

Aims

This white paper presents an overview of the various technologies involved in Wireless LAN for industrial use complying with IEEE 802.11. It describes both the industrial enhancements (I-Features) and the current and future standards of the IEEE. Please note that standards that have already been approved and published are not described in this document. Information on such standards is available under the following links:

http://de.wikipedia.org/wiki/Wireless_LAN

<http://www.wi-fiplanet.com>

Further information on the topic of Industrial Wireless LAN in SIMATIC NET:

- Basics of Industrial Wireless LAN:
<http://support.automation.siemens.com/WW/view/en/9975764>
- Setup of a Wireless LAN in the Industrial Environment:
<http://support.automation.siemens.com/WW/view/en/22681042>

The previous white paper

http://intranet.automation.siemens.com/net/html_00/ftp/whitepaper/ie_wireless.pdf

will be updated with the latest information with publication of this document.

The information in this White Paper is as of Summer 2006



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

Published by
Siemens AG
Automation and Drives Group
SIMATIC NET Industrial Communication Subdivision
P.O. Box 4848
90327 Nuernberg, Germany

Further Support:

If you have any further questions, please contact your local Siemens representative.

You will also find SIMATIC NET on the Internet at



<http://www.siemens.com/simatic-net>

Introduction	4
Industrial Wireless LAN (IWLAN)	5
Rapid Roaming (RR)/ Industrial Point Coordination Function (iPCF).....	5
Industrial Quality of Service (iQoS)	8
Current Wireless LAN Standards.....	11
802.11i, Data Security	11
802.11h, Increased Transmit Power at 5 GHz for Europe	13
802.11e, Prioritization of Data (QoS)	16
Future Wireless LAN Standards	18
802.11n, High Data Rates	18
802.11s, Meshed Wireless LANs.....	20
Glossary.....	23

Introduction

Wireless LAN complying with 802.11 provides a good basis for use in wireless applications for industry and automation whether with driverless transport systems, escalators, storage logistics, transportation of goods, electric monorails, building management or service applications. Such systems can be considered when cabling would be extremely complex and time-consuming, when a high degree of flexibility is called for and/or when the environment is highly contaminated. This can significantly reduce the effort required for maintenance. Since Wireless LAN is the basis, such applications benefit from the wide range of chipsets, end devices and development tools available. All advantages that are provided by an open standard.

Industrial Wireless LAN (IWLAN)

Industrial Wireless LAN is a generic term covering functions and mechanisms that represent an enhancement of the IEEE 802.11 standard. Even the standard mechanisms of 802.11 provide a good degree of ruggedness for use in industrial applications. IWLAN, however, also supports demanding applications that provide a particularly high degree of real time and deterministics such as required in PROFINET.

It should be noted that these enhancements and features are also used outside automation. When using fast vehicles (for example, trains, urban railway systems), rapid roaming from one access point to the next is desirable even though PROFINET is not be used.

Rapid Roaming (RR)/ Industrial Point Coordination Function (iPCF)



With the implementation of the Industrial Point Coordination Function (iPCF), it is also possible to transfer deterministic data even with wireless LAN. iPCF is based on PCF familiar from 802.11 and also allows rapid roaming of clients from one access point to the next. One important application of iPCF is the support of PROFINET IO over wireless LAN. Here, constant, cyclic data exchange must be guaranteed. In practice, wireless PROFINET IO with the aid of iPCF is used, for example to control driverless conveyor vehicles. A fixed number of IO devices is connected by PROFINET to the central PLC controller (programmable controller). The connection is implemented in terms of hardware with Industrial Ethernet and Industrial Wireless LAN. To ensure that the PLC has access to the I/Os at any time, a defined response by the conveyor vehicles to the PLC is necessary. The wireless transmission over IWLAN must not represent a bottleneck. With iPCF, this is achieved by adept control of the access point, among other things to achieve short update times. In iPCF mode, each station also has an opportunity for cyclic communication. To achieve the required update time for all stations in the cell, suitable configuration limits must be planned.

Figure 1 shows the configuration of iPCF and the setting for the update time over the Web interface of a SCALANCE W788-1RR.

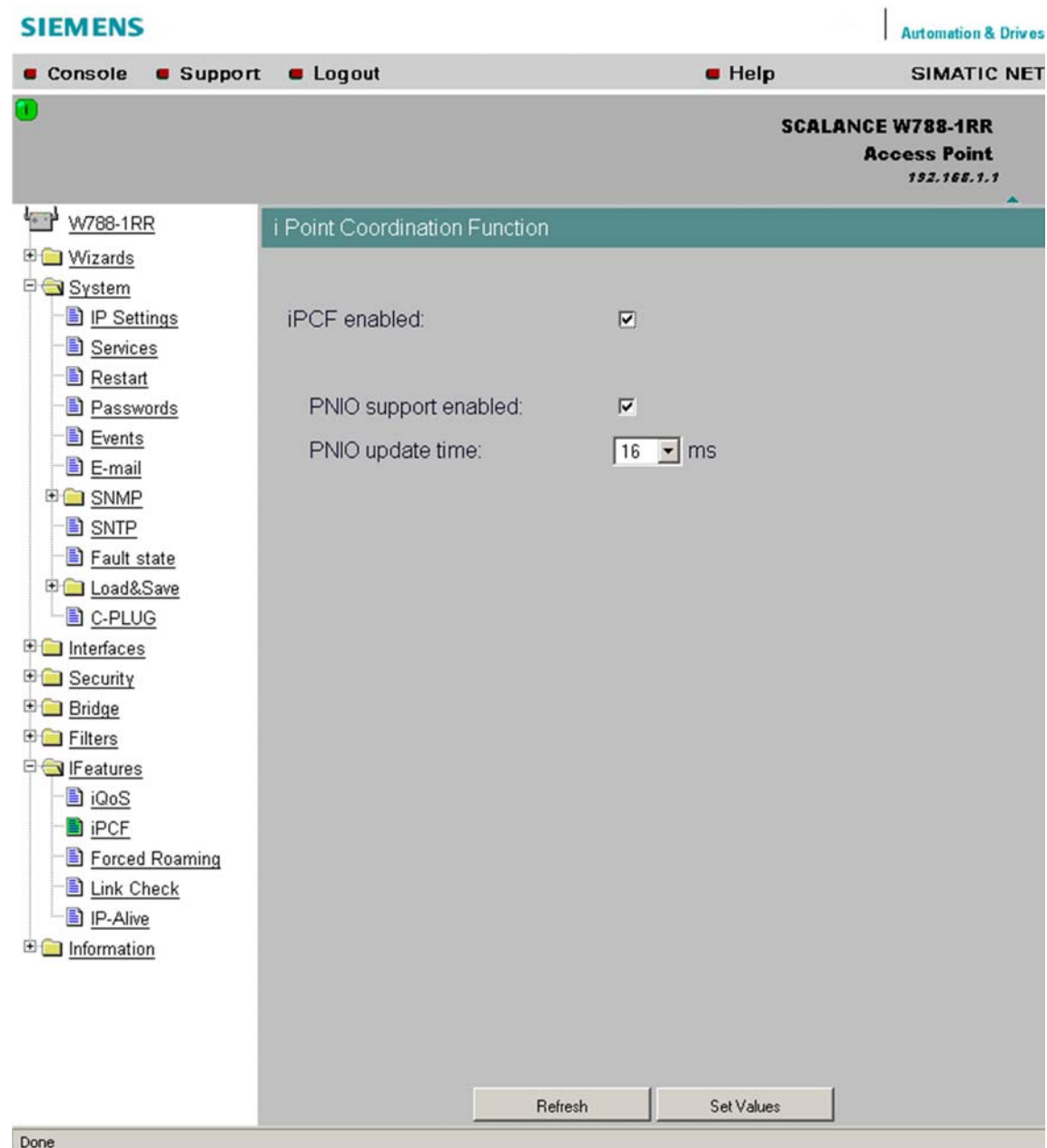


Figure 1: Configuration of iPCF over the Web Interface

Various configurations for IWLAN/iPCF and the corresponding update time for PROFINET IO were measured successfully in a series of tests. The minimum update time of the distributed I/O was calculated. The structure of the tested combinations and the results can be seen on the Internet using the following links. (Interactive tool)

<http://support.automation.siemens.com/WW/view/en/21869080>

and

<http://support.automation.siemens.com/WW/view/en/21869196>

Figure 2 shows an example of connecting the distributed I/O to a SIMATIC CPU with IWLAN. A Scalance W788-1RR access point connected to the SIMATIC CPU over PROFINET services the cell. On the client side, a total of 16 IWLAN/PB Link PNIO modules are used. Downstream from each IWLAN/PB Link there is a distributed I/O ET 200 M with 16 I/O bytes supplied with PROFIBUS. The cycle time (load caused by the program) is specified as 50 ms. This results in a typical reaction time of approximately 140 ms at an update time of 32 ms.

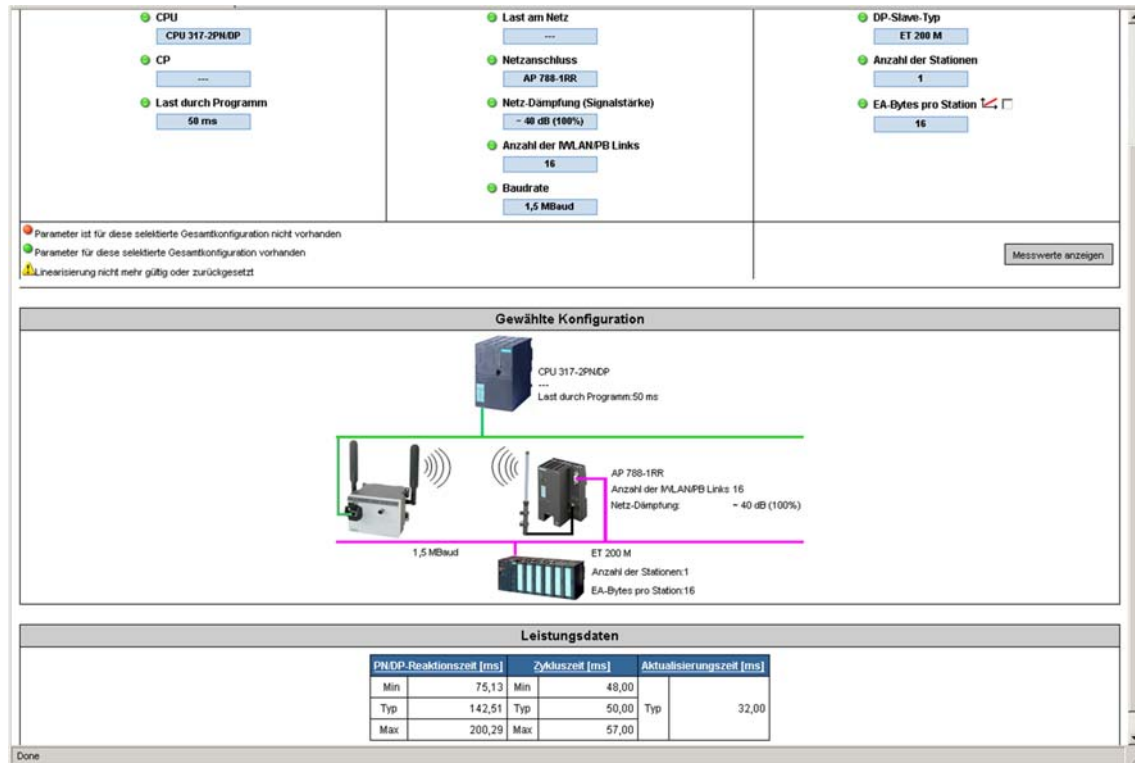


Figure 2: Test Results for a Measurement Setup with Distributed I/O on a SIMATIC CPU over IWLAN with iPCF

The update time describes the period between two of the regular data transfers from/to the distributed I/O. iPCF allows a minimum update time to be kept to so that IWLAN can function as a reliable data channel.

For iPCF to work, this function must be supported and activated on all devices participating in the Wireless LAN both on the access point and on the client modules.

The following IWLAN devices from Siemens support iPCF:

- SCALANCE W788-1RR
- SCALANCE W788-2RR
- SCALANCE W747-1RR
- IWLAN PB/Link PN IO

Industrial Quality of Service (iQoS)



For many use cases in which iPCF would not at first sight appear useful, for example in the case of a heterogeneous wireless LAN network, it is often desirable to assign a fixed data rate for certain devices. In a factory, for example, an engineer wants to transfer a new control program to the CPU of the PLC using a field PG over wireless LAN. At the same time, however, this controller must remain in contact with the individual crane cabins installed in the factory over the same wireless LAN. For safety reasons, there must be a constant exchange of information between the PLC and the cabins. The situation calls for the use of iQoS with which a defined net data rate is reserved for communication between the CPU of the PLC and the distributed I/O in the crane cabins. If there are bottlenecks in the wireless LAN (the shared medium), the engineer will have to show a little patience and the control of the cranes can continue undisturbed. One of the great advantages of iQoS is that a data rate can be assigned to any wireless LAN client module that is compatible with 802.11. The technology is incorporated solely in the access point that supports iQoS and is not dependent on the client modules.

With iQoS, the access point reserves the set data rate within a certain period for the iQoS stations and then releases the medium for general data exchange.

This procedure is illustrated schematically in

Figure 3. Clients 1, 2 and 3 are allowed an equal transmission time in each period, clients 5 and 6 are allocated the remaining time with transmission governed by the Carrier Sense Multiple Access with Collision Avoidance method (CSMA/CA).

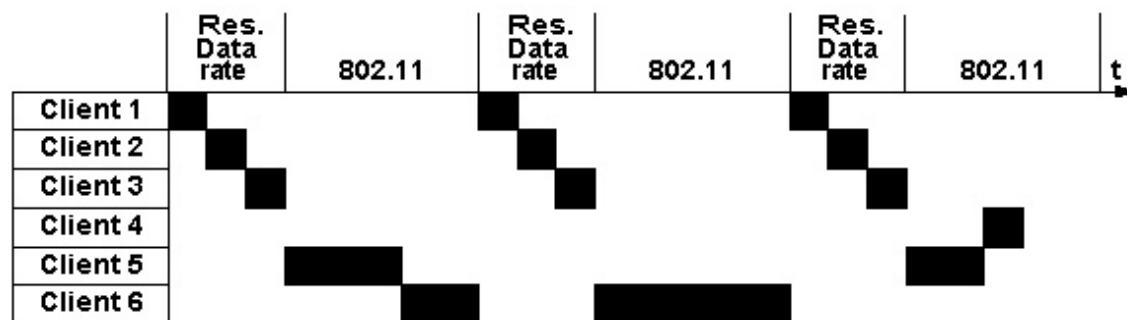


Figure 3: Schematic Representation of iQoS: Reserving the data rate for clients 1, 2 and 3. Clients 5 and 6 share the remaining time

To allow undisrupted iQoS operation, it is advisable to use a maximum of four wireless LAN devices with the appropriate reservation. It must also be remembered that iQoS and iPCF are mutually exclusive; in other words, iQoS is not possible in iPCF mode and vice versa. This results in the reserved data rate not being kept to while a client roams to a different access point. (Typical roaming time of 200-300 ms)

With SCALANCE W devices, the data rate is reserved simply using the Web interface integrated in the access point. The MAC address of the preferred station and the required data rate are entered. The required response time is also entered. This is the time by which an iQoS station must react to the query from the access point before there is a timeout and the next

SIMATIC NET White Paper V.1.0
Industrial Wireless LAN – Industrial Features and Current Standards, Summer 2006

station has its turn. Figure 4 shows an example of a configuration of two reserved stations with 128 Kbps and 64 Kbps and a response time of 50 ms.

The screenshot displays the SIMATIC NET web interface for a SCALANCE W788-1RR Access Point. The interface is titled 'SIMATIC NET' and includes navigation options like 'Console', 'Support', 'Logout', and 'Help'. The main configuration area is titled 'i Quality of Service for Wireless (Bandwidth Reservation)' and shows a table with two reserved stations. The 'Response time' is set to 50 ms.

Del	Sel	MAC address	Bandwidth	Status	Accepted
<input type="checkbox"/>	<input checked="" type="checkbox"/>	00-01-02-03-04-FF	128	-	x
<input type="checkbox"/>	<input checked="" type="checkbox"/>	AA-AB-AC-AD-AE-AF	64	-	x

Response time: ms

Figure 4: Configuration of iQoS on the Web Interface

The study made by ComConsult

http://intranet.automation.siemens.com/net/html_00/ftp/produkte/ComConsult_Siemens_IWL_AN_2004_07.pdf

and

http://intranet.automation.siemens.com/net/html_00/ftp/produkte/ComConsult_Siemens_iWL_AN-RR_2005-11.pdf

investigates the topic of iQoS in depth and confirms its effectiveness in tests.

The following IWLAN access points from Siemens support iQoS:

Access points:

- SCALANCE-W788-1PRO
- SCALANCE W788-2PRO
- SCALANCE-W788-1RR
- SCALANCE W788-2RR

Clients:

- SCALANCE W744-1PRO
- SCALANCE W746-1PRO
- SCALANCE W747-1RR
- IWLAN PB/Link PN IO
- CP 7515
- All IEEE 802.11-compliant clients

Current Wireless LAN Standards

The following IEEE-defined standards have been adopted. Due to their significance for industrial application, they are discussed in some detail here.

802.11i, Data Security

In industrial wireless LAN applications, operational safety is an important issue. This is achieved by the reliability of the devices and planning of the RF field. To prevent operational safety being endangered by unwanted external influences, data security plays an important role. This must not be confused with operational safety and ensures uncorrupted data exchange and protection from unauthorized access. The 802.11i standard describes a modern form of data security for wireless LANs.

Originally the 802.11 wireless LAN standard of 1999 was intended to supplement a standard known as Wired Equivalent Security (WEP) that would only permit selected clients access to a wireless LAN. Due to errors in the basic concept, only two years later it was possible to crack the key in WEP-protected networks. This could, however, be prevented relatively well by continuous automatic key changes. 2003 saw the arrival of Wi-Fi Protected Access (WPA) and two years later WPA2/802.11i - secure successor standards. Recently, researchers at University College in London discovered further flaws in the old WEP standard that rendered frequent automatic key changes practically useless because the WEP-encrypted communication could be cracked within a few seconds. This means that it is time to replace this standard in security risk environments with more robust mechanisms. If it is not possible to use a more modern security concept, WEP will at least prevent inexperienced outsiders from penetrating the network. From a cryptographic perspective, however, it hardly represents a serious obstacle to intruders. A little experience and a few simple programs are all that is needed to launch an attack.

For this reason, 802.11i/WPA2 should normally be used. There are two basic approaches to activating encryption. For straightforward wireless LAN environments, a pre shared key (PSK) is used. This secret, user-definable key is selected (must be of minimum length, should have special characters, should have no words from a dictionary etc.) and entered on every station on the wireless LAN (as shown in Figure 5 over the Web interface). In this case, the PSK is called "Pass phrase".

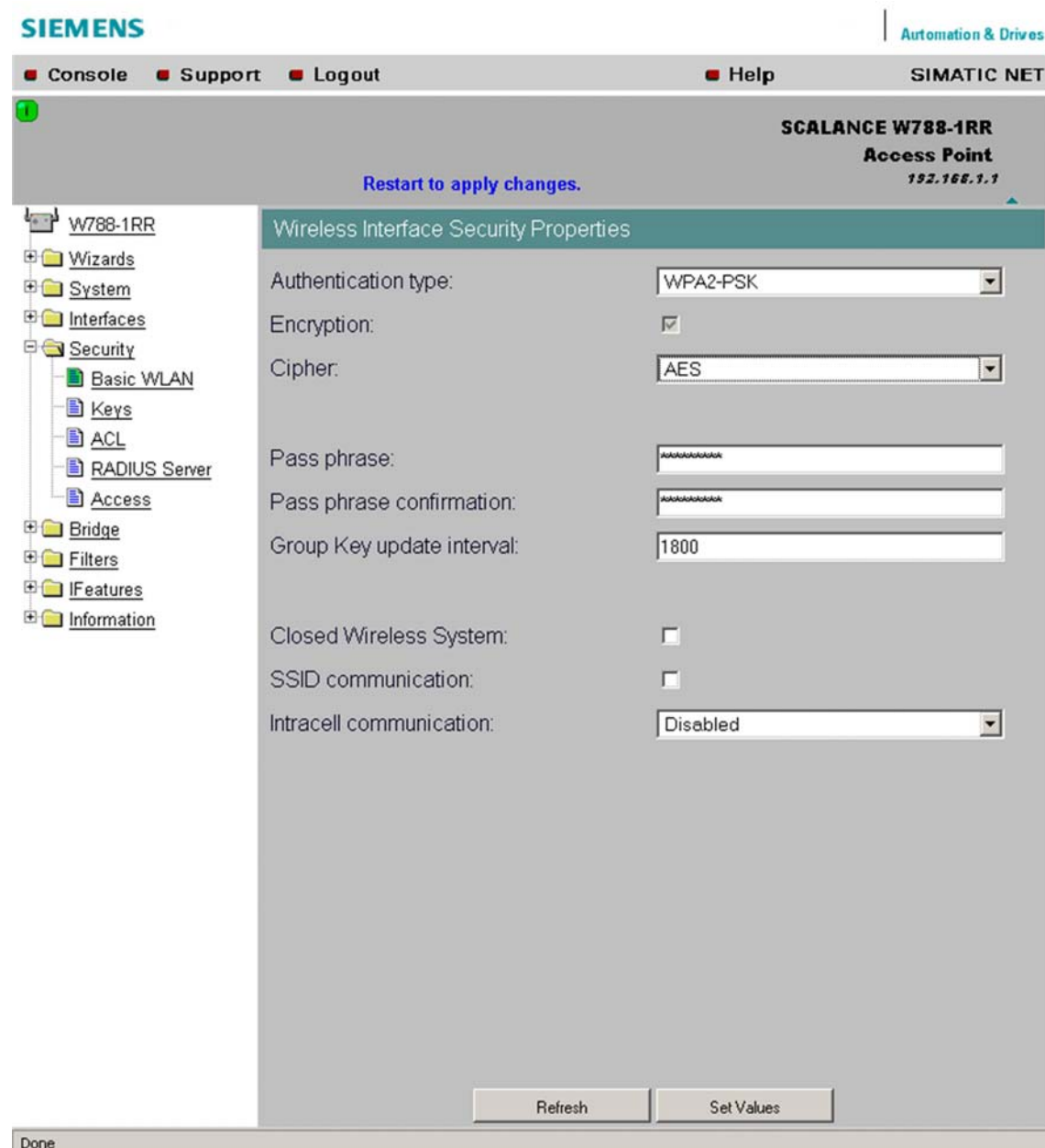


Figure 5: Configuration of the Pre Shared Key for WPA2/802.11i Encryption

The second approach is intended for large centrally administered enterprise networks and provides key management with a RADIUS server. This RADIUS server is made known to all participating stations and handles automatic key distribution and access control (authentication). The procedures were specified by the IEEE with the 802.1x standard and at the time of writing along with WPA2/802.11i this represents the highest degree of security for wireless LANs. One disadvantage is, however, the extreme complexity of such an infrastructure. The effort can only be justified in large plants or when the security demands are particularly high. This scenario is illustrated schematically in Figure 6. A wireless LAN client wants to access the secure network. It first requests access to the access point and must then authenticate itself with the RADIUS server over the access point. If this is successful and

if the station is known on the RADIUS server, the access point enables the client and communication with other wireless LAN stations or other downstream LAN resources is possible.

802.1x Authentifizierung

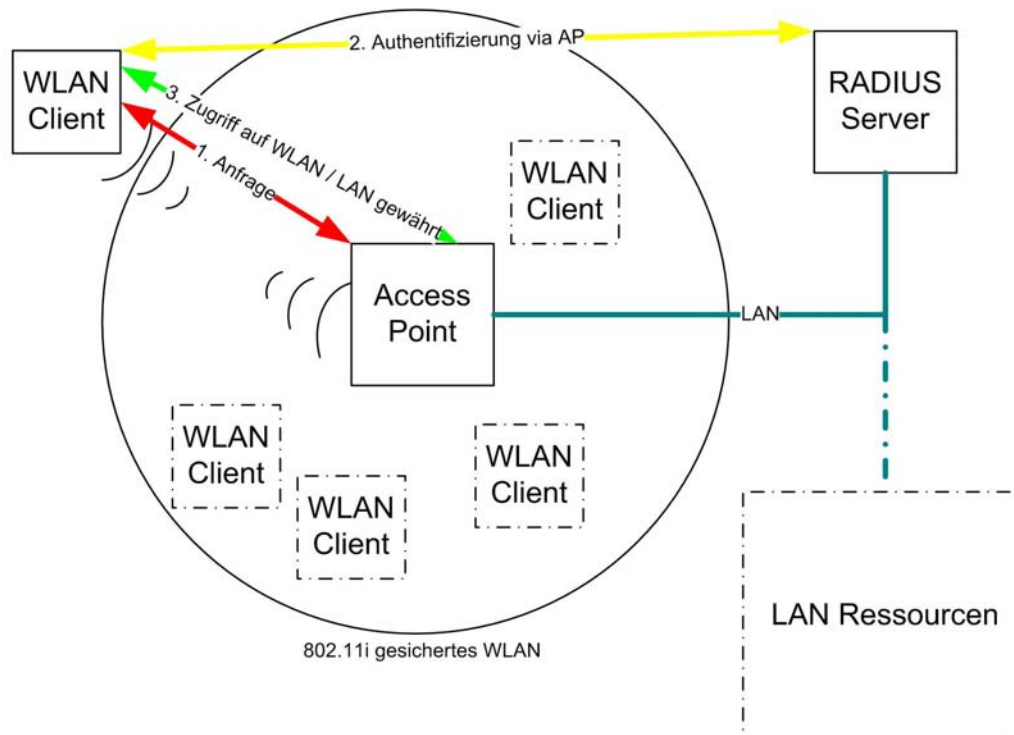


Figure 6: Schematic Sequence of Authentication on a Wireless LAN with RADIUS Server and 802.1x

802.11h, Increased Transmit Power at 5 GHz for Europe

Apart from the original frequency band of the IEEE 802.11 standard at 2.4 GHz, the 802.11a standard and the 802.11h standard that is based on it use frequencies in the GHz band. The advantage of the 5 GHz band is that few applications transmit in this band compared with the 2.4 GHz band. Here, there are no disturbances caused by defective microwave ovens or video/audio transmission systems and because they are not widely implemented, other wireless LANs hardly cause any problems either. 802.11a also provides better channel spacing so that in conjunction with a wider frequency spectrum, there are more non-overlapping channels available. There are disadvantages due to the higher attenuation of 5 GHz waves in the atmosphere.

The greatest problem with the introduction of 802.11a was, however, that the intended frequencies, particularly in Europe, were already being used by civil and military applications such as radar systems so that, for example in Germany, transmission was permitted only within buildings and only at a low transmit power. To make full use of the 5 GHz technology, the 802.11h standard was developed with additional mechanisms to prevent interfering with the so-called primary user (for example radar).

These include Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). If a channel is in use, DFS allows a controlled change to an alternative channel and is therefore useful for redundant systems in automation engineering.

Figure 7 shows how the alternative channel 40 is entered alongside the actual channel 60 over the Web interface of a SCALANCE-W access point. If the access point, for example, detects a radar system, there is a channel change according to the DFS settings. Interference-free simultaneous operation of multiple 802.11h access points in the RF field is only possible and practicable with manual channel assignment.

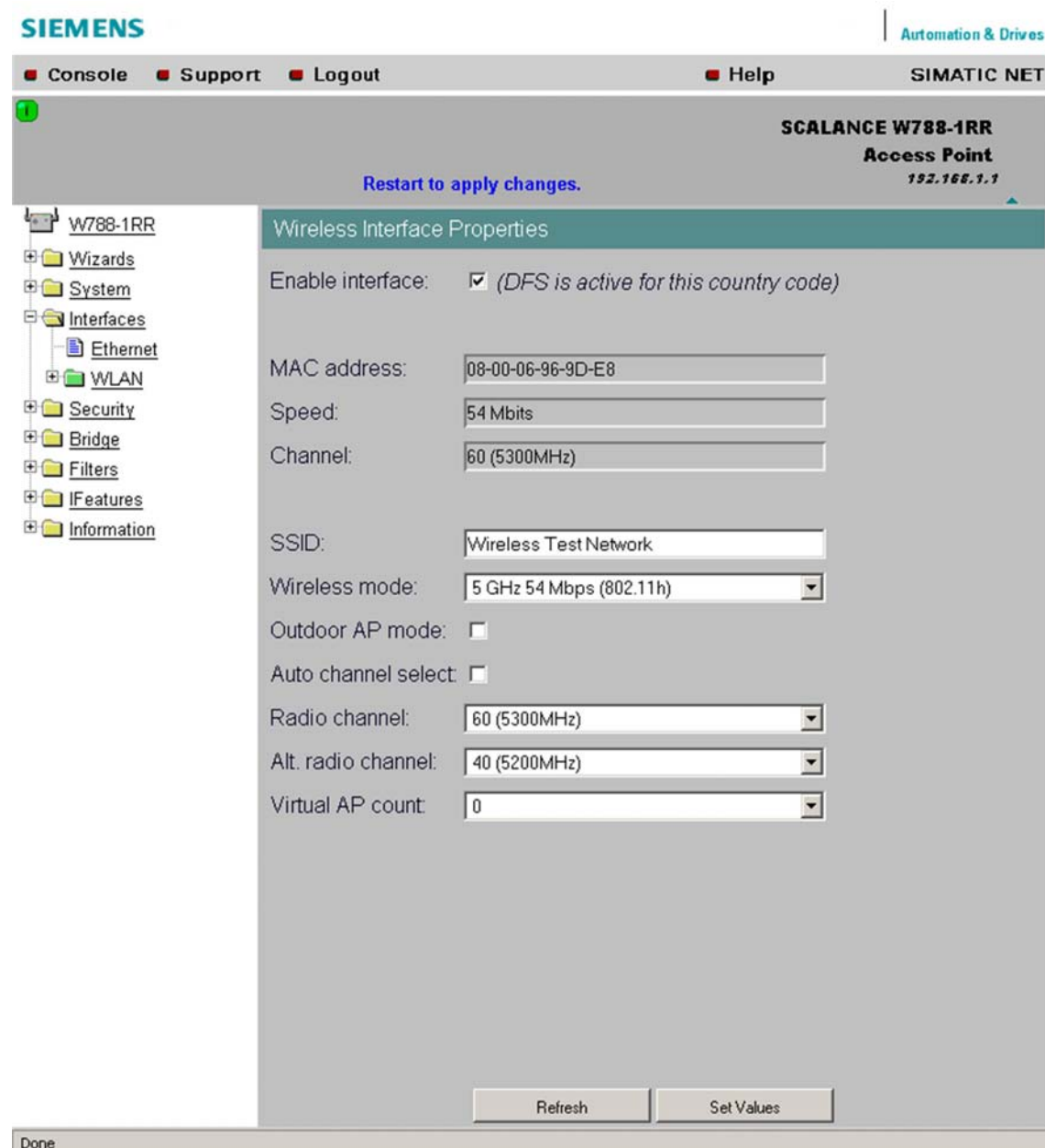


Figure 7: Configuration of the frequencies for 802.11h

The second major difference between 802.11h and 11a is TPC that limits the transmit power to the power necessary to prevent disturbing primary users in the 5 GHz unnecessarily. At the same time, it ensures restrained use of transmit power so that the frequencies used in the area can be "recycled" after shorter distances.

As already mentioned, the 802.11h standard is handled very differently in different countries and, for example, in Germany is permitted only with DFS and TPC. To compensate this, on the other hand, Germany permits the highest transmit power outdoors for the upper end of the 5 GHz band at 1 W (otherwise 200 mW). This allows the use of antennas with higher power and allows greater distances to be covered, for example for directional wireless applications

outdoors. Figure 8 explains the differences between 11a and 11h based on the example of the regulations in Germany.

	802.11a	802.11h
Betrieb	nur indoor	5,17 - 5,24 GHz: indoor 5,26 - 5,32 GHz: indoor 5,5 - 5,7 GHz: in-/outdoor
Sendeleistung	30 mW	5,17 - 5,24 GHz: 200 mW 5,26 - 5,32 GHz: 200 mW 5,5 - 5,7 GHz: 1 W
Sendeleistung in [dbm]	15	5,17 - 5,24 GHz: 23 5,26 - 5,32 GHz: 23 5,5 - 5,7 GHz: 30
Überlappungsfreie Kanäle	4	19
Einschränkungen		<ul style="list-style-type: none"> ■ ohne TPC/DFS: 30 mW ■ mit TPC: 60 mW ■ mit TPC/DFS: 200 mW / 1 W

Figure 8: Comparison of the Related Standards 802.11a and h Based on the Example of Germany

802.11e, Prioritization of Data (QoS)

Since the principle of wireless LAN is that all stations access a shared medium as peers, applications with special time requirements represent a particular challenge. Alongside the developments of various manufacturers for special quality of service requirements (see also iQoS developed for industrial application), 2005 saw completion of the 802.11e standard. This is intended to allow cross-vendor QoS. Applications that use 802.11e include, for example, telephony applications over IP (VoIP) that require preference over other data traffic. Without QoS implementation, voice transmission over a limited bandwidth could bring the other data traffic practically to a standstill.

Another example might be the operation of mesh wireless LANs (see section on 802.11s). In this case, both control information and useful data must be transferred over the same wireless network. Here, control information can be given priority to avoid data stream tailbacks and to activate alternative routes.

The standard implementation of 802.11e stipulates a cooperative procedure known as Enhanced DCF Channel Access (EDCA) and as an option, the centrally controlled HCF Controlled Channel Access Function (HCCF).

As the name implies, EDCA works according to the DCF principle (from the 802.11 standard) and introduces eight different QoS groups with different priorities. Within such a group there is no prioritization. DCF works according to the CSMA/CA principle by listening in on the medium. If there is no data exchange taking place, a station stops transmitting once a standard wait time has elapsed. Similarly with EDCA, the priority of the data to be transmitted is

converted to wait times of different lengths prior to transmission. Low priority means a long wait time, data with higher priority has a shorter wait time. Packets with higher priority (and a shorter wait time) are now given preference and transferred before other packets because their wait time has not yet elapsed.

Although EDCA does not guarantee any QoS, it is simple to handle. One disadvantage is the fact that each participating station can set any prioritization so that the data can be categorized incorrectly.

The optional HCCF which is based on the more complex PCF represents a different and smarter approach. In this case, the polling principle (see PCF from the 802.11 standard and iPCF) is used. The access point retains control at all times and can evaluate and enable or deny incoming QoS requests. This allows adherence to QoS rules to be monitored and means that QoS expectations can be delivered. A further advantage is that the available bandwidth is not wasted by time-consuming competition for the right to transmit.

Based on IEEE 802.11e, the Wi-Fi consortium has drafted the Wi-Fi Multimedia (WMM) specification that is intended to guarantee interoperability between different vendors. A product with the WMM seal therefore includes a subset of 802.11e, with particular emphasis on support of the multimedia content (audio/video applications) over wireless LAN.

QoS with 802.11e in heterogeneous networks is extremely complicated and is not dealt with in detail in this white paper. The complexity increases when QoS is required between different networks (wireless LAN, LAN, other) and also in higher OSI layers (for example layer 3, IP), for example with VoIP transmission over the Internet.

Future Wireless LAN Standards

The definition of the following standards is not yet completed. They nevertheless all have a significance for industry and automation.

802.11n, High Data Rates

The IEEE is currently pressing ahead with the 802.11n standard to increase the transmittable data rate on wireless LANs. The current target data rate is an overall throughput of 540 Mbps (depending on the technology used). In other words, there would finally be an adequate alternative to 100 Mbps cable LAN available that could conceivably be used in an Industrial Ethernet environment/TWLAN. Completion is planned for the end of 2007.

During the preparations for this white paper, the standardization process was in the voting phase with comments from competing lobbies.

There are nevertheless numerous technologies that are extremely likely to be included in the final standard. Some will be obligatory and some options.

Based on these assumptions, several manufacturers have brought products onto the market since the start of 2006 that are already advertising with the pre-11n or Draft-11n seals. These are products in which parts of the future 802.11n standard are already integrated, though there can no guarantee on finalization of the standardization that a firmware update will achieve full or partial compatibility with 802.11n. Nevertheless, these products are the first indicators of how the new technology will fare in practice. Their characteristics are described below.

To achieve the aims of the 802.11n standards, namely a significant increase in data throughput compared with 802.11a/g, not only optimized modifications to the PHY-/MAC layer and channel bonding but probably interesting new techniques such as beamforming, spatial multiplexing (along with antenna diversity) and power saving measures will be incorporated in the standard.

The improvement of the layers mentioned above will be achieved by optimization and will profit from the experience gained in the meantime with the older 802.11 standards. These include a higher coding rate, more rational use of the bandwidth which is available anyway by changing acknowledge algorithms, bundling frames that belong together (frame bursting) and similar approaches.

In beamforming, the existence of several antennas arranged as an array is an important factor. By suitable distribution of phase-shifted signals to the antennas and by using the known spatial arrangement of the send and receive lobes, it is possible to align with the required receiver in much the same way as with a rotating directional antenna. This improves not only the transmission and reception properties but also reduces unnecessary interference of neighboring networks. The location of the wireless partner must be calculated from the received radio signals and corrected accordingly on the mobile stations. Figure 9 illustrates the principle of the lobe directed to the receiver.

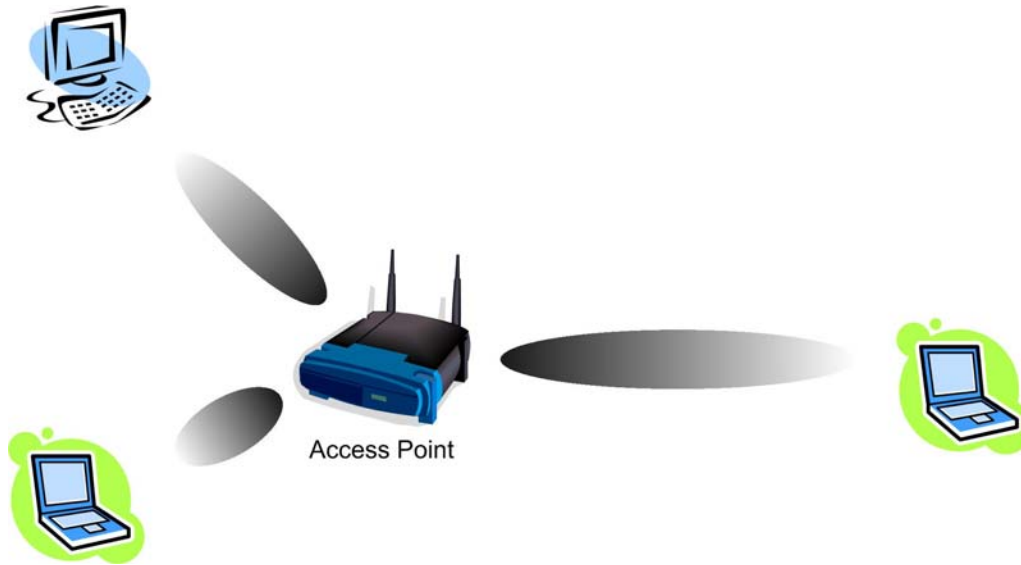


Figure 9: Idealized Representation of Communication with Beamforming

Spatial multiplexing stands for a technique that turns the disadvantage of the (actually undesirable) multipath propagation of radio waves into an advantage. By splitting the data stream into several substreams and by using multiple transmitters, it is possible to distribute the streams to multiple (spatially separate) antennas. Due to the spatial separation, the transmitted signals follow different paths, reflect at different points in space and therefore arrive at the receiver at different times. The receiver requires at least the same number of antennas and receiver modules and can filter out the original data streams using mathematical methods. The transmittable bandwidth increases almost linearly with the number of data streams/antennas used. This technology is often called MIMO (Multiple Input Multiple Output, a term from system theory).

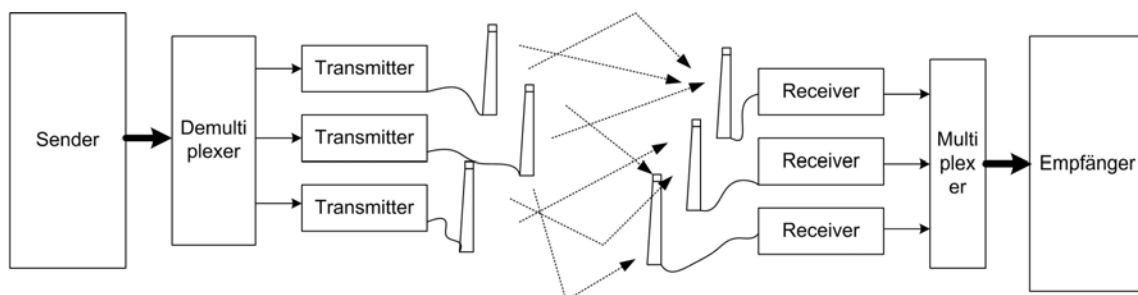


Figure 10: Increasing the data rate by utilizing multipath propagation (spatial multiplexing)

In conjunction with this technology, a further variant of antenna diversity is possible. This is the use of more antennas than existing data streams. A data stream is distributed redundantly to several antennas and therefore allows the receiver to filter out the useful signal better. Such

a constellation often results from an access point working with 3 antennas, the client only with 2 (for example, PC card where there is no space for more antennas).

In 802.11n, there are also several power saving modes being discussed, for example turning off unused transmitters and activating them only on demand. This is particularly useful when several transmitters/antennas are used as in spatial multiplexing. This is not only important for environmental reasons but also to make better use of the limited battery life in mobile devices.

802.11s, Meshed Wireless LANs

The term meshed or mesh network means literally what it says. The basic idea behind mesh networks is based on redundant paths for the transfer of data from one node to the next. If one path is disrupted, the network automatically finds a new one. In many cases, the declared aim is also to be able to add additional nodes in a mesh network with little effort. Ideally, the network should manage itself.

In conjunction with wireless LAN networks, the idea of a mesh network has become reality in the meantime although previously implemented meshed MANs were always based on proprietary developments. There are also many types of mesh network. Some providers call a Wireless Distribution System (WDS) for converting a wireless backbone a mesh network. There are versions with only one or multiple gateways to other cable networks or the Internet. Other providers, on the other hand, consider that a pure mesh network completely does without the use of any backbone infrastructure. In this case, the data is sent over several nodes to a recipient without any routers in between. The clients also function as routers for other clients.

In automation, mesh networking allows redundant data paths with which the loss of individual connections (meshes) can be compensated fully automatically. The use of wireless LAN technology in conjunction with meshed networking can allow operation in environments where cable trays would be difficult or uneconomical to install. A further scenario for the use of such networks could be in ad hoc wireless LANs that (equipped with meshed networking technology) could be set up quickly with little administrative effort, for example for trade fairs, festivals or military applications in the field.

An IEEE working group is aiming to establish a heterogeneous standard for wireless mesh networks by the year 2008. This is known as 802.11s. The aims of this standard are simple extensibility up to and including large distributed wireless LANs, flexibility in production facilities and in similar fast changing environments, the possibility of setting up networks for crisis management, for example in the case of catastrophes, and the formation of highly redundant networks that can be used by the military and in safety-oriented environments.

The future standard currently envisages three basic infrastructure elements for setting up meshed wireless LAN structures. Mesh points establish and expand a wireless backbone, mesh access points have the same function with the additional option of linking clients over a second wireless module. Mesh portals function as backbone providers and acting as a bridge also provide access to different network types. Figure 11 illustrates how the components could be arranged.

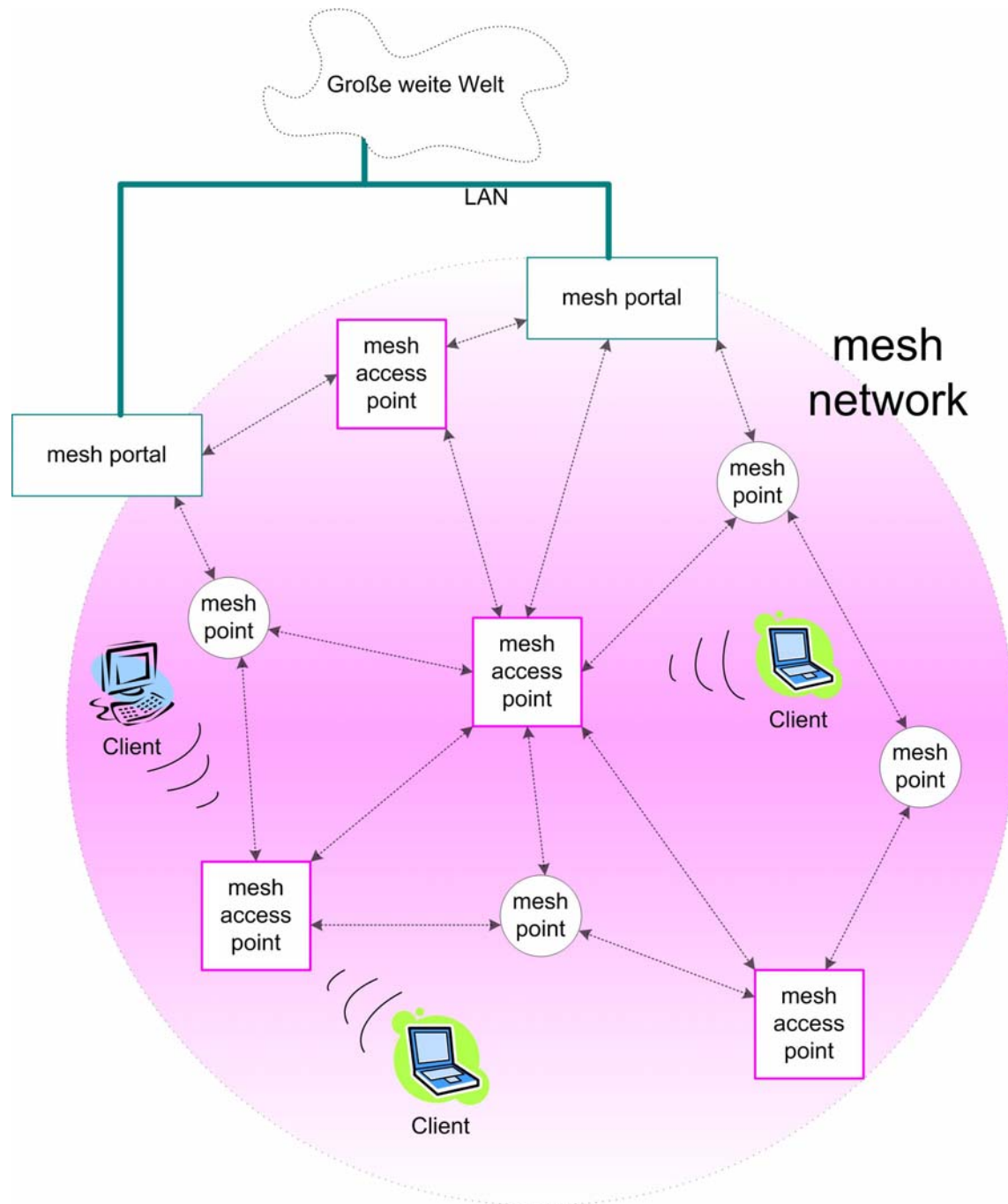


Figure 11: Setup of a Mesh Network

The 802.11s standard describes the capabilities of a mesh point.

It should be capable of recognizing its neighbors and of finding the correct route using a path selection protocol. The routing should be very hardware-oriented, in other words, optimized for speed.

Data security is based on 802.11i for which an enhancement is necessary compared with normal wireless LAN environments to implement secure connections with clients over several hops.

The mesh points must, of course, establish secure connections among themselves for which suitable mechanisms must be included for two-way authentication. To allow roaming from one mesh access point to the next, fast reauthentication must also be possible (seamless roaming) to avoid disrupting time-critical applications or sessions relevant for security. A further point is management in mesh networks to avoid overload. An expansion of the 802.11e standard is planned for management packets (for example flow control). Since the mesh points are located very close to each other, there is inevitably a strong mutual influence due to overlapping of the RF fields and mutual interference. It is therefore important that techniques such as beamforming are used to ensure that the same radio channels are used "at the earliest" in the next but one cell to avoid the channels in immediately neighboring cells from overlapping. The risk of collisions is also greater.

Glossary

2G	Digital mobile wireless networks of the second generation, for example GSM
3G	Digital mobile wireless networks of the third generation, for example UMTS Occasionally the term 2.5G is used. In this case, the expansions of GSM are meant (EDGE, GPRS)
IEC 61508	Standard relating to functional safety (new)
EN 954-1	Standard relating to functional safety (old)
Access point	WLANs are set up using access points. They also connect the wired data network.
ACK	Acknowledge Signal in handshake protocol for avoiding the hidden node problem
ACL	Access Control List List of MAC addresses with the right to access the wireless network
Ad hoc network	Wireless network between individual devices (point-to-point)
AES	Advanced Encryption Standard New standard for encryption of data in WLANs
Antenna diversity	Technique with which a radio receiver is equipped with two antennas so that it can select the better of two signals
Antenna gain	Improvement of the antenna compared with an isotropic radiator achieved by suitable construction (passive!)
ATM	Asynchronous Transfer Mode Wired network used particularly in the backbone for large distances at high data rates
Authentication	Access control in communication networks (Who am I?) to increase data security
Authorization	Distribution of authorizations in communication networks (What can I do?) to increase data security
BPSK	Binary phase shift keying Modulation technique in WLANs
BQTF	Bluetooth Qualification Test Facility

	Facility for monitoring the interoperability of products of various vendors
BSS	Basic Service Set WLAN network with access to the infrastructure over a single access point
CCK	Complementary code keying modulation mechanism in WLAN
CDMA	Code Division Multiplex Code-controlled medium access control
CF	Compact flash
CFP	Contention free period Period during which access is managed by the access point (to support time-critical services)
CP	Contention period Period in which access is controlled according to CSMA/CA (to support time-critical services)
CP	Communications processor
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, medium access control on a wireless IEEE 802.11 network
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, medium access control for wired Ethernet network
CTS	Clear to send Signal in handshake protocol for avoiding the hidden node problem
DDE	Dynamic Data Exchange
DCF	Discrete coordinated function Normal medium access control in 802.11 in contrast to PCF
DECT	Digital Enhanced Cordless Telecommunications, European standard for language and data communication
DFS	Dynamic Frequency Selection in the 5 GHz band
Diversity	Wireless receiver with two antennas allowing selection of the best signal
Downstream	Communication from access point to client
DSSS	Direct Sequence Spread Spectrum (IEEE 802.11b)
EDGE	Enhanced Data Rates for Global Systems for Mobile Communications Evolution Further development of GSM with data rates up to 384 Kbps

	for video and wireless applications
EIRP	Equivalent isotropic radiated power The power output that would have to be applied to an isotropic radiator so that it would radiate the same effective power as another antenna in a specific direction. An isotropic radiator is a theoretical antenna that radiates in all directions with equal intensity (isotropic) and is assumed to be infinitesimally small.
ESM	Electrical Switch Module
ESS	Extended Service Set Wireless network consisting of several overlapping basic service sets (BSS)
ETSI	European Telecommunication Standard Institute
Fall back	Gradual reduction of the data rate when receiving conditions are bad to allow the connection to be maintained
FDMA	Frequency Division Multiplex Access
FEC	Forward Error Correction Inclusion of redundant bits in the useful data to make the signal less sensitive to interference
FHSS	Frequency Hopping Spread Spectrum A method used in 802.11b and Bluetooth.
FTEG	Law regarding wireless equipment and telecommunications installations in Germany
GFSK	Gaussian Phase Shift Keying Modulation technique in 802.11
GPRS	General Packet Radio Service Expansion of GSM for packet-oriented data communication at up to a maximum 170 Kbps.
GSM	Global System for Mobile Communications Digital telephone services at frequencies in the 900 MHz, 1800 MHz and 1900 MHz ranges
GSM-R	GSM for railroad traffic at high speeds
Handover	Mechanism for transferring a station from one radio cell to the next. The term is often used in conjunction with <i>roaming</i> .
Handshake	Acknowledgment process to establish a connection between stations ready to communicate.
Hidden node problem	Two nodes are arranged in a radio cell so that they are outside their own transmission range. If they both access the

	medium of the same time, collisions result.
HIPERLAN	High-performance Radio LAN in the 5 GHz band
Home RF	Standard for wireless communication between PCs and home-oriented consumer devices.
HSCSD	High Speed Circuit Switched Data GSM wireless network for higher data rates
IAPP	Inter Access Point Protocol Protocol for communication between the APs
IBSS	Independent Basic Service Set Ad-hoc network for spontaneous and simple establishment of wireless connections without a wireless infrastructure
IE	Industrial Ethernet
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 2 Mbps.
IEEE 802.11a	Standard for wireless networks in the 5 GHz range with transmission rates of up to 54 Mbps.
IEEE 802.11b	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 11 Mbps.
IEEE 802.11g	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 54 Mbps.
IEEE 802.11h	Standard for wireless networks in the 5 GHz band with transmission rates up to 54 Mbps. Standard for continental Europe; condition DFS/TPC
IEEE 802.11i	Security standard that replaces the obsolete WEP standard; It includes, among other things, the AES encryption technique
IEEE 802.3af	Standard defining power-over-Ethernet (PoE)
IP	Internet Protocol Collection of program routines that the TCP protocol accesses
IP20	Device degree of protection
IP 65	Device degree of protection
IPSec	Internet Protocol Security Open standard for increasing data security in IP networks

IrDA	Infrared Data Association Standard for data communication with infrared over short distances
IS	Intrinsically Safe (protected against explosion)
ISM band	Industrial, Scientific and Medical Band Frequency band for use without license
ISO	International Organization for Standardization
Kerberos	Security system for the encryption of sensitive data
FOC	Fiber-optic cable Transmission medium for optical networks.
Multipath propagation	Reflections of an electromagnetic wave from different objects. As a result, the electromagnetic wave arrives at the receiver with different intensities and after different propagation times
MIC	Message Integrity Protocol Technique for increasing the integrity of data in WLANs
MIMO	Multiple In, Multiple Out, with multiple antennas
Mini PCI	Special design of WLAN adapters for direct integration in products
MSS	Mobile Satellite Service within UMTS
OFDM	Orthogonal Frequency Division Multiplex Method of modulation in 802.11a
OFDM/CCK	Orthogonal Frequency Division Multiplex/complimentary code keying Method of modulation in 802.11a
PAN	Personal Area Network Network for devices at relatively short distances from each other.
PC Card	Design and use, see PCMCIA. In contrast to PCMCIA, instead of a 16-bit interface, a 32-bit interface is used so that in the case of WLAN high data rates up to 54 Mbps can also be transmitted
PCF	Point coordinated function Medium access control technique to support time-critical services in WLANs
PCMCIA	Standard for PC cards (credit card size). PCMCIA cards (Personal Computer Memory Card International Association) are used for input/output (for example modem), as additional memory, and also as interfaces for WLAN particularly in

	laptops
PDA	Personal Digital Assistant Mobile end device
Pico network	Network structure in Bluetooth in which up to eight stations are organized
QAM	Quadrature amplitude modulation
QPSK	Quadrature phase shift keying
QoS	Quality of Service
R&TTE	Radio and Telecommunications Terminal Equipment Directive EU directive for telecommunications terminal equipment
RADIUS	Remote Authentication Dial - In User Service for secure communication networks
RCM	Radio Client Module (Ethernet adapter, Ethernet client)
RegTP	Regulatory body for telecommunication in Germany
RLM	Radio Link Module (access point)
Roaming	Free movement of wireless LAN nodes even beyond the boundaries of an access point's cell. The station can change from one radio cell to the next without any noticeable interruption (see also handover)
RT	Real Time
RTS	Request To Send Signal in handshake protocol for avoiding the hidden node problem
Scatter network	Network structure in Bluetooth in which several Pico networks are organized
SIG	Special Interest Group The user organization for Bluetooth
SNMP	Simple Network Management Protocol Standardized protocol for transporting network management information.
SSID	Service Set Identifier Address Name of the WLAN
TDMA	Time Division Multiplex Access
TKIP	Temporal Key Integrity Protocol Scheme for cyclic changing of the keys in WLANs

TPC	Transmission Power Control Automatic control of transmitter power in the 5 GHz band
UMTS	Universal Mobile Telecommunications System Mobile wireless transmission for voice, audio, image, video, and data communications
UNII	Unlicensed National Information Infrastructure Name of the 5 GHz band in American literature
Upstream	Communication from client to access point
URAN	UMTS Radio Access Network
UTRAN	UMTS Terrestrial Radio Access Network
WCDMA	Wideband CDMA Method of modulation for high data rates
WDS	Wireless Distribution System Radio links for connecting the access points for an extended service set (ESS)
Web pad	Portable device in DIN-A4 size with a touchscreen for Internet use
WECA	Wireless Ethernet Compatibility Alliance An alliance of various wireless LAN product manufacturers who ensure product compatibility through product testing.
WEP	Wired Equivalent Privacy Encryption scheme for WLANs (obsolete)
Wi-Fi seal	Wireless Fidelity Seal of approval of the WECA alliance for compatible and tested components.
Wired LAN	Network operated on guided media
Wireless LAN	Network operated using unguided media
WLAN	Wireless LAN (here: IEEE 802.11)
WLANA	The Wireless LAN Association Consortium of wireless LAN providers promoting wireless LAN technology
WPA	Wireless Protected Access A provisional security mechanism from WECA that closes existing security gaps in WEP. The AES encryption scheme is used. This will be replaced by IEEE 802.11i.

SIMATIC NET White Paper V.1.0

Industrial Wireless LAN – Industrial Features and Current Standards, Summer 2006
