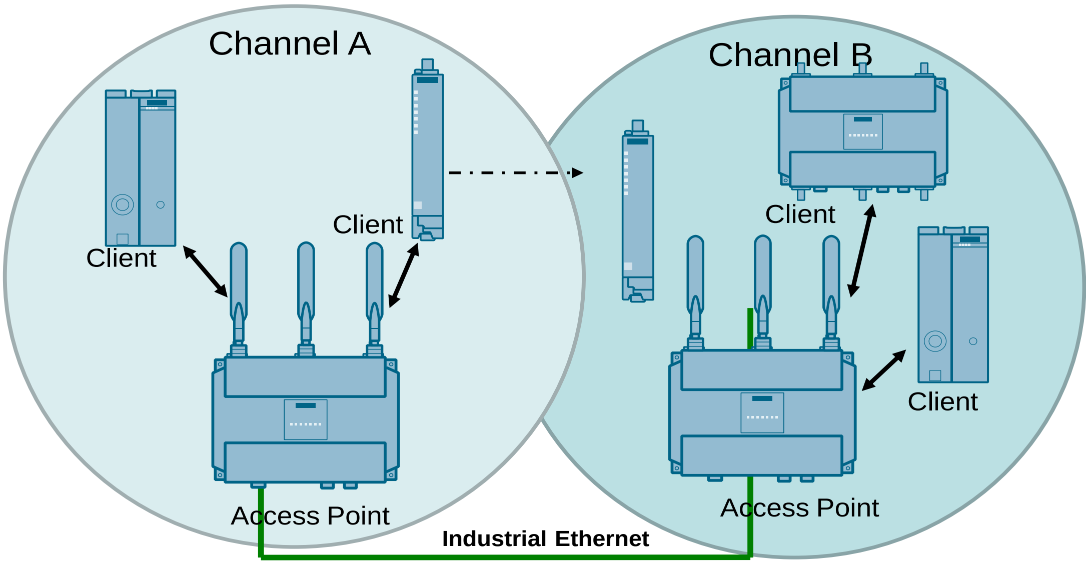
Description

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 radio cells overlap.

At the same time, roaming, thus the change of one client from one cell to another is facilitated, which results 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 cable-based 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 on which the access points transmit are indicated by circles in different colors.

In practical operation, this configuration is most frequently used for WLAN and is normally chosen.

4.3.4 Wireless Distribution System (“WDS”)

Description

In normal operation, the access point is used as interface to a cable-bound network and communicates with the clients. However, there is also the application case where several access points have to communicate with each other, for example, in order to enlarge the range or to establish a wireless backbone (see following chapter). This mode 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 one another* via a second medium (Industrial Ethernet cable in the case of the multi-channel configuration) but via the radio network.

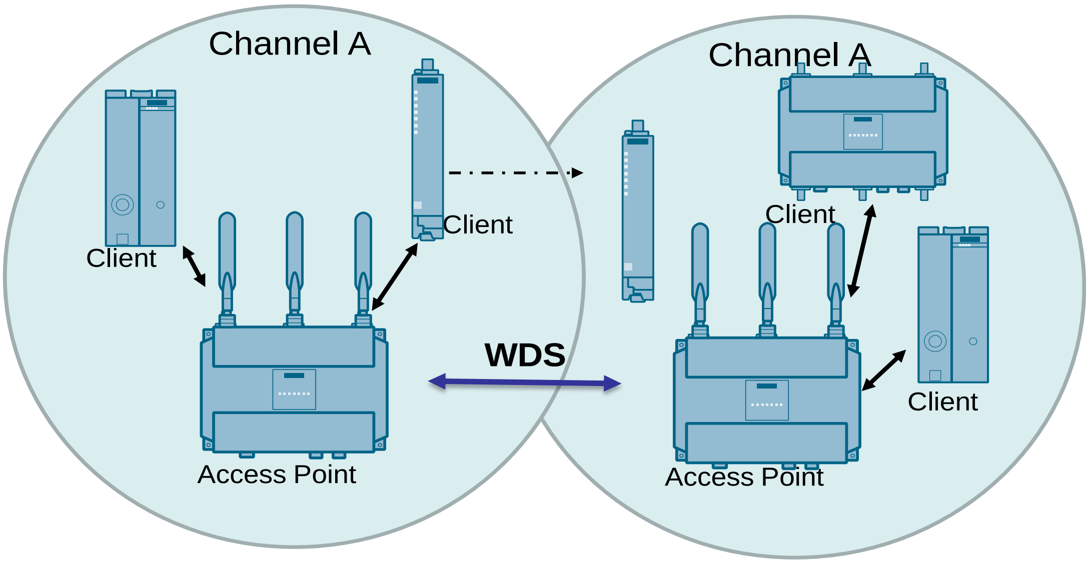
If communication between the access points is now permitted and the access of clients is blocked, it is referred to as a pure WDS.

The WDS is characterized by three properties:

- The distance between the access points must be small enough to each other to ensure that every access point is 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 additionally permitted, the effective data rate of the access point is reduced, since the bandwidth has to be shared.
- All access points that are to communicate with each other, have to use the same channel.

Illustration

Figure 4-6



The above figure illustrates the principle of operation, compare also Figure 4-4. Several nodes connected via WLAN (clients) are located within the radio field covered by the access points (red circles above). Additionally, the access points maintain a further radio connection between each other.

4.3.5 Redundant radio connection

Description

To establish a redundant backbone it is necessary to use access points which feature two radio interfaces and which can thus simultaneously transmit on several frequencies.

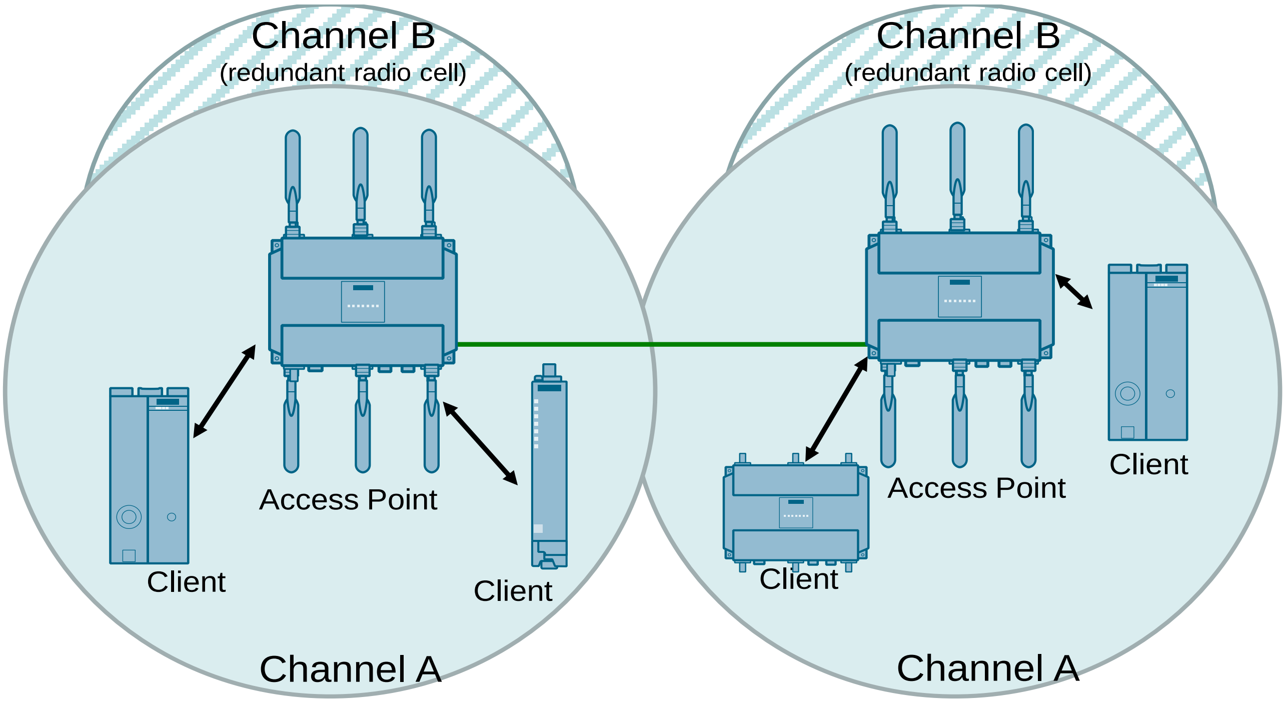
With this condition it is possible to establish:

- a redundant mixed network or
- a redundant wireless distribution system (see chapter 4.3.4), which, based on its location cannot be set up as a wired network.

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

Redundant mixed network

Figure 4-7

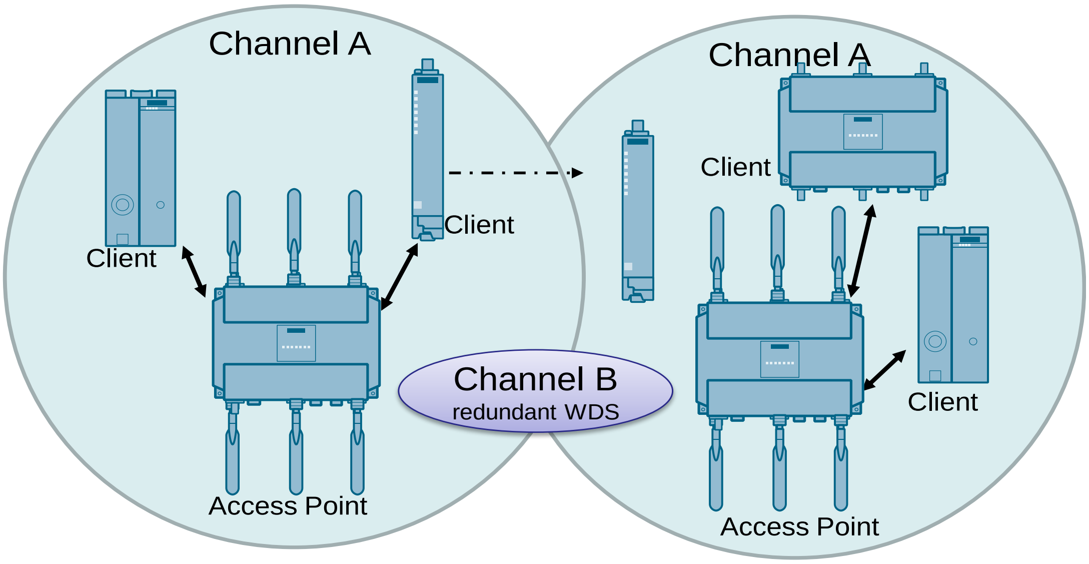


The access points establish an independent radio cell per radio interface, where primarily only one radio cell is used.

If data transfer is no longer possible via the radio cell of the first radio interface, the clients can automatically switch to the radio cell of the second radio interface. The 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 antennae.

4.4 Coordinating the data transfer

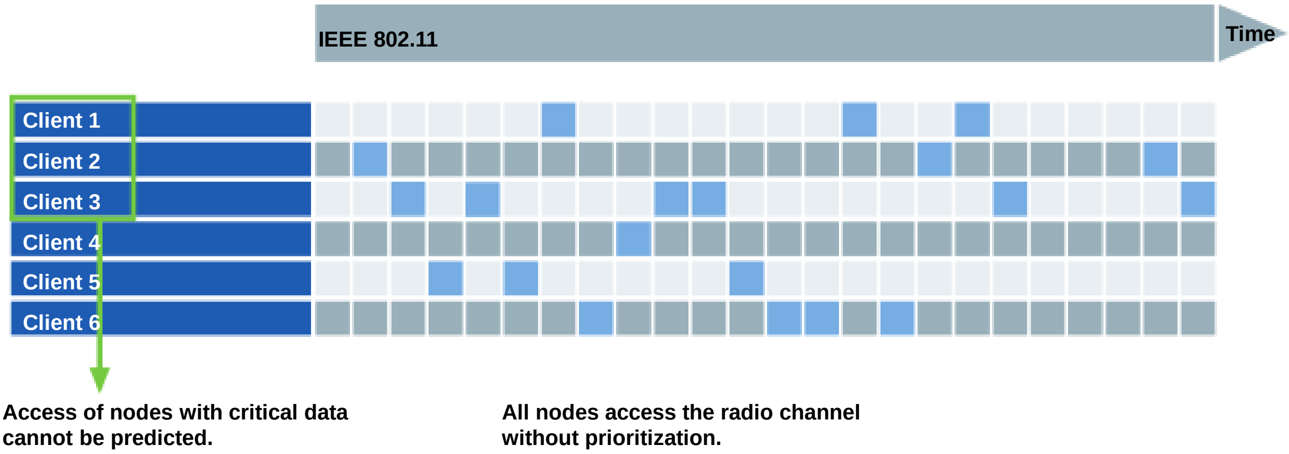
For a WLAN according to the IEEE 802.11 standard two approaches are differentiated to coordinate the communication in a shared medium:

- the basic access method with distributed coordination function (DCF)
- The point coordination function (PCF)

4.4.1 DCF ("Distributed Coordination Function")

For a WLAN in accordance with the IEEE 802.11 standard, all nodes are principally "responsible for themselves" and access the radio channel in an uncoordinated way. The access of nodes with critical data cannot be forecasted.

Figure 4-9


IEEE 802.11
Time
Client 1
Client 2
Client 3
Client 4
Client 5
Client 6
Access of nodes with critical data cannot be predicted.
All nodes access the radio channel without prioritization.

The data transmission according to the CSMA/CA method is binding for all participants.

In order to reduce the collision probability, a station ready to transmit, listens to the medium for a wait time that is made up of a constant wait time (DIFS; Distributed Coordination Function InterFrame Space) and a random wait time. If the medium is occupied it is waited until the end of the data transmission. Afterwards a fixed wait time starts again that is extended with the reduced random wait 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 acknowledgement telegram. Here, a constant wait time (SIFS; Short Coordination Function InterFrame Space) also has to be maintained first, in order to avoid collision.

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

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

4.4.2 "Hidden Station and RTS/CTS" method for collision avoidance

A station cannot always detect whether the medium is free. This is especially the case if two nodes of a radio cell cannot "see" each other (i.e., they are not located within each other’s reach). This WLAN problem is defined by the expression “hidden station”.

If, however, both try to communicate with a third node which is located between them (and which simultaneously has contact with both transmitters), conflicts occur.

The solution of the “hidden station” problem lies in the RTS/CTS method.
In order to avoid interferences, the medium is blocked for other stations for a period of time, by the station ready to transmit and the receiving station by a request to send (RTS) and clear to send (CTS) dialog. It is sufficient here when all stations in the catchment area of the transmitting station listen to one of the two RTS/CTS signal, in order to put them to wait mode.

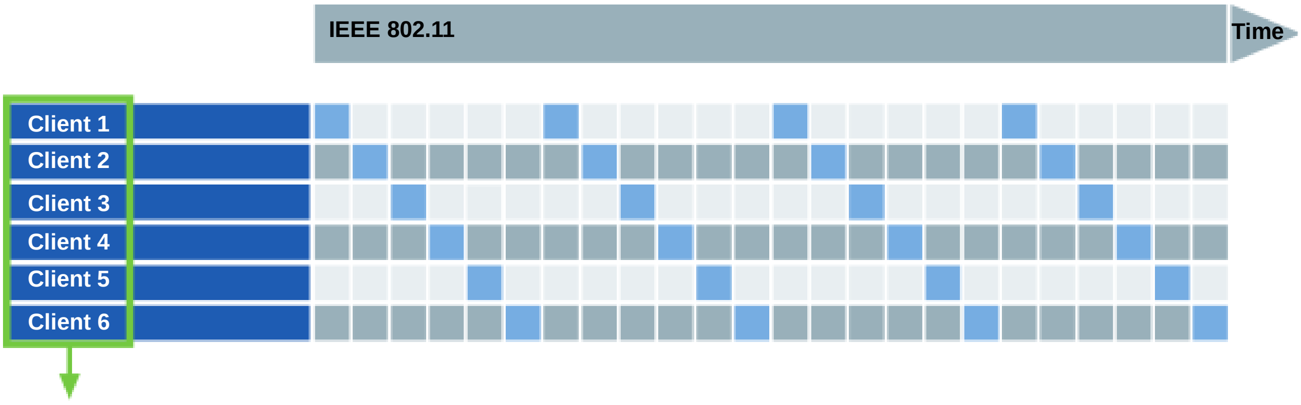
With the aid of this method, the number of necessary transmission repetitions is considerably reduced since the collision is already detected before sending longer data packets. However, the overhead produced by the RTS/CTS frames can reduce the achievable data throughput.

4.4.3 PCF (“Point Coordination Function”)

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

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

Figure 4-10



Access for all nodes can be predicted.

All nodes can predictably access the radio channel.

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

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

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

4.5 Functions for the network management

4.5.1 VLANs ("Virtual LANs")

The segmentation of a physical network into several logic "virtual" networks can be performed for cable-based as well as radio networks. Today VLANs normally follow the IEEE 802.1Q standard.[15]

Segmentation of the data traffic

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

Advantages

Using VLANs achieves a number of advantages:

- Configuration errors remain restricted to the VLAN, in which they were made, and can no longer bring down the entire LAN.
- Broadcasts, i.e. transmissions to a general circle of receivers, are no longer performed via the entire LAN but only via the respective VLAN; this reduces the network load.
- The individual VLANs can have various priorities assigned to them for preferred transportation of messages from high-priority stations.
- In contrast to using IP subnets, the stations of different VLANs can have the same IP addresses. This makes better use of the restricted IP address space and production cells of identical structure can be configured with identical IP addresses, which reduces configuration and administration expenses.
- 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 security of the network.

Note

You will find an animated demonstration system on this topic in the Siemens Industry Online Support (Entry ID: 31770396):
http://support.automation.siemens.com/WW/view/en/31770396

[15] Older protocols such as ISL ("Inter Switch Link") and VLT ("Virtual LAN Trunk") have become insignificant today.

4.5.2 STP (“Spanning Tree Protocol”)

Description

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

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

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

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

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

In regular operation all messages run via the optimal path.

4.5.3 RSTP ("Rapid Spanning Tree Protocol")

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

For these reasons, STP was expanded to the "Rapid Spanning Tree Protocol" (RSTP, IEEE 802.1w).
This mainly differs from STP by the switches, which already collect information on alternative routes at the time of undisturbed operation.

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

Note Further information on the topic of "RSTP in wireless LANs" is available in the Siemens Industry Online Support (Entry ID 30805917):
http://support.automation.siemens.com/WW/view/en/30805917

4.5.4 MSTP ("Multiple Spanning Tree Protocol")

STP as well as RSTP works with a global tree topology (spanning tree) for the entire network. Certain paths are not used to guarantee loop freedom. The existing path resources are therefore not efficiently used. An individual spanning tree has the disadvantage that the reconfiguration takes relatively long for large networks.

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

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

4.6 Proprietary expansions of the IEEE 802.11 standards: iFeatures

4.6.1 iPCF (“Industrial Point Coordination Function”)

iPCF (“Industrial Point Coordination Function”) provides a proprietary alternative to PCF developed by SIEMENS, which solves several problems related to PCF (see chapter 4.4.3). Furthermore iPCF enables the clients a very fast exchange of the radio cell, where the log-off and new logon of the client ("handover") happens so quickly that the real time requirements to the communication are still met.

Function principle

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

These properties result in the following effects:

- The access point can be parameterized to perform the pollings in a very fast sequence. This results in very short guaranteed response times (deterministic transmission): The response times can be reduced to about 2 ms per network node, i.e. a response time of less than 10 ms is guaranteed for 4 clients.
- The transmission of larger, non-time critical messages is delayed until free cycle time is available.
- Polling a node can be seen by all other nodes in the radio cell. This is how a client can detect the quality of the radio connection to the access point even if it does not itself communicate with the access point.
- Due to the shorter polling cycle times a client will very quickly know whether the connection to its access point still exists or not. If the contact has got lost, the client can react very quickly and establish a connection to an alternative access point.
- In the iPCF mode, the search for a new access point as well as the logon to this access point is optimized in its time behavior. Handover times of clearly below 50 ms are achieved.

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

An optimal performance with iPCF is achieved if the clients follow fixed paths (e.g. when using RCoax cables). For movable nodes in communication with stationary access points the application of iPCF-MC is recommended (see 4.6.2).

Restrictions by iPCF

iPCF can only be operated alone. A combination with other industrial functionalities (iFeatures such as, for example, iPCF-MC, Dual Client) is not possible.

The iPCF method is a proprietary development of Siemens AG and works only with nodes where iPCF has been implemented. For one access point with two WLAN interfaces, however, it is possible to simultaneously set iPCF as well as standard WLAN.

If the iPCF mode is enabled, only the “open system” security settings with the AES encryption methods with 128 bit key length are supported.

Compatibility with other WLAN standards

“Mixed networks”, in which part of the devices is connected via DCF/iPCF, are not possible with iPCF.

4.6.2 iPCF-MC ("iPCF – Management Channel")

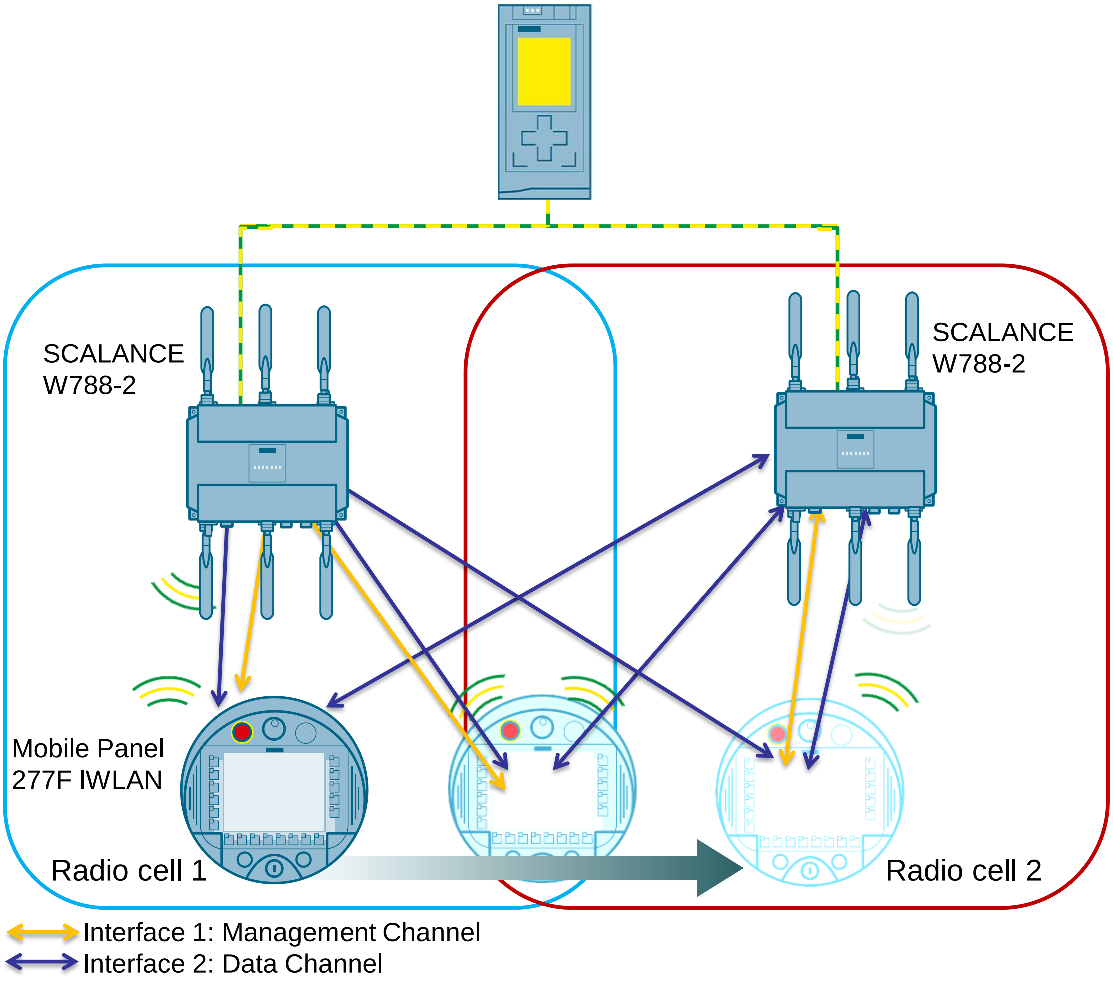
iPCF and iPCF-MC

iPCF-MC was developed in order to make the advantages achieved by iPCF also possible for freely movable nodes (see chapter 4.6.1) that communicate independent of a RCoax cable or directional antennae. For iPCF-MC, the client still searches for potentially suitable access points if it receives iPCF requests of the access point and the existing connection to an access point works interference free. If required, this enables a very fast change to a different access point. As compared to iPCF, the handover times of the iPCF-MC depend on the number of the radio channels used.

Function principle

If iPCF-MC is used, it is required to use an access point with two radio interfaces, a so called dual access point. One interface works as management channel and transmits short telegrams ("beacon") with administrative information (e.g. channel setting of the data channel and SSID). The other interface (data channel) only transmits the user data.

Figure 4-11



Restrictions by iPCF-MC

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

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

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

Requirements

For the use of this function, the following requirements are necessary:

- iPCF-MC uses both radio interfaces of the access point differently: One interface works as management interface. The other interface transfers the user data. Therefore only SCALANCE W700 devices with two WLAN interfaces can be used as access points.
- Management cannel and data channel must be operated in the same frequency band and have to match regarding their radio coverage. iPCF-MC will not function if both radio interfaces are equipped with directional antennae which cover different areas.
- The management channel of all access points between which a client should change must use the same channel. A client only scans this one channel to find an accessible access point.
- For the management 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 the transmission conditions.

By minimizing the number of access points used along the path and avoiding overlapping radio channels, fewer interferences occur with the neighboring access points. This leads to a higher data throughput of the entire system.

Function principle

iREF (industrial Range Extension Function) makes sure that the data traffic from access point to each individual client occurs through the respectively best suitable antenna.

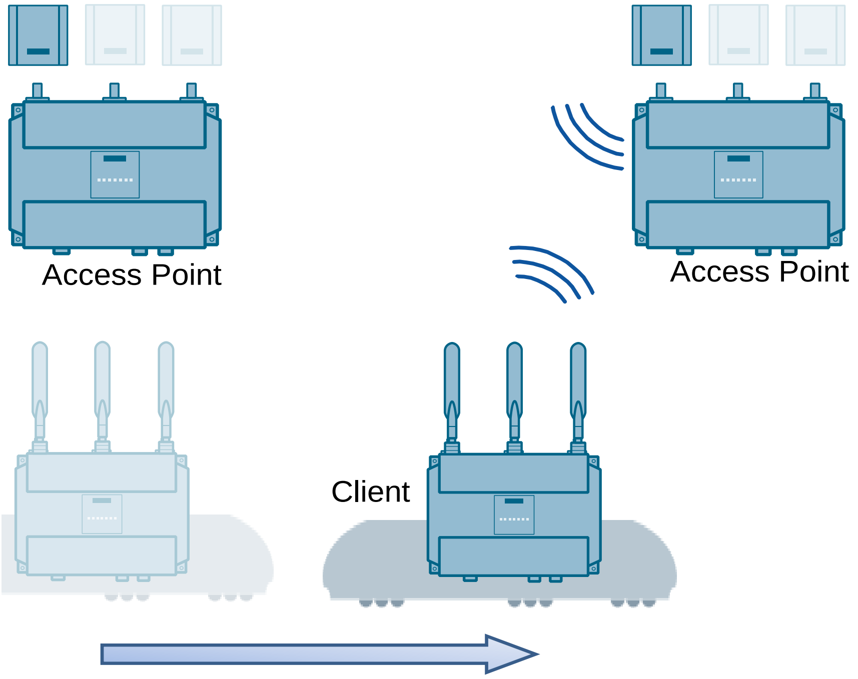
The access point specifies what antenna is best suitable on the basis of the RSSI values of received packets. Whilst taking into account antenna gain and possible cable losses, packets are only transmitted on those antennae, for which a maximum signal strength is to be expected on the side of the client.

During this time, the other antennae are inactive and the legally permitted transmission power is available for the selected antenna.

Figure 4-12

Through the switching off of antennae that do not recognize WLAN node, the transmitting power of the other antennae is increased in order to achieve the maximum range.

Antenna 1 active, because WLAN node is connected.



Restrictions by iREF

iREF can only be operated alone. A combination with other industrial functionalities (iFeatures such as, for example, iPCF, iPCF-MC) is not possible.

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

Requirements

In order to be able to use the iREF technology, the device has to have a minimum of two active antennae.

4.6.4 Inter AP Blocking

The clients that are connected with an access point, can normally communicate with all devices of the layer 2 network.

The communication to the clients that are connected with the access point can be restricted with Inter AP Blocking. Only the devices whose IP addresses are known to the access point are accessible to the clients. A communication with the other nodes in the network is therefore prevented.

Note

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

http://www.automation.siemens.com/net/html_00/support/whitepaper.htm

4.6.5 Usable IWLAN devices

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

Table 4-1

IWLAN device	Type	iPCF	iPCF-MC	iREF	Inter AP Blocking
SCALANCE W788-1 RJ45 / M12	AP	KEY PLUG	- (only as client)	KEY PLUG	KEY PLUG
SCALANCE W788-2 RJ45 / M12 (EEC)			KEY PLUG		
SCALANCE W786-1 RJ45			- (only as client)		
SCALANCE W786-2 RJ45 / SFP			KEY PLUG		
SCALANCE W786-2IA RJ45					
SCALANCE W774-1 RJ45/ M12 (EEC)			- (only as client)		
SCALANCE W761-1 RJ45		-	-	-	-
SCALANCE W748-1 RJ45 / M12	Client	KEY PLUG		-	-
SCALANCE W734-1 RJ45				-	-
SCALANCE W722-1 RJ45		x	x	-	-
SCALANCE W721-1 RJ45		-	-	-	-
Mobile Panel 277 IWLAN		-	x	-	-

[16] x: The function is available
-: The function is not available
KEY-PLUG: The function requires enabling via respective KEY-PLUG (see chapter 9.1.1).

4.6.6 iFeatures and PROFINET I/O

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

The WLAN is a shared medium in its origin. All nodes are principally “responsible for themselves” and access to the radio channel in an uncoordinated way. The access of nodes with critical data cannot be forecasted. Under these conditions PROFINET I/O can only be used at very limited or certain boundary conditions in a standard WLAN.

Real time communication is also made possible for a radio network through the proprietary SIEMENS iFeatures

- iPCF
- iPCF-MC

.

5 Data Security and Encryption

5.1 Attack scenarios and security mechanisms

5.1.1 Basics of WLAN security

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

Due to advances in security standards and the performance of the components, the radio networks today can be considered as secure as cable-based networks.

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

A reduction of the radio power can of course only provide limited protection and cannot be realized at any scale. More advanced, effective and secure methods are 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

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

- *Access Points configured with errors*: Access points which were connected with the cable-based network by an internal user but contain a configuration error. If, for example, no security settings were made, the respective access point provides free network access for all.
- *Ad hoc wireless network:* Operating systems such as Windows enable configuring networks consisting of several wireless clients without the access point in between. If one of the computers is configured so that it forms part of an ad hoc network as well as establishing connections with the company WLAN, it may provide unintentional access for hackers.
- *Faulty client connections*: If companies are located directly within physical vicinity, the company WLANs most probably use the same network information. In this case a wireless client connects with the first accessible access point. However, if it is part of a neighboring WLAN, this may cause a security risk.

Attack methods

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

- *Rogue Access Points*: An illegal access point connects with the cable-based network and creates free LAN access for malicious or unauthorized users.
- *Honeypot Access Points*: Some hackers are capable of determining the configuration settings of WLANs and use an access point with the same settings within network reach. Through this intentional faulty connection the clients create a connection with these "honeypots" assuming that they are contacting an official access point. Experienced hackers can make use of this by connecting network resources with the AP, which act as bait so that the users log on as usual and so give the hacker the opportunity to take unauthorized possession of passwords or confidential documents.
- *Access Point MAC Spoofing*: Wireless client computer can be configured as access points. This way a hacker can abuse a normal PC as honeypot.

Manipulation options

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

- *Unauthorized client accesses*: Hackers permanent search access options in wireless networks. If a network has a weak, or non-existent user authentication, access to the company network is made very easy and the hackers can retrieve information or attack resources, leading to failures.
- *Denial of Service (“DoS”)* Networked devices must react to all client requests. Hackers use this property by flooding a network resource with more requests than they can handle. Distributed DoS attacks increase the problem by preparing a number of “ignorant” computers using a hidden code, which then simultaneously perform DoS attacks of a possibly enormous proportions.
- *“Man in the Middle”*: If data is unprotected, hackers can intercept messages and manipulate contents by disguising themselves as nodes on the travel path of a communication connection.
- *IP Spoofing:* By manipulating the source IP address in the package header, a hacker can access traffic of a correctly authenticated user and pretend that the user uses the computer of the hacker. Subsequently, all data and messages of the server go back to the hacker.
- *Hijacking*: Using software, secretly installed on the PC of a company user, a hacker can take control over the affected computer and gain access to the resources which the user can access, or damage servers or other computers.

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.

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

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

On the other hand, statistical methods can be used to determine characteristics from the transmitted message traffic, which again enable to draw conclusions about the used key as long as there is an adequate number of messages for the analysis.[17]

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

ACL access control

In the network management, filter tables ("Access Control List") with IP addresses can be created which allow or refuse access to specific addresses. This way, simple, albeit comparatively insecure access protection can be implemented for the network.

It actually cannot be excluded that IP addresses are manipulated (so called "spoofing") so that ACL will only offer adequate protection for a network in connection with other measures.

SSID

The SSID ("Service Set Identifier") is a freely selectable name for the WLAN and identifies it.
A WLAN access point sends this SSID if a client searches for wireless networks.

For this reason – from a security point of view - SSID should not give any clues to the company, purpose of the network or location, otherwise the curiosity of hackers or other unauthorized people could be aroused.
However, the transmission of the network name can also be suppressed. Since the clients can no longer "see" the radio network, the SSID has to be entered correctly in the client configuration so that it can connect with the desired WLAN.

[17] Frequent manual change of the key by the user would increase security, however, in practice this is rarely pursued conscientiously.

Note Since no encryption is used for the SSID transmission, this function can only basically protect from unauthorized accesses. The use of an authentication method (e.g. WPA2 (RADIUS), if not possible WPA2-PSK) offers greater security. Furthermore, it has to be expected that certain terminal devices may have problems with access to a hidden SSID.

5.2 Measures for increasing the WLAN security

5.2.1 The IEEE 802.11i expansion

The WEP method has some weaknesses, so 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 expansion of the 802.11i standards was founded that deals with the security of the data transmission via WLANs, especially with the definition of encryption algorithms and integrity checks[18] for wireless transmission.
The aim of the IEEE 802.11i extension is the development of standardized security measures for wireless data transmission that satisfy today’s security requirements.

Three methods were the result:

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

TKIP

With TKIP an optional encryption method was developed by the task group which is based on the WEP method but largely fills its security gaps. This interim solution was necessary to guarantee the operation of older WLAN devices in a network.

To encode a message, the “Temporal Key Integrity Protocol” uses a key as well as an additional initialization vector. Various combinations of initial key and initialization vector makes the encoding work as if the key was continuously changed which makes cracking the code more difficult.

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

[18] An integrity check can prevent data manipulation during the data transmission.

AES-CCMP

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

This method requires new WLAN chip sets and can therefore no longer be used on older WLAN products.

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

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

Note Due to the increasing security requirements only the AES encryption method is supported for iPCF and iPCF-MC

AKM

Apart from the definitions for secure data transmission and checking the frame integrity, the IEEE 802.11i extension also intends further authentication measures and algorithms for automatic key management. As authentication method the standards of IEEE 802.11X or PSK (“Pre-Shared Key”) are used (see chapter 5.3).

5.2.2 Wi-Fi Protected Access security standard

The development of an encryption algorithm that was supposed to replace WEP by the IEEE task group 802.11i was delayed so that the “Wi-Fi Alliance” recommended the application of WPA (“Wi-Fi Protected Access”) with TKIP as a subset of the 802.11i standard as an interim solution.

WPA provides two options as authentication:

- WPA (RADIUS): The authentication by a server (RADIUS server) is mandatory for WPA (RADIUS) (see chapter 5.3.1). Further security is built in through dynamic key exchange at each data frame.
- WPA-PSK: For this method, the authentication is by password and not by server (see chapter 5.3.2). This password is configured manually on the client and on the server.

However, following the adoption of the 802.11i standard this is superfluous and the Wi-Fi alliance has established WPA2 (“Wi-Fi Protected Access 2”) as the new security standard. The encryption of WPA2 orientates itself on the full implementation of the IEEE 802.11i extension and uses AES-CCMP.

As for WPA, the authentication can be performed via an authentication server or PSK.

Note The transmission standard IEEE 802.11n with the setting "802.11n" or "802.11n only" 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 IEEE802.1X does not define the encryption of the data traffic between access point and client, but the login procedure as well as the assignment of access rights for clients. For this purpose, the RADIUS protocol is used on the basis of “EAP” (“Extensible Authentication Protocol”) for larger networks and PSK in office networks.

RADIUS protocol

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

For RADIUS there is a central so-called RADIUS server, which contains a list with the access authorizations of all nodes. If a client wishes to connect to the network, the access point forwards the request to the RADIUS server. It reacts by generating a “challenge”, i.e. a request for which the client can only send the 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, it can therefore not be intercepted by somebody without authorization.
- Since the access authorizations are saved on a central server, the method is particularly suitable when using roaming clients. Not all access points need to store the access data of the clients, but they can request them any time at the RADIUS computer.

EAP

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

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

Aside from this method, a large number of other, partly manufacturer-specific, protocols exist that can be used 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 by the nodes before communicating.

Further parameters for generating the PSK are the SSID and the SSID length.

5.4 Security functions and data rate

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

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

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

Note

Observe the following notes to protect your network from attacks:

● Use as secure connection with HTTPS. In contrast to HTTP, HTTPS enables you secure access to the configuration of WLAN clients and access points via the web based management.

● Use WPA2/ WPA2-PSK with AES in order to prevent password abuse. WPA2 / WPA2-PSK with AES offers greater security.

● Protect your network from man-in-the-middle attacks by a network setup that makes it more difficult for the attacker to get into the communication path between two terminal devices:

- WLAN device, for example, can be protected by the agent IP, only being accessible via an individual management VLAN.
- Another possibility is to install an independent HTTPS certificate on the WLAN client / access point. The HTTPS certificate checks the identity of the device and regulates the encrypted data exchange. You can install the HTTPS certificate, for example, via HTTP.

● Use SNMPv3. SNMPv3 offers you the greatest possible security when accessing WLAN devices via SNMP.

6 Coexistence of IWLANs with other Radio Networks

Possible sources interfering with the operation

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

- An environment with obstacles and objects that have an influence on the propagation of radio waves (e.g. metal etc.),
- other radio transmitters using the same frequency band (other WLAN nodes, but also Bluetooth, etc.),
- devices sending unspecific interference pulses (welding devices, switching devices)

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

Coexistence management

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

An expert should always be consulted for the coexistence management.

Radio analysis

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

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

The principle of decoupling

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

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

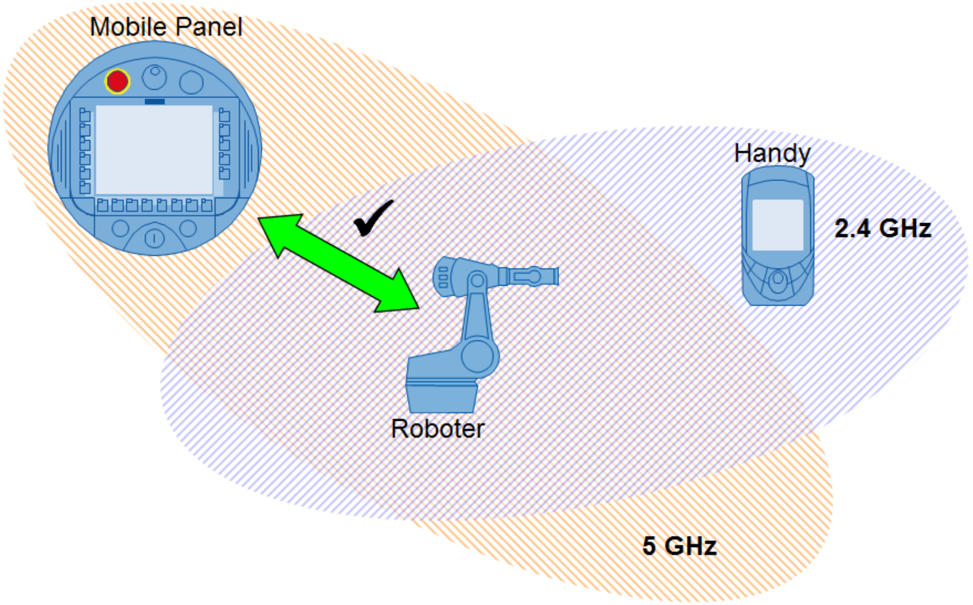
For the **frequency decoupling** it is decisive that the frequency ranges of the individual radio systems overlap as little as possible. In the easiest case this is done by selecting the respective radio channels, in a more advanced case this is achieved by modulation and multiplex method (see chapter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

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

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

The following graphic shows an example for decoupling in the frequency range: The MP277 Mobile Panel can communicate with the robot, even though it is at the same time within in the transmission range of the cellular phone, since both communicate on different frequencies (orange: 5 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 issue can be found on the web in the following brochure which was edited by “ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V”[19]:

ZVEI_Koexistenz_von_Funksystemen_in_der_Automatisierungstechnik.

The individual steps of the coexistence management are summarized in the VDI/VDE guideline 2185 (payable download)

"Funkgestützte Kommunikation in der Automatisierungstechnik"

7 Country Approvals

7.1 General

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

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

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

Respective components

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

- access points
- clients (including interface modules)
- mobile operator panels (see chapter 8.7)
- Antennae

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.com/radio approvals

Responsibility

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

[19] www.zvei.org

7.2 Country approvals in the SCALANCE W devices

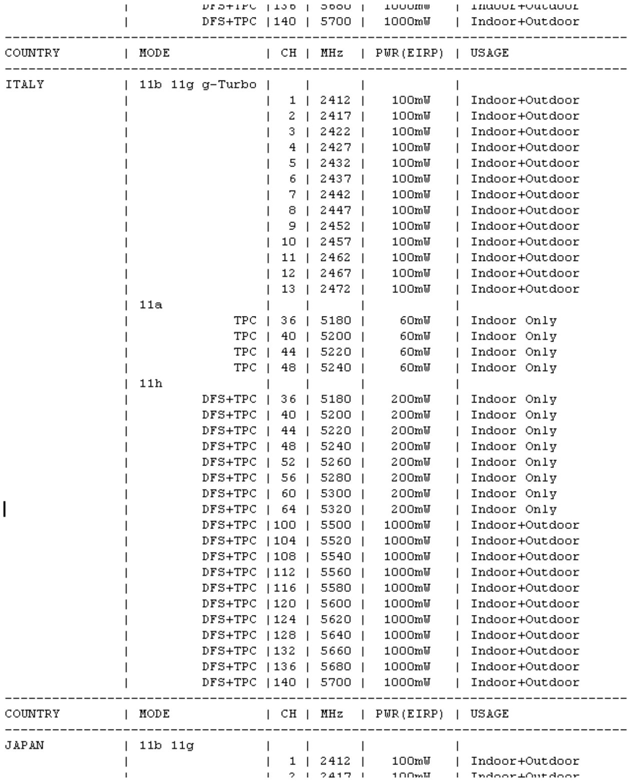
The national standards that were current at the time the firmware was published are stored in the firmware of each SCALANCE W device (compare chapter 8.1.2). These standards can be read out via the web interface of the access point or the client in the menu “System” > “Load&Save”.

Note Current descriptions can be found in the manual of the respective device. They can be found in Siemens Industry Online Support: https://support.industry.siemens.com/cs/ww/en/ps/15853/man

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

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 For updated lists with country approvals for the individual SCALANCE W products please refer to the manual "SIMATIC NET Industrial Wireless LAN Approvals SCALANCE W700 802.11n" in entry ID 109476834.

8 SIEMENS NET Products for Setting up an IWLAN

8.1 General information

8.1.1 Overview of the product range

For the setup of a secure and reliable WLAN, SIEMENS offers a wide product range. The next chapters introduce you to these properties and show you the application and the practical use.

The following figure shows you an selection of SIMATIC wireless products.

Figure 8-1

Note Further, continuously updated information on SCALANCE W products are available at: http://www.siemens.com/iwlan

8.1.2 Division of the SCALANCE W products

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

The SCALANCE W device family comprises the products:

- IWLAN controller,
- Access Points and
- Client module.

The IWLAN controller

The SCALANCE WLC711 IWLAN controller is a network device for the central management of a wireless LAN in the industrial environment. It supports commissioning, diagnostic, access control and security settings of the wireless network as well as firmware updates of the access points.

Note More and detailed information on SCALANCE WLC711 can be found in the Siemens Industry Online Support: https://support.industry.siemens.com/cs/ww/en/ps/15870/man

The access points

In this series, the W78x, W77x and W76x modules are access points which are used as network switches of the individual radio cells and as transitions between Industrial Ethernet and WLAN segments. Two different variants of access points belong to the modules:

- Standalone Access Points
- Controller-based access points

Note Manuals on 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 designation "W74x", "W78x" and "W73x". They are connected to mobile end nodes via Ethernet and communicate 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 WLC711 IWLAN controller

SCALANCE WLC711 is a network instance for the central management of a wireless LAN in the industrial environment. It supports commissioning, diagnostic, access control and security settings of the wireless network as well as firmware updates of the access points.

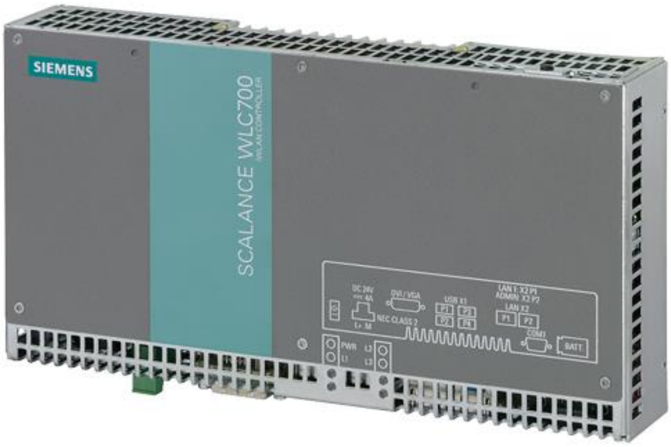
Only controller-based access points can be operated on the SCALANCE WLC711.

General

The requirements to WLAN in the industrial area as well as the variety of the possible applications and uses have continuously increased over the last years. Aspects such as higher performance and data rate as well as low management effort of the network, present new challenges today. As a reply, a further architecture has established itself in WLAN networks in the office area for years: the controller-based architecture.
With this architecture, access points are no longer as operated as standalone but are controlled by an IWLAN controller. Via the controller, management data and user data can be transmitted to and from the individual access points.

With the SCALANCE WLC711 the SIMATIC NET portfolio offers the option of controller-based IWLANs.

Figure 8-2



Basic hardware

The basic hardware is a fan-less industrial PC with two separate gigabit Ethernet interfaces:

- Management port: The controller is configured via this port.
- Data port: This is where the data is transmitted.

Characteristics

The SCALANCE WLC711 is characterized by the following characteristics:

- Central configuration and firmware upgrade of the access points via a user interface in the controller.
- Monitoring of larger WLAN networks: The IWLAN controller offers the option to monitor the network in real time via the "Wireless Assistant Home Screen".
- Assigning of properties to groups of users, devices and services.
- Roll-based security functions (authentication, intrusion detection, rogue AP detection, firewalls, etc.).
- Fast layer2 and layer3 roaming (e.g. for logistic scanner and VoIP).
- Expanded QoS functions guarantee end-to-end IP prioritization for voice, video & data.
- RF management (automatic setting of channels and transmission power).
- Reliable meshed WLAN through redundant paths: In the event of a failure of a connection or an access point, the network and the packet route is automatically reconfigured.
- Internal and external captive portal (guest portal): The guest is automatically forwarded to a login web site where s/he has to enter his/her login data.

Note

More and detailed information on SCALANCE WLC711 can be found in the Siemens Industry Online Support:
https://support.industry.siemens.com/cs/ww/en/ps/15870/man

8.3 SCALANCE W Standalone Access Points

Standalone means that the access points are configured individually and that there is no higher instance that can control the network.
The access point in accordance with IEEE 802.11n can work in the 2.4 GHz band as well as in the 5 GHz band (see chapter 2.2.4).
Using special mechanisms and new technologies, a data throughput of up to 450 Mbps (gross) and an improved radio coverage is possible.

Per radio module up to three antennae can be connected. This divides the data stream between up to three transmitting antennae (spatial multiplexing).

Note With the implication of the new WLAN standard 802.11n in the SCALANCE W products, the modules have been completely innovated and all old devices are discontinued. The new devices cannot be used as spare parts for the old devices.

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

SCALANCE W788-x RJ45 Access Points

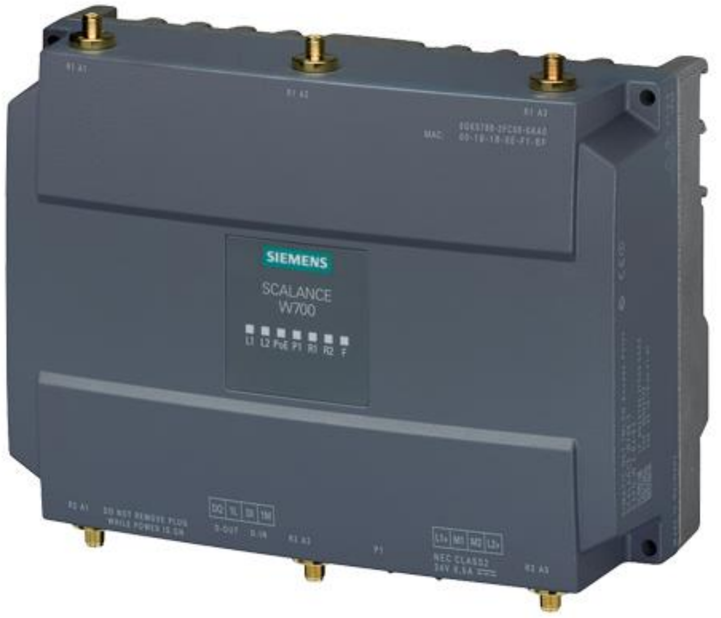
The SCALANCE W788-x RJ45 modules are built according to protection class IP30 and are, amongst other applications, very suitable for the use in control cabinet in industrial environments.

The Ethernet interface has been designed electrically (RJ45), is gigabit-capable and enables Power over Ethernet.

For the connection of the external antennae, R-SMA sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-3



The SCALANCE W788-x RJ45 can be ordered in the following variants:

- W788-1 RJ45 with one radio interface
  - MLFB: 6GK5788-1FC00-0AA0 or
  - MLFB: 6GK5788-1FC00-0AB0 (US variant)
- W788-2 RJ45 with two radio interfaces that are independent from each other
  - MLFB: 6GK5788-2FC00-0AA0 or
  - MLFB: 6GK5788-2FC00-0AB0 (US variant)

SCALANCE W788-x M12 (EEC) Access Points

The SCALANCE W788-x M12 is available in two versions:

- The standard W788-x M12 variant
- The EEC variant W788-x M12 EEC (Enhanced Environment Conditions)

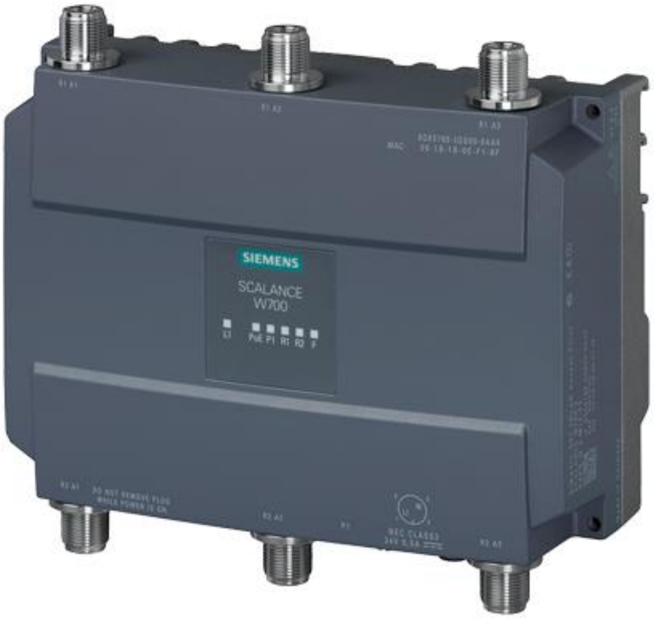
Both access points have protection class IP65 and are suitable for internal installation within industrial environments with particularly demanding environmental conditions.

Additionally, the EEC variant can be used in high-performance plant networks and applications with high temperature or EMV requirements.

The Ethernet interface has been designed electrically (M12). For the connection of the external antennae, robust N connect sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-4



The SCALANCE W788-x M12 can be ordered in the following variants:

- W788-1 M12 with one radio interface
  - MLFB: 6GK5788-1GD00-0AA0 or
  - MLFB: 6GK5788-1GD00-0AB0 (US variant)
- W788-2 M12 with two radio interfaces that are independent from each other
  - MLFB: 6GK5788-2GD00-0AA0 or
  - MLFB: 6GK5788-2GD00-0AB0 (US variant)
- W788-2 M12 EEC with two radio interfaces that are independent from each other
  - MLFB: 6GK5788-2GD00-0TA0 or
  - MLFB: 6GK5788-2GD00-0TB0 (US variant)

SCALANCE W786-x RJ45/SFP access points

The SCALANCE W786-x RJ45/SFP access points have been designed for protection class IP65 for the use within industrial environments with particularly demanding environmental conditions in public spaces or outside of buildings. The most important properties include insensitivity to extreme effects of the weather such as salt water spray, but also the rugged design in an impact-resistant and shock-proof plastic housing without destructible parts facing outwards.

The Ethernet interface is either designed as RJ45 or SFP.

SFP interface modules (Small Form Factor Pluggable) are small compact and pluggable transceiver modules and form the physical interface between the transmission medium and gigabit Ethernet. SPF modules are offered for various fiber optic cables.

Note Further information on SFP can be found in the operating instruction for the SCALANCE W786 in the Siemens Industry Online Support (Entry ID:62521860): http://support.automation.siemens.com/WW/view/en/62521860

For the connection of the external antennae, R-SMA sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-5

The SCALANCE W788-x RJ45/SFP can be ordered in the following variants:

- W786-1 RJ45 with one radio interface and external antennae
  - MLFB: 6GK5786-1FC00-0AA0 or
  - MLFB: 6GK5786-1FC00-0AB0 (US variant)
- W786-2 RJ45 with two radio interfaces that are independent from one another and external antennae
  - MLFB: 6GK5786-2FC00-0AA0 or
  - MLFB: 6GK5786-2FC00-0AB0 (US variant)
- W786-2IA RJ45 with two radio interfaces that are independent from each other and internal antennae
  - MLFB: 6GK5786-2HC00-0AA0 or
  - MLFB: 6GK5786-2HC00-0AB0 (US variant)
- W786-2 SFP with two radio interfaces that are independent from one another and external antennae
  - MLFB: 6GK5786-2FE00-0AA0
  - MLFB: 6GK5786-2FE00-0AB0 (US variant)

Access Points SCALANCE W774-1 RJ45

The SCALANCE W774-1 RJ45 modules are built according to protection class IP30 and are, amongst other applications, very suitable for the control cabinet in industrial environments.

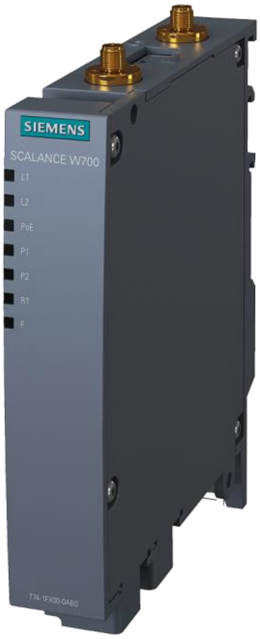
The well-balanced housing design makes them perfectly compatible with existing SIMATIC products in the control cabinet
(e.g. ET200SP, ET200MP, …).

The two Ethernet interfaces are electric (RJ45), one of which is suitable for the feed via Power over Ethernet.

For the connection of the two external antennae, R-SMA sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-6



The SCALANCE W774-1 RJ45 can be ordered in the following variants:

- MLFB: 6GK5774-1FX00-0AA0 or
- MLFB: 6GK5774-1FX00-0AB0 (US variant)

SCALANCE W774-1 M12 EEC access points

The SCALANCE W774-1 M12 EEC (Extended Environmental Conditions) have protection class IP30 and are suitable for the use in environments with extended environmental conditions.

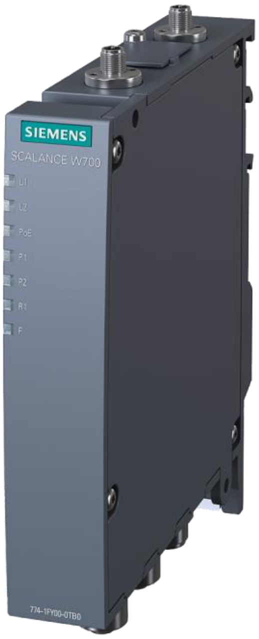
SCALANCE W774-1 M12 EEC products are particularly suitable for the use in vehicles or control cabinets due to the robust housing material (aluminum) and the compact design. They comply with approval
EN 50155 for railway applications and approval E1 for use in vehicles.

The well-balanced housing design makes them perfectly compatible with existing SIMATIC products.

The Ethernet interface has been designed electrically (M12). For the connection of the external antennae, two antennae connections of type R-SMA are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-7



The SCALANCE W774-1 M12 EEC can be ordered in the following variants:

- MLFB: 6GK5774-1FY00-0TA0 or
- MLFB: 6GK5774-1FY00-0TB0 (US variant)

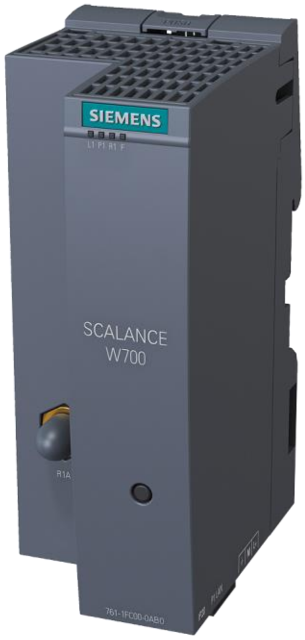
SCALANCE W761-1 RJ45 access points

The SCALANCE W761-1 RJ45 modules are built according to protection class IP20 and are, amongst other applications, very suitable for the use in control cabinet in industrial environments.

The well-balanced housing design makes them perfectly compatible with existing SIMATIC products.
(e.g. ET200SP ET200MP, ...).

The Ethernet interface has been designed electrically (RJ45). For the connection of the external antenna, a R-SMA socket is provided.

Figure 8-8



The SCALANCE W761-1 RJ45 can be ordered in the following variants:

- MLFB: 6GK5761-1FC00-0AA0 or
- MLFB: 6GK5761-1FC00-0AB0 (US variant)

8.4 Controller-based SCALANCE W access points

Controller-based access points can only be used in a network with an IWLAN controller, because they need its central management functions.

The controller-based access points in accordance with the IEEE 802.11n standard work in the 2.4 GHz band as well as in the 5 GHz band.

Regarding design and functionality they are identical to the standalone access points for IEEE 802.11n (see chapter 0). In contrast to those, the controller-based access points can only be used together with a controller.

The following controller-based access points can be ordered from the product portfolio:

- SCALANCE W788C-2 RJ45 with two radio interfaces that are independent from each other:
  - MLFB 6GK5788-2FC00-1AA0
- SCALANCE W788C-2 M12 with two radio interfaces that are independent from each other:
  - MLFB 6GK5788-2GD00-1AA0
- SCALANCE W788C-2 M12 EEC with two radio interfaces that are independent from each other:
  - MLFB 6GK5788-2GD00-1TA0
- SCALANCE W786C-2x RJ45 in the following variants:
  - W786C-2 RJ45 with two radio interfaces that are independent from one another and external antennae:
    - MLFB 6GK5786-2FC00-1AA0.
  - W786C-2IA RJ45 with two radio interfaces that are independent from each other and internal antennae
    - MLFB 6GK5786-2HC00-1AA0
- W786C-2 SFP with two radio interfaces that are independent from one another and external antennae
  - MLFB: 6GK5786-2FE00-1AA0

8.5 SCALANCE W clients

The SCALANCE W clients can be operated as standalone access points, as well as controller-based access points.

The modules are identical in construction to the corresponding access points (see chapter 8.3). However, the software differs in the functionalities, so that these devices are not intended for the network management as the access points, but for a communication amongst each other and with other network devices.

The clients furthermore form the interface between Ethernet-connected devices and WLAN. However, they do not transmit the complete network traffic, but only the messages of a limited number of Ethernet nodes.

The client modules in accordance with the IEEE 802.11n standard can work in the 2.4 Ghz band as well as in the 5 GHz band.

Using special mechanisms and new technologies, a data throughput of up to 450 Mbps (gross) and an improved radio coverage is possible.

The clients have a radio module. Up to three antennae can be connected here. Thus, the data stream can be divided between up to three transmitting antennae (spatial multiplexing).

Note

With the implication of the new WLAN standard 802.11n in the SCALANCE W products, the modules have been completely innovated and all old devices are discontinued. The new devices cannot be used as spare parts for the old devices.

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

SCALANCE W748-1 RJ45 clients

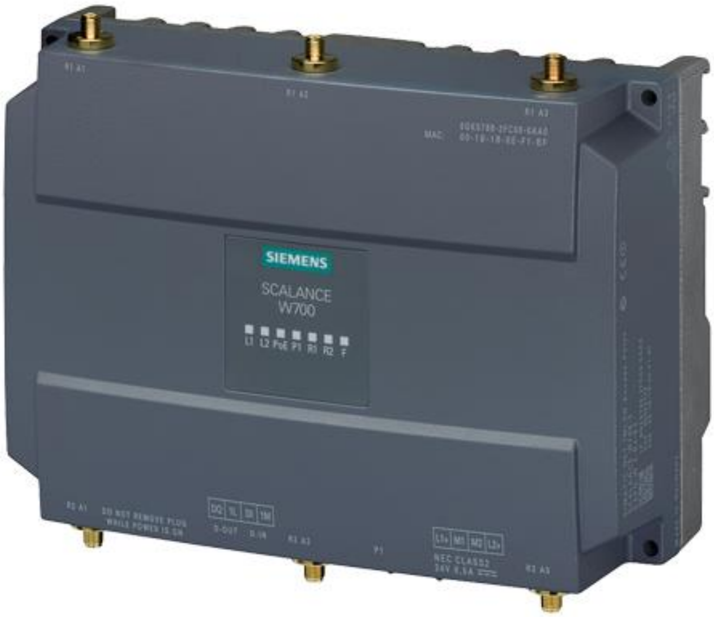
The SCALANCE W748-1 modules are built according to protection class IP30 and are, amongst other applications, very suitable for the control cabinet in industrial environments.

The Ethernet interface has been designed electrically (RJ45), is gigabit-capable and enables Power over Ethernet.

For the connection of three external antennae, R-SMA sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-9



The SCALANCE W748-1 RJ45 can be ordered in the following variants:

- MLFB: 6GK5748-1FC00-0AA0 or
- MLFB: 6GK5748-1FC00-0AB0 (US variant)

SCALANCE W748-1 M12 clients

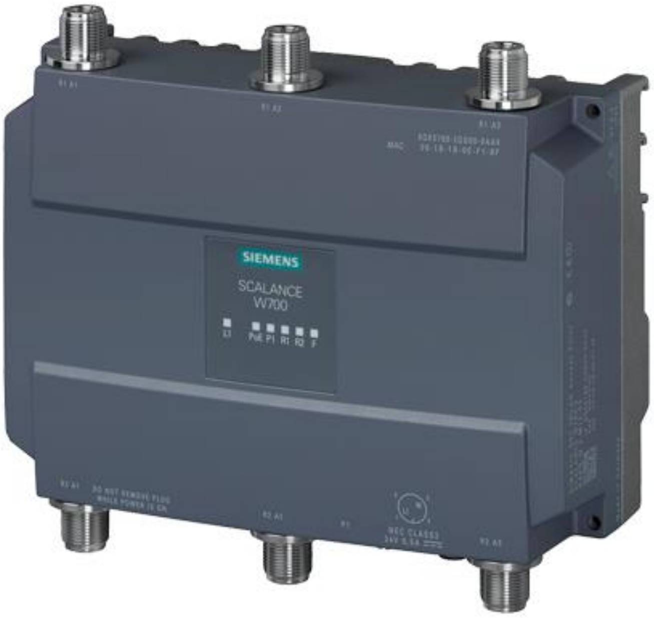
These clients have the IP65 protection class and are suitable for installation indoors in industrial environments.

The Ethernet interface has been designed electrically (M12), is gigabit-capable and enables Power over Ethernet.

For the connection of the three external antennae, robust N connect sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-10



The SCALANCE W748-1 M12 can be ordered in the following variants:

- MLFB: 6GK5748-1GD00-0AA0 or
- MLFB: 6GK5748-1GD00-0AB0 (US variant)

SCALANCE W734-1 RJ45 clients

The SCALANCE W734-1 RJ45 modules are built according to protection class IP30 and are, amongst other applications, very suitable for the use in control cabinet in industrial environments.

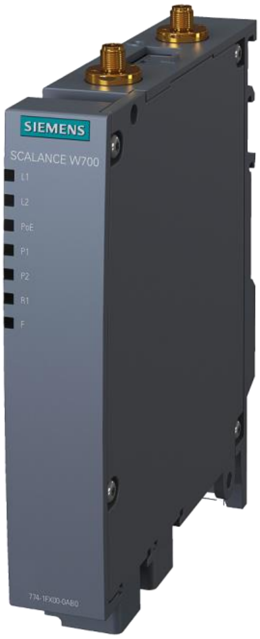
The well-balanced housing design makes them perfectly compatible with existing SIMATIC products.
(e.g. ET200SP ET200MP, ...).

The two Ethernet interfaces are electric (RJ45), one of which is suitable for the feed via Power over Ethernet.

For the connection of the two external antennae, R-SMA sockets are provided.

The module has a PLUG receptacle to insert a C PLUG or KEY PLUGs.

Figure 8-11



The SCALANCE W734-1 RJ45 can be ordered in the following variants:

- MLFB: 6GK5734-1FX00-0AA0 or
- MLFB: 6GK5734-1FX00-0AB0 (US variant)

SCALANCE W72x-1 RJ45 clients

The SCALANCE W72x-1 RJ45 is available in two versions:

- The basic version SCALANCE W721-1 RJ45
- The SCALANCE W722-1 RJ45 with support of iPCF and NAT.

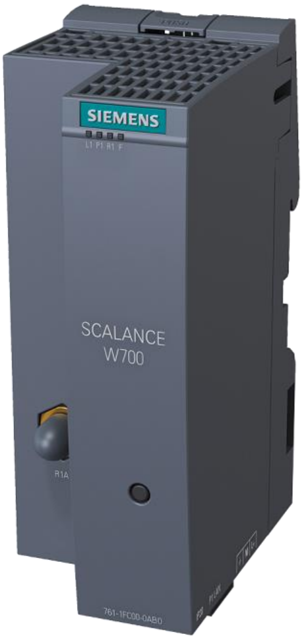
Both modules are built according to protection class IP20 and are, amongst other applications, very suitable for the control cabinet in industrial environments.

The SCALANCE W722-1 is furthermore suitable for wireless PROFINET IO communication through the support of iPCF.

The well-balanced housing design makes them perfectly compatible with existing SIMATIC products.
(e.g. ET200SP ET200MP, ...).

The Ethernet interface has been designed electrically (RJ45). For the connection of the external antenna, a R-SMA socket is provided.

Figure 8-12



The SCALANCE W72x-1 RJ45 can be ordered in the following variants:

- W721-1 RJ45 with basic function
  - MLFB: 6GK5721-1FC00-0AA0 or
  - MLFB: 6GK5721-1FC00-0AB0 (US variant)
- W722-1 RJ45 with additional iPCF and NAT function
  - MLFB: 6GK5722-1FC00-0AA0 or
  - MLFB: 6GK5722-1FC00-0AB0 (US variant)

8.6 Configuring the SCALANCE W devices

The SCALANCE W700 access points, client modules and controllers can be configured via “Web Based Management” (WBM) or Telnet via the command line (“Command Line Interface”, CLI).

For WBM the SCALANCE W configuration data is accessed via the Ethernet interface or an existing WLAN connection. A web browser on the PC of the configurator communicates with an HTTP server that runs on the SCALANCE W. With the aid of the HTTP server, the configuration data can be read and changed with forms as known from conventional websites.

A number of wizards are available in web-based management for user-friendly installation and configuration of both, access points and client modules. Using these wizards, the modules can be optimally adapted to the communication task. Both network mode and the required WLAN security level can easily be set.

Note

A number of configuration manuals are available in the Siemens Industry Online Support. A selection can be found at the following links:

- Configuration of the SCALANCE W780/ W740 via WBM: http://support.automation.siemens.com/WW/view/en/62516763
- Configuration of the SCALANCE W770/ W730 via WBM: https://support.industry.siemens.com/cs/en/en/view/109480849
- Configuration of the SCALANCE W760/ W720 via WBM: https://support.industry.siemens.com/cs/en/en/view/109480845
- Getting started for the IWLAN controller WLC711: https://support.industry.siemens.com/cs/document/62523066

8.7 SIMATIC Mobile Panels 277(F) IWLAN V2

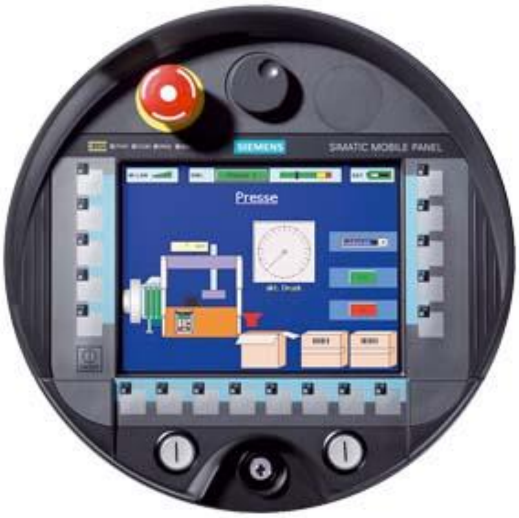
SIEMENS offers a wide range of HMI devices (“panels”) for automation, which can be used to monitor, surveil and operate complete plants or individual devices within the series. This also includes “mobile panels” with integrated radio interfaces which can be used in the course of an IWLAN. These panels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

They combine capabilities of an IWLAN client with the function scope of an HMI panel such as

- archive (storage of measured values and entries within temporal context),
- recipes (sets of associated process data that are managed “as an entity”)
- a highly-developed messaging, protocol and alarm system.

Operation is via touch screen, the configurable function buttons or via hand wheel, key switches and illuminated push-button. The SIMATIC mobile panels 277(F) IWLAN V2 have been constructed according to protection type IP 65 and communicate via the WLAN standard IEEE 802.11a/b/g/h via PROFINET.

Figure 8-13



Note Further information on this product is available in the SIEMENS Industry Mall at: http://www.automation.siemens.com/panels

Note An application example incl. safety can be found in _Siemens Industry Online Support at: http://support.automation.siemens.com/WW/view/en/25702331

9 Accessories for Wireless Networks (WLANs)

9.1 Optional storage media

A KEY PLUG or C PLUG (“Configuration Plug“) is a removable storage medium that is plugged into the respective hardware slot.
C and KEY-PLUG have a similar design but differ in function and color.

Figure 9-1

9.1.1 KEY PLUG

With the help of various KEY PLUGs, additional functions are made available in several industrial network components of Siemens AG.

In connection with the SCALANCE W7xx for IEEE 802.11a/g/n the iFeatures are enabled with the KEY PLUG W780 or W740 (see chapter 4.6):

- the KEY PLUG W780 iFeatures enables the iFeatures in the access point mode and in the client mode,
- the KEY PLUG W740 iFeatures only enables the iFeatures in client mode.
- the KEY PLUG W700 security switches on other security functions in the access point.

This means any SCALANCE W 11n standalone device can be expanded/upgraded with further functions without making a hardware exchange necessary.

In addition, the KEY PLUG has the same functions as the C PLUG.

9.1.2 C PLUG

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

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

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

http://support.automation.siemens.com/WW/view/en/29823212

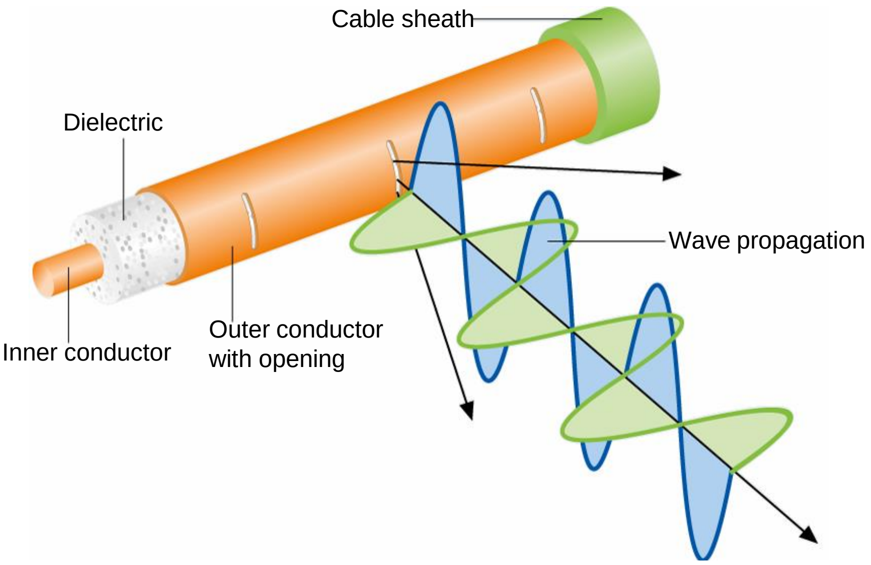
9.2 RCoax leaky wave cable

Description

The RCoax cables are leaky wave cables that act as special antennae for environments that are demanding from the point of view of radio technology, for SCALANCE W access points.

Leaky wave cables are coaxial transmission lines whose external shield is interrupted in a defined way. This constructive structure has the effect that a defined, cone-shaped radio field is formed along the RCoax line.

Figure 9-2



The RCoax cable

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

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

iPCF and PROFINET I/O

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

Note An application example for using RCoax cables in a PROFINET I/O environment is available in the Siemens Industry Online Support (entry ID 23488061): http://support.automation.siemens.com/WW/view/en/23488061

Data rate and segment length

Each SCALANCE W access point can be equipped with an RCoax cable. In order to generate longer, uninterrupted radio ranges, several leaky wave segments (with an assigned access point) can be arranged one after another.

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

Note Further information on this topic and performance data is available in the “RCoax System Manual” in Siemens Industry Online Support (entry ID 21286952): http://support.automation.siemens.com/WW/view/en/21286952

Connecting of mobile nodes

In a RCoax network the RCoax cable is fed by an access point. The RCoax cable acts as antenna to mobile partner stations (e.g. SCALANCE W clients), that move along the RCoax cable and which receive the information via their antenna from this cable or which couple into it.

The connection to the wireless RCoax network is performed via antennae that are to be installed by means of the flexible connection cable in the immediate vicinity of the RCoax cable.

Note Updated product information on RCoax cables is available on the web at: http://w3.siemens.com/mcms/industrial-communication/en/industrial-wireless-communication/iwlan-industrial-wireless-lan/Pages/radiating-cable-rcoax.aspx

9.3 Antennae

9.3.1 Overview of the WLAN antennae

For optimum radio field architecture, antennae are top priority, next to the selection of the devices. Decisive are particularly these points:

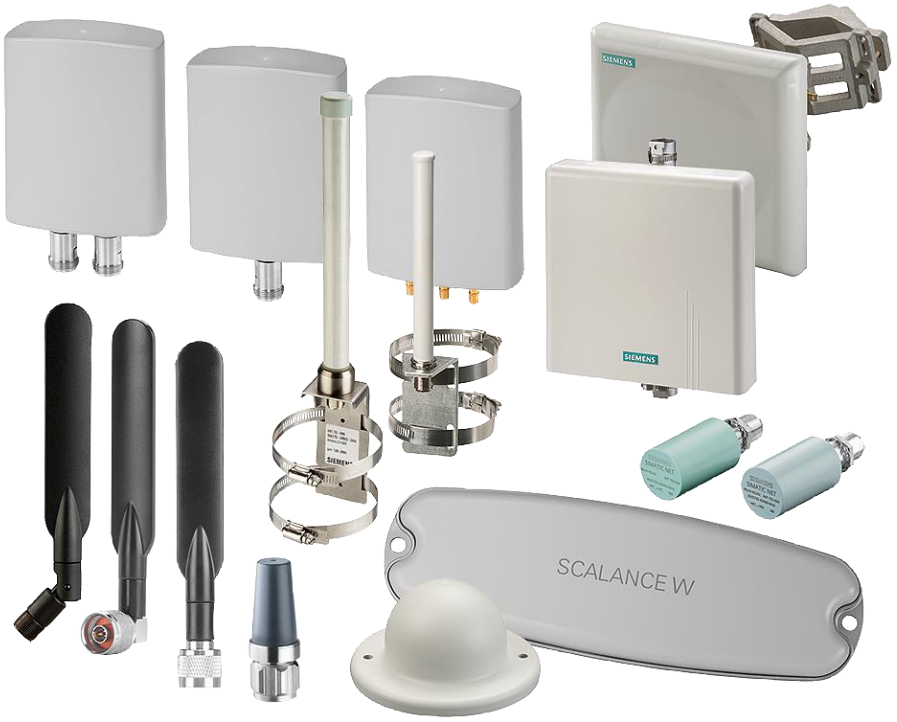
- Characteristic of the antenna (radio coverage)
- Place of application (indoors or outdoors)
- Required data rates

The SIMATIC portfolio has a number of omnidirectional antennae and directional antennae available (basic information on antennae, see also chapter 1.5). They can be either installed directly or separate from the device, e. g. at a mast or a wall, in order to achieve an optimum illumination of the space to be covered.

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

An overview of the WLAN antennae is displayed by the following figure:

Figure 9-3



The properties of the most important antenna types are listed in the following table:

Table 9-1

Type	Installation	Property	Antenna gain	SCALANCE W780/ W740	SCALANCE W770/ W730	SCALANCE W760/ W720
ANT795-4MC	Directly on the device	Omnidir.	2.4 GHz: 3.0 dB 5.0 GHz: 5.0 dB	x	-	-
ANT795-4MD				x	-	-
ANT795-4MA				x	x	x
ANT795-4MX			2.4 GHz: 2.0 dB 5.0 GHz: 2.5 dB	x	-	-
ANT792-6MN	Wall or mast		2.4 GHz: 6.0 dB	x	x	x
ANT793-6MN			5.0 GHz: 5.0 dB	x	x	x
ANT795-6MP			2.4 GHz: 5.0 dB 5.0 GHz: 7.0 dB	x	x	x
ANT795-6MN	Ceiling		2.4 GHz: 6.0 dB 5.0 GHz: 8.0 dB	x	x	x
ANT795-6MT			2.4 GHz: 4.0 dB 5.0 GHz: 6.0 dB	x	-	-
ANT795-6DC	Wall or mast	Directional	2.4 GHz: 9.0 dB 5.0 GHz: 9.0 dB	x	x	-
ANT793-6DG			5.0 GHz: 9.0 dB	x	x	-
ANT793-6DT			5.0 GHz: 8.0 dB	x	-	-
ANT792-8DN			2.4 GHz: 14.0 dB	x	-	-
ANT793-8DP			5.0 GHz: 13.5 dB	x	-	-
ANT793-8DJ			5.0 GHz: 18.0 dB	x	-	-
ANT793-8DK			5.0 GHz: 23.0 dB	x	-	-
ANT793-8DL			5.0 GHz: 14.0 dB	x	x	x
ANT793-4MN	RCoax	Omnidir.	5.0 GHz: 6.0 dB	x	x	x
ANT792-4DN		Directional	2.4 GHz: 4.0 dB	x	x	x

Note on name convention for IWLAN antennae

The most important functional characteristics are stored in a code in the name of the antennae 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: Omni (omnidirectional) / directional

Example: ANT792-8DN (2 GHz, high amplification, directional, N-Connect)

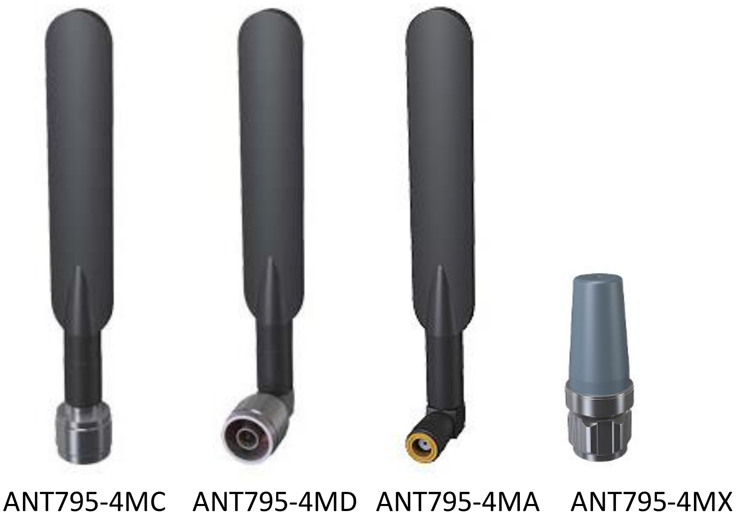
9.3.2 Antennae with omnidirectional characteristic

SIMATIC NET offers a well-balanced range of antennae with omnidirectional characteristics for various application cases for indoors as well as outdoors. The antennae differ in view of their place of installation, the connections, the protection class and the frequency range.

ANT795-4Mx antenna

The antennae of type ANT795-4Mx are suitable for installation directly on the access point or client.

Figure 9-4



The following table shows the variants:

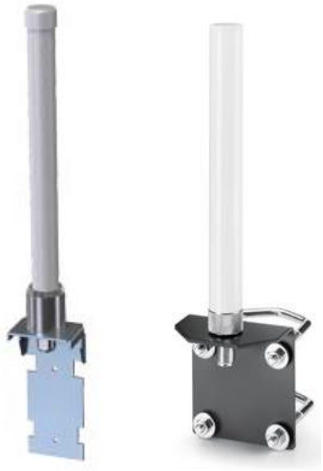
Table 9-2

ANTENNA	Connection	Class of protection	Remark
ANT795-4MC	1 x N-Connect male	IP65	even
ANT795-4MD	1 x N-Connect male	IP65	Window 90° angle
ANT795-4MA	1 x R-SMA male	IP30	With additional joint; pivotable at an angle of between 0° and 90°.
ANT795-4MX	1 x N-Connect male	IP68	even

Antenna ANT79x-6MN / ANT795-6MP

The antennae of type ANT79x-6Mx can be installed on a wall as well as on a mast.

Figure 9-5



ANT79x-6MN ANT795-6MP

The following table shows the variants:

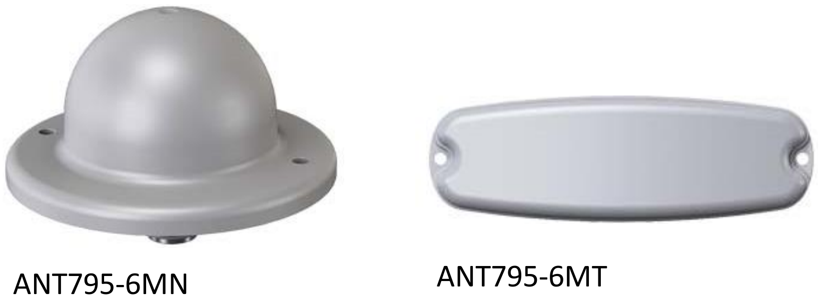
Table 9-3

ANTENNA	Connection	Class of protection	Remark
ANT792-6MN	1 x N-Connect female	IP65	.
ANT793-6MN	1 x N-Connect female	IP65	
ANT795-6MP	1 x N-Connect female	IP67	

ANT795-6Mx antenna

The installation of antennae of type ANT795-6Mx can be directly on a wall, ceiling or roof.

Figure 9-6



The following table shows the variants:

Table 9-4

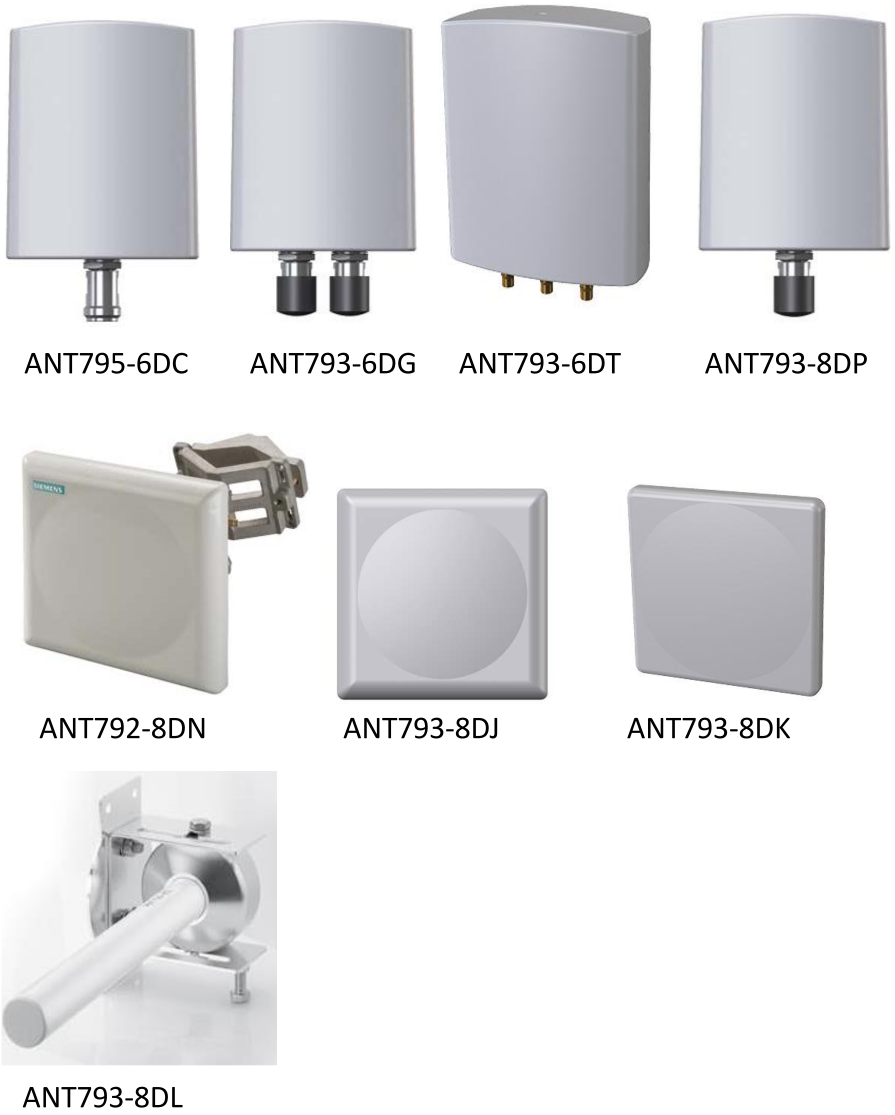
ANTENNA	Connection	Class of protection	Remark
ANT795-6MN	1 x N-Connect female	IP65	
ANT795-6MT	3 x QMA female	IP65	MIMO antenna;

9.3.3 Antennae with beamforming

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

The antennae of type ANT79x-xDx have been designed for wall or mast installation.

Figure 9-7



ANT795-6DC ANT793-6DG ANT793-6DT ANT793-8DP

ANT792-8DN ANT793-8DJ ANT793-8DK

ANT793-8DL

The following table shows the variants:

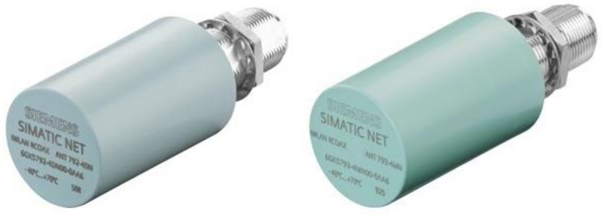
Table 9-5

ANTENNA	Connection	Class of protection	Remark
ANT795-6DC	1 x N-Connect female	IP67	
ANT793-6DG	2 x N-Connect female	IP67	Dual Slant
ANT793-6DT	3 x QMA female	IP67	MIMO antenna
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 Antennae for RCoax

When using an RCoax system, the portfolio offers two antennae that only differ regarding their frequency range.

Figure 9-8



ANT792-4DN ANT793-4MN

The following table shows the variants:

Table 9-6

ANTENNA	Connection	Class of protection	Remark
ANT793-4MN	1 x N-Connect female	IP66	
ANT792-4DN	1 x N-Connect female	IP65	

Note

Further product information regarding antennae can be found at the URL:

http://w3.siemens.com/mcms/industrial-communication/en/industrial-wireless-communication/iwlan-industrial-wireless-lan/Pages/accessories-antenna.aspx.

Further information on RCoax antennae is available in the “RCoax System Manual” in Siemens Industry Online Support (entry ID 21286952): http://support.automation.siemens.com/WW/view/en/21286952

9.4 Connections and cabling

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

The SCALANCE W access points and clients have N-connect or R-SMA connection, depending on the model. The antennae additionally have QMA connections. These applications are marked by high-class transmission, reliable connections and the application of cap nuts and a low form factor.

N-Connect connection

The N plug has been designed for all coaxial cable types. Due to a mechanical fixture it has a high robustness and is very well suited for outdoor use due 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 following table:

Table 9-7

Plug/socket variant	Characteristic
SMA plug	Internal thread and pin as inner contact
SMA socket	External thread and cup as inner contact
R-SMA plug	Internal thread and cup as inner contact
R-SMA socket	External thread and pin as inner contact

For SCALANCE W with connections of this size, the R-SMA variant is used.

QMA connection

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

9.5 Additional accessories

For a flexible combination and installation of the individual IWLAN components, indoors as well as outdoors, an extensive and well-balanced range of coaxial accessories is offered. It comprises antennae connection cables as well as diverse plug connectors, lightning protection elements, a power splitter and an attenuator.

Note

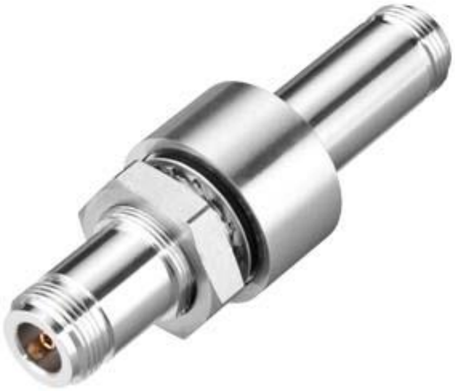
Several FAQs in Siemens Industry Online Support (entry ID:22167025) show what connection cables and additional devices can be used for the connection of an external antenna to the SCALANCE W:

http://support.automation.siemens.com/WW/view/en/22167025

Lightning protection element

The LP798-2N lightning protection element expands the applications of SCALANCE W700 products with remote antennae particularly for outdoors.

Figure 9-9



A lightening protection element secures the active device against destructive overvoltage (e.g. lighting) via the antennae connections. If an overvoltage event occurs, the respective currents are grounded.

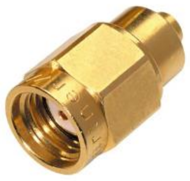
The lighting protection element should be installed and grounded as near as possible to the active device (e.g. the control cabinet wall). It is connected to the antenna and the active device via antennae connection cables.

Different variants of lightening protection elements are available.

Terminating resistor

The TI795-1R terminating resistor (see figure) or TI795-1N has to be used for each antenna connection that is not used for SCALANCE W700 products, in order to terminate them in terms of high-frequency.

Figure 9-10

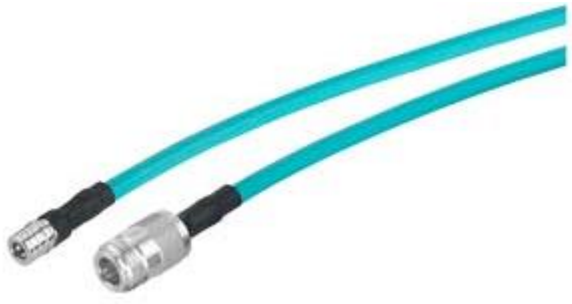


Flexible connection cables

The flexible IWLAN RCoax/antenna connection cables are required for the connection of RCoax segments or antennae with active devices. They can furthermore 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).

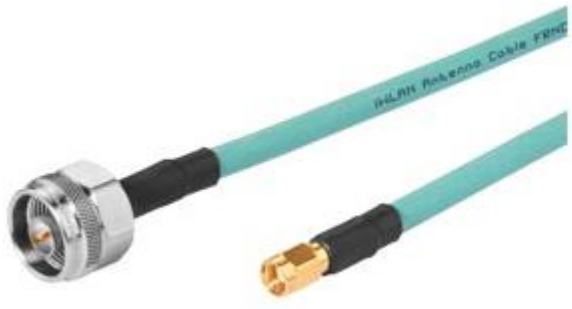
The following figure shows a QMA/N-Connect male/female connection cable:

Figure 9-11



The next figure shows a connection cable that is used between a SCALANCE W78x RJ45 and, for example, a remote antenna or a different component with N-Connect connection:

Figure 9-12



Note

Further information, as well as application examples can be found in the FAQ "Which connection cables and IWLAN devices can you use to connect an external antenna to the SCALANCE W?" (Entry ID 43895062)

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

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

Power Splitter

Figure 9-13

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

SITOP PS307 power supply

The SITOP PowerSupply is a high-quality DC voltage supply for the use in the industrial environment with protection type IP20. Special additional modules protect the power supply from disturbances on the side of the network as well as on the DC side and provide the required supply security.

Figure 9-14

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

Alternating voltage power supply with IP65

The SCALANCE W modules (IEEE 802.11 a/b/g) in protection type IP65 can be directly supplied with voltage supplied 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 9-15

The power supply unit itself has a robust metal housing with protection from water and dust in protection class IP65. Short-circuit strength, open-circuit safety and the bridging of short power network disturbances guarantee high operational safety.

Attenuator

The attenuator is always used when the transmitted power has to be reduced in sending and receiving direction. Typical fields of application are short RCoax segments or radio path where the extent is to be limited. The insertion loss of the attenuator is 10 dB.

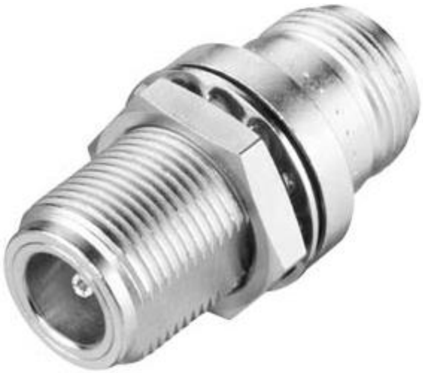
Figure 9-16

Control cabinet feed-throughs

The control cabinet feed-throughs together with the connection cables enable a simple connection of remotely installed antennae with the active components located in the control cabinet/box. The control cabinet feed-through is available in the following connection combinations:

- SMA-female / N-female for wall thickness up to max. 4.5 mm
- N-Connect female / N-Connect female for wall thickness of up to max. 4.5 mm

Figure 9-17



Note Further product information on passive network components can found in the “SIMATIC NET Industrial Wireless LAN Passive network components IWLAN System Manual” in the Siemens Industry Online Support (entry ID 67701823): http://support.automation.siemens.com/WW/view/en/67701823

9.6 TIA Selection Tool

General

The TIA Selection Tool selection and ordering aid, assists you in selecting industrial Ethernet switches and components for industrial wireless communication.

The tool is primarily used to simplify the ordering process and to assist the customer in selecting the products.

Description

The TIA selection tool is the successor of the SIMATIC selection tool and unites already known configurators for automation technology in one tool with clearly more products than the predecessor.

It offers several wizards to select the desired devices and networks. In addition, it provides configurators for selecting modules and accessories and checking the correction function.

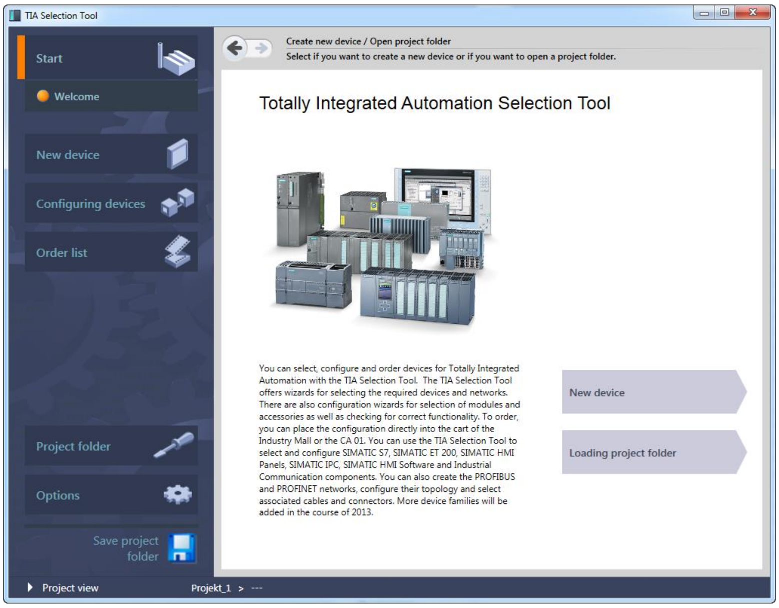
A complete order list can be generated from the product selection or the product configuration. You can export it directly into the shopping cart of the Industry Mall or to the CA 01.

User interface

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

The tool has a java-based, graphic interface. The individual selection options and products are displayed as tabs. It is possible to directly select the tab or to be guided step-by-step with the help of the tool.

Figure 9-18



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

Furthermore PROFIBUS and PROFINET networks can be generated, their topology can be configured and the appropriate cables and plugs can be selected.

Installation

The TIA selection tool can be started directly in Siemens Industry Mall or downloaded as file.

Note Further information can be found at URL: http://www.siemens.com/tia-selection-tool

10 IWLAN in Use

By using wireless data networks, process can be designed significantly more efficiently. The advantage of wireless solutions is mainly the simple and flexible reachability of mobile or difficult to reach participants.

Due to wireless communication to automation devices and industrial terminal devices, a higher flexibility is attained, maintenance work is simplified, service and downtimes are reduced and staff can be used most effectively.

Even demanding applications with real time and redundancy requirements in the industry can be realized with Industrial Wireless LAN (IWLAN).

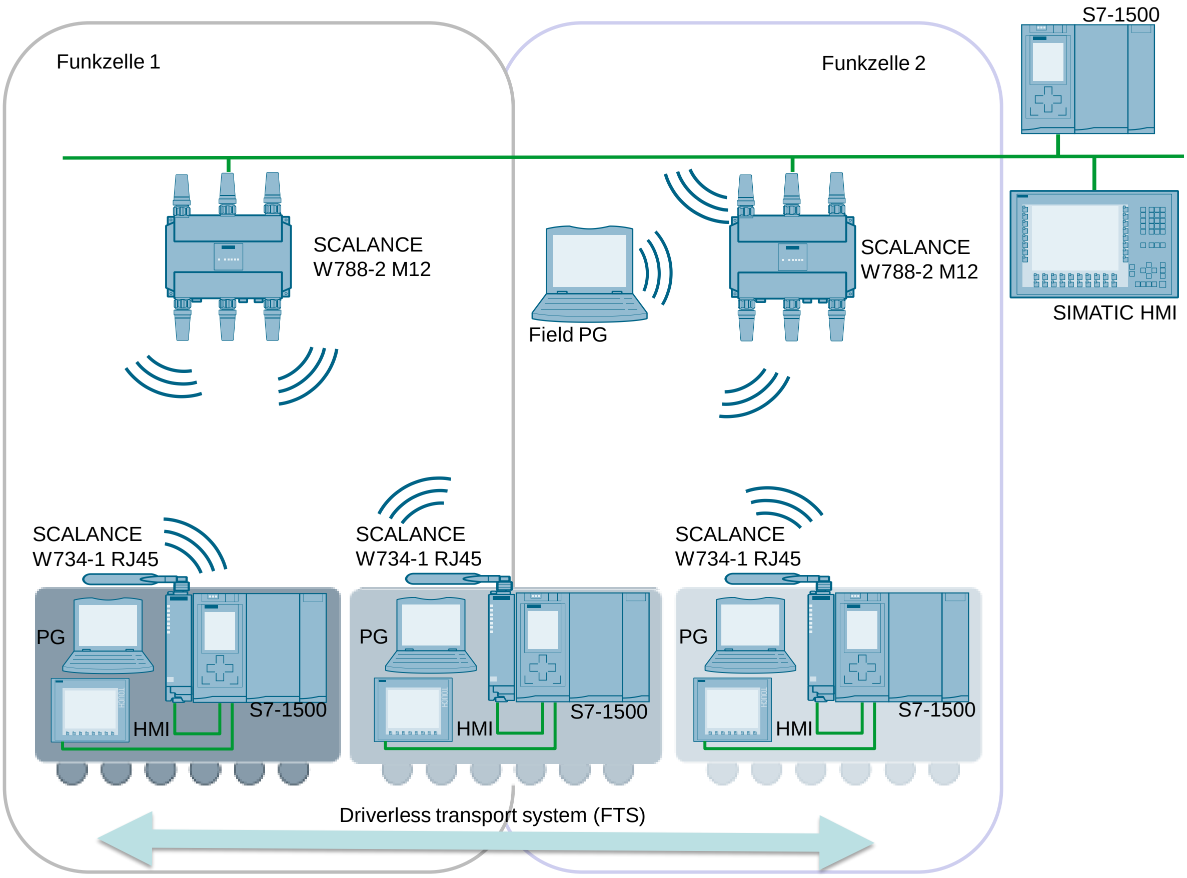
Based on selected places of application and application examples, the use of IWLAN is briefly demonstrated below.

Driverless transport system: Roaming of moving devices

The figure below shows an example from intralogistics, where individual W788-2 access points span several neighboring radio cells. Interconnected via a cable-based Ethernet string they mediate the communication between the driverless transport system on which a W734-1 client module and a mobile S7-1500 CPU are located, and a stationary S7-1500 CPU on one hand and an HMI panel on the other hand.

This configuration enables the driverless transport system to change from radio cell to radio cell (“roaming”) without losing contact.

Figure 10-1

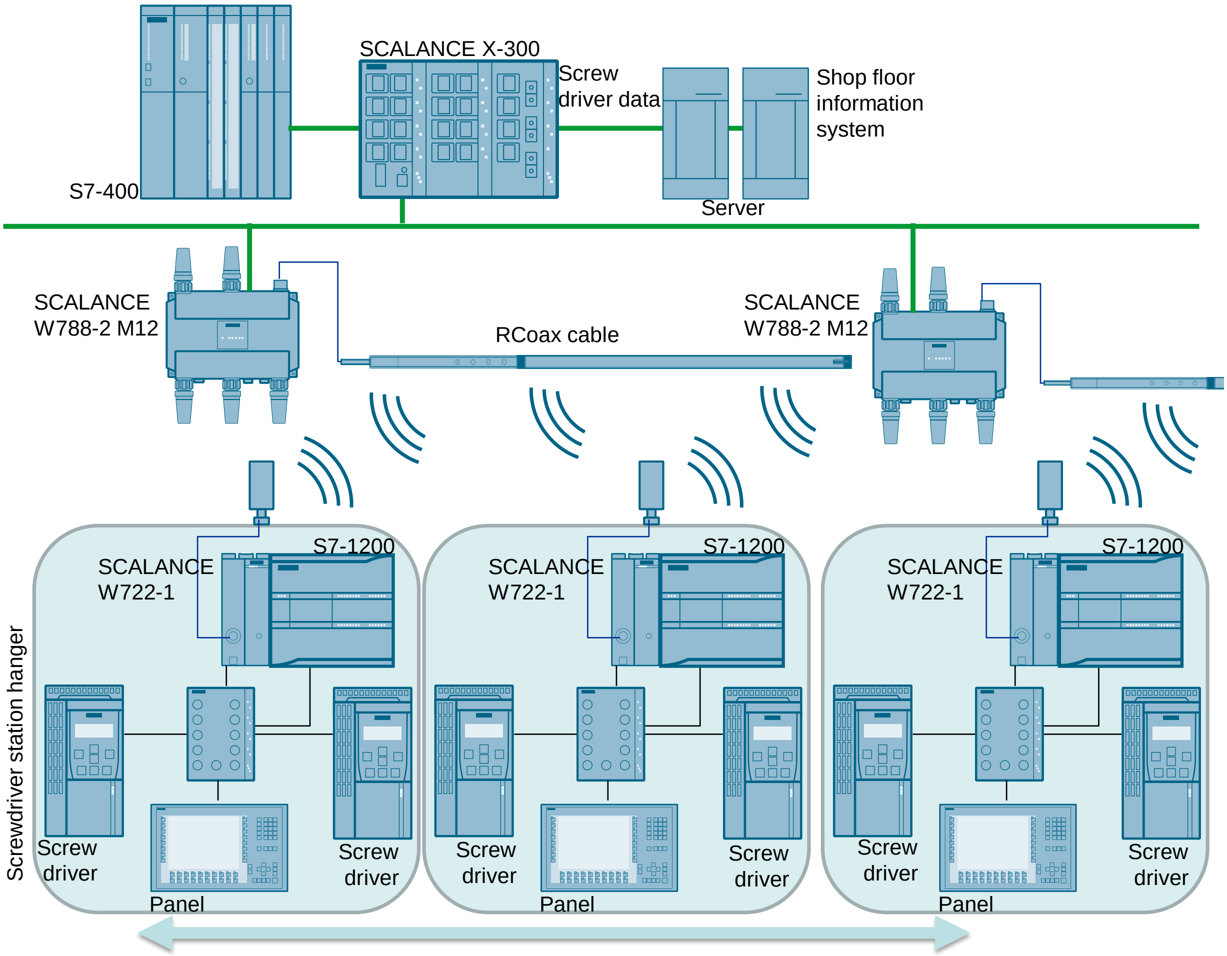


Overhead conveyor system: Using RCoax

In the example below from the automotive industry, the IWLAN RCoax leaky wave cable is used for setting 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 supplying station for the RCoax cable.

The mobile screwing stations - each equipped with one client module W748-1, a SIMATIC S7-1200, two screwdrivers and a panel – move along the path of the overhead conveyor system and can communicate with the cable-based network via their client module and the access point.

Figure 10-2



Controller-based WLAN: Using SCALANCE WLC711

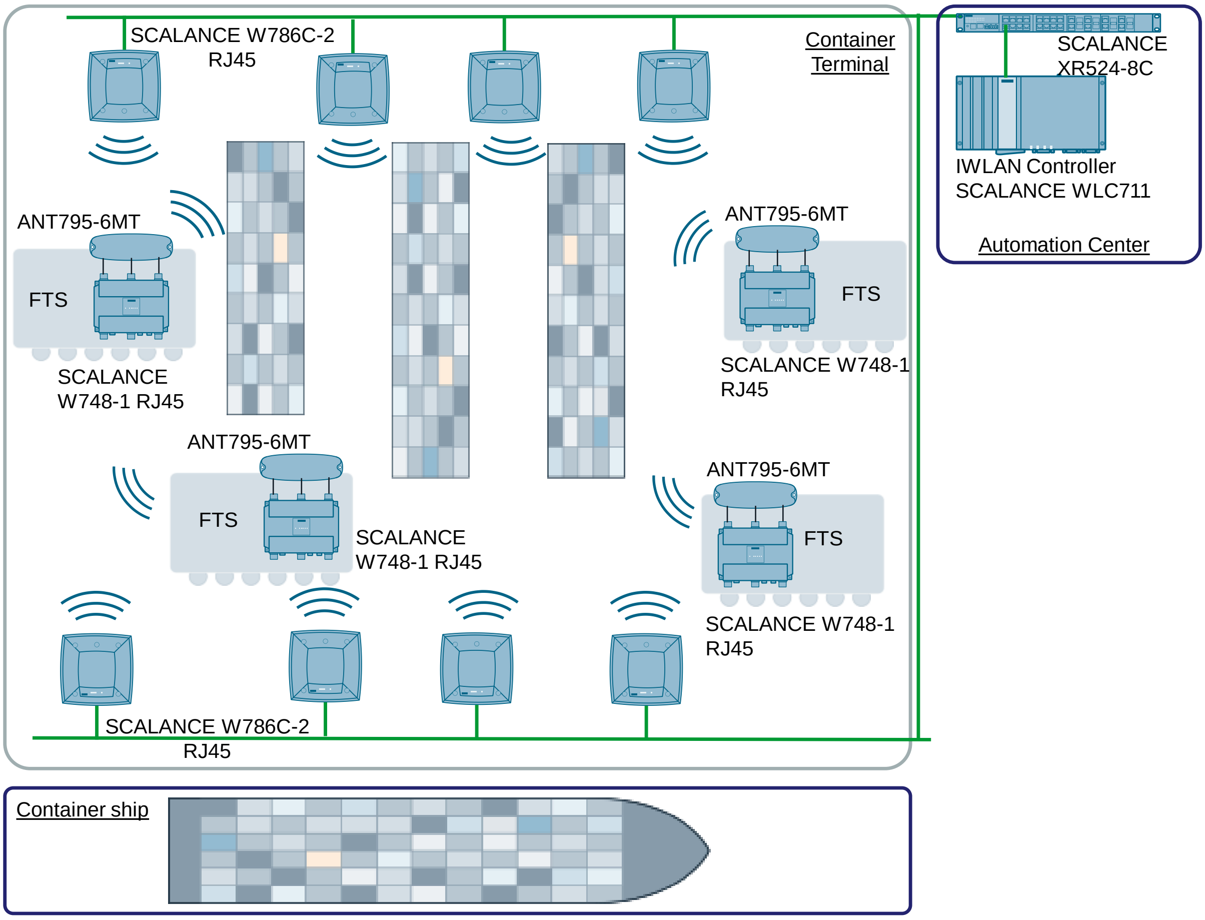
The use of controller-based WLANs is shown exemplary on a container loading and unloading plant. For an efficient transfer of the container, driverless transport systems are used which can freely move on the large area of the terminal.

Since driverless transport systems are moving outdoors, it is important that a robust connection that is suitable for outdoors is established so that the position data and drive commands can be safely and reliably transmitted.

A suitable solution can be established with different products of the SCALANCE W portfolio. The driverless transport systems are equipped with W748-1 RJ45 client modules. The communication between the driverless transport system is then controlled by the controller-based SCALANCE W786-2C access points.

By using the SCALANCE WLC 711 the W786-2C access points can be centrally configured and operated. The controller furthermore supplies additional features in order to yet again increase the quality of the solution. This is how, for example, an even distribution of the clients on the individual access points can be achieved via load balancing.

Figure 10-3



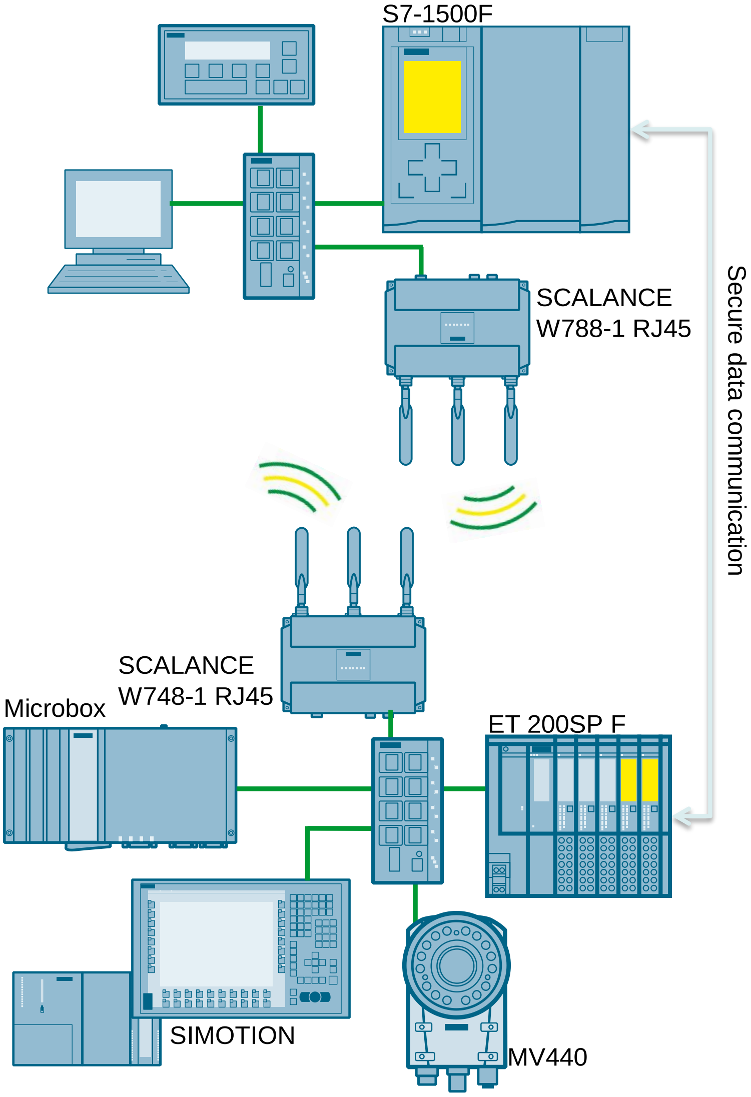
Safety over Wireless: PROFIsafe with SCALANCE W

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

In the example below, the safety-related operation of a robot is demonstrated.

Since PROFIsafe is a protocol extension, mixed traffic of “secure” and standard messages can take place on the same network.

Figure 10-4



11 Glossary

802.11

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

Access Point

“Access point”, a node of a → WLAN which simultaneously performs administrative functions in the network and which e.g. provides the connection to wire-bound networks to → clients, other clients in the same radio cell or in other radio cells. See Chapter 4.1.2

***Ad hoc* network**

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

AES

“Advanced Encryption Standard”, an encryption method, see chapter Chapter 5.2.2.

Antenna pattern

A graphic display of the antenna's radiation pattern, to be able to estimate its performance. The values for the antenna pattern are measured and recorded or generated through simulation programs.

Antenna Diversity

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

Antenna gain

The concentration of the radio field of an antenna in a limited spatial direction is achieved through suitable design. This achieves a (passive!) amplification in this direction in space in comparison to an isotropic radiator. Other directions are weakened in turn. The form of the radio field is specified in more detail in the → antenna pattern

Bandwidth

Can be described as “maximum available data rate”. The term derives from the fact that a proportionally wide section of the radio spectrum is used by the transmission at a specific data rate. See also chapter 1.4.4.

Bluetooth

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

CCMP

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

Client

In this case: a node of a → WLAN which has no internal infrastructure capabilities but which accesses a radio network via an → access point.

CSMA/CA

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

DCF

“Distributed Coordination Function”, an organization model for radio networks (see chapter 4.4.1).

DFS

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

DoS

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

DSSS

“Direct Sequence Spread Spectrum“, a spread spectrum communication method for IEEE 802.11b.

EAP

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

GFSK

“Gaussian Phase Shift Keying“, a modulation method for IEEE 802.11.

GPRS

“General Packet Radio Service”, a data transmission service used for cellular phone communication.

Handover

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

Hidden node problem

Similar to → hidden station problem

Hidden station problem

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

HMI

“Human/Machine Interface”, display and operating devices for plant control, such as, for example, SIMATIC mobile panels

IEEE

“Institute of Electrical and Electronics Engineers” (read I-Triple-E), a US association which among other things develops guidelines and technical recommendations; in the broader sense comparable to DIN (German Standards Institution).

.

Infrastructure mode

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

IP 30

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

IP 65

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

iPCF

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

iQoS

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

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”, locally defined network, in contrast to, for example, the internet

Leaky wave cable

A coaxial cable whose outer shield is interrupted at defined points. As a consequence, the cable generates a spatially limited radio field that can be “formed” since it follows the cable bend.

Link Check

An access point functionality for monitoring the connection to the clients. Different events (logging on, logging off of the clients, etc.) can cause automated reactions of the access point (sending mails/traps, switching on *Fault* LED, etc.). All SCALANCE W access points support link check.

MAC

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

MAC address

A globally unique identification number for each hardware component of importance in a network. → MAC

Middleware

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

MIMO

"Multiple Inputs, Multiple Outputs", a method where each radio node sends and receives simultaneously with several antennae. 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 connection system for IWLAN antennae.

OFDM

“Orthogonal Frequency Division Multiplex”, a modulation method for IEEE 802.11a and g.

PCF

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

PoE

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

Polling

Regular polling of status data or variables from a data source (“server”) by a client. (This client is not necessarily the client of a WLAN.) The alternative to this is event-controlled transmission. Here, the server independently transmits data to the client as soon as there are any changes in the data.

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 to meet the “Industrial Ethernet” requirements, i.e. the use in an industrial environment. New properties are the measures to increase the transmission security and fault tolerance and the use of sturdy components, etc. The SCALANCE product generation is designed for use with PROFINET.

PROFIsafe

A protocol extension for → PROFIBUS and → PROFINET with which the transmission security and reliability is considerably increased.

PSK

“Pre-Shared Key”, a method for authentication within the framework of the → WPA/WPA2 protocols.

Quality of Service

Transmission quality guaranteed in the framework of a network.

RADIUS

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

Rapid spanning tree

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

RC4

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

RCoax

A → leaky wave cable used for setting up realtime-capable radio networks with limited range, particularly suitable for → clients with fixed motion paths (e.g. automated guided vehicle systems) or in heavily shaded 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 the request of a sender (e.g. read device at the borrowing section of the library) with an ID to track them. The transponders are small, cheap and are fed by the energy of the reading device. Range and data capacity, however, are low.

Roaming

The motion of a → WLAN node from one radio cell to the next.

R/SMA

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

RSTP

"Rapid Spanning Tree Protocol", an algorithm used by switches in a network to automatically determine the optimal travel to the data transmission between two end nodes, and also to determine alternatives in the event of a failed transmission point. See chapter 4.5.3.

RTS / CTS

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

Spanning Tree

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

Spoofing

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

SSID

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

SSL

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

TKIP

"Temporary Key Integrity Protocol", a method for the dynamic change of the keys in a → WLAN.

TPC

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

UMTS

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

VLAN

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

VNS

“Virtual Network Services”, the organization of logical networks within one or several 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 within a larger network is “tunneled”, e.g. invisible for the other nodes. This property makes VPNs suitable for increasing the security of a network.

WAN

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

WBM

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

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

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

Wireless HART

(“Highway Addressable Remote Transducer”), the wireless variant of a field bus standard.

WLAN

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

WMM

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

WPA, WPA2

“WiFi Protected Access”, two encryption methods in wireless data communication.

Zigbee

A radio standard similar to → WirelessHART, however, it is used for operation in home or facility automation.

Enabling button

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

12 Links & Literature

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

Table 12-1

	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Download page of this entry https://support.industry.siemens.com/cs/ww/en/view/22681042
\3\	

13 History

Table 13-1

Version	Date	Modifications
V1.0	01.04.2006	First version
V2.0	01.01.2010	Various updates
V2.1	08.02.2011	Various updates
V3.0	04/2013	Complete revision of the structure and extension with new functions / devices for IEEE 802.11n
V4.0	01/2016	Including new WLAN components, removing old hardware; actualizing pictures