The IEEE 802.11 universe

Article *in* IEEE Communications Magazine · February 2010

DOI: 10.1109/MCOM.2010.5394032 · Source: IEEE Xplore

The IEEE 802.11 Universe

Guido R. Hiertz, RWTH Aachen University
Dee Denteneer, Philips
Lothar Stibor and Yunpeng Zang, RWTH Aachen University
Xavier Pérez Costa, NEC Laboratories Europe
Bernhard Walke, RWTH Aachen University

ABSTRACT

The introduction of IEEE's 802.11 standards has enabled a mass market, with a huge impact in the home, office, and public areas. Today, laptops, PCs, printers, cellular phones, VoIP phones, MP3 players, Blu-Ray players, and many more devices incorporate wireless LAN technology. With low-cost chipsets and support for high data rates, 802.11 has become a universal solution for an ever increasing application space. As a direct consequence of its high market penetration, several amendments to the basic 802.11 standard have been developed or are under development. They fix technology issues or add functionality expected to be required by future applications. In this article we overview the emerging 802.11 standard and address the technical context of its extensions. The article highlights its finalized amendments and those under development.

INTRODUCTION

Standards in the IEEE project 802 target the physical layer (PHY) and medium access control (MAC) layer. When wireless local area network (WLAN) was first conceived, it seemed that it would be just another PHY of one of the available standards. The first candidate considered for this was IEEE's most prominent standard 802.3 (Ethernet). However, it soon became obvious that the radio medium is very different from the well-behaved wire. Due to tremendous attenuation even over short distances, collisions cannot be detected. Hence, 802.3's carrier sense multiple access with collision detection (CSMA/CD) could not be applied.

The next candidate standard to be considered was 802.4. Its coordinated medium access, the token bus concept, was believed to be superior to 802.3's contention-based scheme. Hence, WLAN began as 802.4L [1]. However, already in 1990 it was obvious that token handling in radio networks was difficult. The standardization body realized that a wireless communication standard would need its own very unique MAC. Finally, on March 21, 1991, project 802.11 was approved.

The first 802.11 standard was published in 1997. At the lowest layer (PHY,) it provides three solutions: a frequency hopping (FHSS) and a direct sequence spread spectrum (DSSS) PHY in the unlicensed 2.4 GHz band, and an infrared PHY at 316–353 THz. Although all three provide a basic data rate of 1 Mb/s with an optional 2 Mb/s mode, commercial infrared implementations do not exist.

Similar to 802.3, basic 802.11 MAC operates according to a listen-before-talk scheme [2], and is known as the distributed coordination function (DCF). It implements carrier sense multiple access with collision avoidance (CSMA/CA) rather than collision detection as in 802.3. Indeed, as collision cannot be detected in the radio environment, 802.11 waits for a backoff interval before each frame transmission rather than after collisions. In addition to DCF, the original 802.11 standard specifies an optional scheme that depends on a central coordination entity, the point coordination function (PCF). This function uses the so-called point coordinator (PC) that operates during the so-called contention-free period. The latter is a periodic interval during which only the PC initiates frame exchanges via polling. However, the PCF's poor robustness against hidden nodes resulted in negligible adoption by manufacturers.

Having published its first 802.11 standard in 1997, the Working Group (WG) received feedback that many products did not provide the degree of compatibility customers expected. As an example, often the default encryption scheme, called Wired Equivalent Privacy (WEP), would not work between devices of different vendors. This need for a certification program led to the foundation of the Wireless Ethernet Compatibility Alliance (WECA) in 1999, renamed the Wi-Fi Alliance (WFA) in 2003. Wi-Fi certification has become a well-known certification program that has significant market impact.

The tremendous success in the market and the perceived shortcomings of the base 802.11 standard provided a basis and impetus for a prolific program of improvements and extensions.

0163-6804/10/$25.00 © 2010 IEEE

Title	Project approval date	Final approval date	802.11-1999 Amendment	Title	Comment
802.11-1997	1991-03-21	1997-06-26		IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	Initial standard
802.11-1999	1997-09-12	1999-03-18		Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	Superseded by ISO/IEC 8802.11: 1999
ISO/IEC 8802.11: 1999	N/A	2005-09-30		IEEE Std 802.11-1999 (R2003)	International standard
802.11a	1997-09-16	1999-09-16	1	Higher Speed PHY Extension in the 5 GHz Band	54 Mb/s OFDM PHY @ 5 GHz
802.11b	1997-12-09	1999-09-16	2	Higher Speed PHY Extension in the 2.4 GHz Band	11 Mb/s DSSS PHY @ 2.4 GHz
802.11b-cor1	2000-01-30	2001-10-10		Corrigenda to IEEE 802.11b-1999	Clarifies amendment 2
802.11d	1999-06-26	2001-06-14	3	Operation in Additional Regulatory Domains	Allows devices to comply with regional requirements
802.11e	2000-03-30	2005-09-22	8	MAC Enhancements	Support for QoS
802.11f	2000-03-30	2003-06-12		Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation	Released as 802.11.1 and administratively withdrawn by IEEE-SA Standards Board on 2006-02-03
802.11g	2000-09-21	2003-06-12	4	Further Higher Data Rate Extension in the 2.4 GHz Band	54 Mb/sOFDM PHY @ 2.4 GHz
802.11h	2000-12-07	2003-09-11	5	Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe	In Europe, 5 GHz devices must implement 802.11h
802.11i	2001-05-30	2004-06-24	7	MAC Security Enhancements	MAC Security enhancements, known as WPA and WPA2 from Wi-Fi Alliance
802.11j	2002-12-11	2004-09-23	6	4.9 GHz–5 GHz Operation in Japan	Compliance with Japanese 5 GHz spectrum regulation
802.11ma	2003-03-20	2007-03-08		802.11 Standard Maintenance & Revision	Prepared 802.11-2007 that supersedes 802.11-1999
802.11t	2004-08-12	2009-12-31		Recommended Practice for the Evaluation of 802.11 Wireless Performance	Task Group aimed to develop 802.11.2, 2006-02-03 administratively withdrawn by IEEE-SA

Table 1. *Withdrawn and superseded documents. The 802.11-1999 standard and its amendments, 1–8, have been incorporated by the 802.11-2007 standard.*

This has led to revisions of the draft, driven by a complete alphabet of amendments. The complete history of this process is detailed in Tables 1 to 3. It is the purpose of this article to review this process and explain both the contents of these amendments and their interrelation. In the following we first describe the changes made to the PHY layer and then turn to the improvements to the MAC layer. In both, we make a distinction between what has already been accepted and what is currently in the process of being standardized.

PHY Related Amendments

Although not interoperable, the DSSS and FHSS PHY initially seemed to have equal chances in the market. The FHSS PHY even had a duplicate in the HomeRF group that aimed at integrated voice and data services [3]. This used plain 802.11 with FHSS for data transfer, complemented with a protocol for voice that was very similar to the Digital Enhanced Cordless Telecommunications standard. Neither HomeRF nor 802.11 saw FHSS extensions, although plans

Title	Project approval date	Final approval date	802.11-2007 Amendment	Title	Comment
802.11-2007	2003-03-20	2007-03-08		Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	802.11-2007 supersedes 802.11-1999 and incorporates amendments a, b, d, e, & g–j
802.11c	1997-12-09	1998-09-16		Media Access Control (MAC) Bridges — Supplement for Support by IEEE 802.11	Part of IEEE 802.1D-2004 bridging standard
802.11k	2002-12-11	2008-03-31	1	Radio Resource Measurement	Measurements of the wireless channel
802.11n	2003-09-11	2009-09-11	5	Enhancements for Higher Throughput	600 Mb/s MIMO PHY @ 2.4 GHz and 5 GHz
802.11r	2004-05-13	2008-06-30	2	Fast Roaming	Fast hand-off for moving devices
802.11w	2005-03-20	2009-09-30	4	Protected Management Frames	Security for management frames
802.11y	2006-03-16	2008-06-30	3	3650–3700 MHz Operation in USA	Contention-based protocols for FCC band 3.65 GHz in the U.S.

Table 2. *The currently active 802.11-2007 standard has five amendments. To avoid confusion with other 802 standards letters l, o, q, and x are not used.*

for a second-generation HomeRF existed that targeted at 10 Mb/s. In contrast, the high-rate project 802.11b was started in December 1997 and boosted the data rates of the DSSS PHY to 11 Mb/s. This caused 802.11b to ultimately supersede FHSS, including HomeRF, in the market. Figure 1 provides an overview of the 802.11 PHY amendments and their dependencies.

802.11a, g, h, j: OFDM for WLAN

The first extension project, 802.11a, started in September 1997. It added an orthogonal frequency-division multiplexing (OFDM) PHY that supports up to 54 Mb/s data rate. Since 802.11a operates in the 5 GHz band, communication with plain 802.11 devices is impossible. This lack of interoperability led to the formation of 802.11g, which introduced the benefits of OFDM to the 2.4 GHz band. As 802.11g's extended rate PHY provides DSSS-compatible signaling, an easy migration from 802.11 to 802.11g devices became possible. During the standardization process, a single manufacturer already sold pre-802.11g chipsets. With its proprietary packet binary convolutional code (PBCC), additional data rates of 22 Mb/s and 33 Mb/s were supported. Today rarely applied, PBCC set a de facto standard and became an optional modulation and coding scheme (MCS) of 802.11g.

To comply with the European regulatory requirements for the 5 GHz band, 802.11h was introduced at the end of 2003. While in the United States the FCC describes absolute radio output power limits, in Europe antenna gain must not be used for transmission. Furthermore, satellite uplink and radar stations must be secured from interference. Therefore, 802.11h defines MAC mechanisms for dynamic frequency selection (DFS) and transmit power control (TPC), which we explain in the MAC section.

Ratified in 2004, 802.11j describes the necessary means to comply with Japanese regulatory requirements for the operation of 802.11 equipment in the 4.9 GHz and 5 GHz frequency bands. Besides requirements on medium access discussed in the next section, 802.11j is the first amendment that defines PHY operation with 10 MHz bandwidth in addition to the formerly preferred 20 MHz channelization.

802.11n: High Throughput

As the first project whose targeted data rate is measured on top of the MAC layer, 802.11n provides user experiences comparable to the well-known Fast Ethernet (802.3u). Far beyond the minimum requirements that were derived from its wired paragon's maximum data rate of 100 Mb/s, 802.11n delivers up to 600 Mb/s.

Its most prominent feature is multiple-input multiple-output (MIMO) capability. A flexible MIMO concept allows for arrays of up to four antennas that enable spatial multiplexing or beam forming. Its most debated innovation is the usage of optional 40 MHz channels. Although this feature was already being used as a proprietary extension to 802.11a and 802.11g chipsets, it caused an extensive discussion on neighbor friendly behavior. Especially for the 2.4 GHz band, concerns were raised that 40 MHz operation would severely affect the performance of existing 802.11, Bluetooth (802.15.1), ZigBee (802.15.4), and other devices. The development of a compromise, which disallows 40 MHz channelization for devices that cannot detect 20 MHz-only devices, prevented ratification of 802.11n until September 2009.

As a consequence of 20/40 MHz operation and various antenna configurations, 802.11n defines a total of 76 different MCSs. Since several of them provide similar data rates, WFA's certification program decides the MCSs finally used in the market. 802.11n's PHY enhancements are supported by medium access enhancements we introduce in the MAC section.

802.11ac and ad: Very High Throughput

802.11ac and 802.11ad develop amendments that fulfill the International Telecommunication Union's (ITU's) requirements on proposals for the

Title	Project approval date	Expected final approval date	Title	Comment
802.11mb	2007-03-22	2011-03-31	802.11 Accumulated Maintenance Changes	Second maintenance TG
802.11p	2004-09-23	2010-06-30	Wireless Access for the Vehicular Environment	Car to car communication, closely related to IEEE 1609
802.11s	2004-05-13	2010-09-30	Mesh Networking	Transparent multi-hop operation
802.11u	2004-12-08	2010-09-30	Interworking with External Networks	Convergence of 802.11 and GSM
802.11v	2004-12-08	2010-06-30	Wireless Network Management	Management
802.11z	2007-08-22	2010-01-31	Extensions to Direct Link Setup (DLS)	AP independent DLS
802.11aa	2008-03-27	2011-06-30	Video Transport Streams	MAC enhancements for robust audio video streaming
802.11ac	2008-09-26	2012-12-31	Very High Throughput <6 GHz	Enhancements for >1 Gb/s throughput for operation in bands below 6 GHz
802.11ad	2008-12-10	2012-12-31	Very High Throughput 60 GHz	Enhancements for >1 Gb/s throughput for operation in 60 GHz band

Table 3. *Amendments under development.*

IMT Advanced standard [4]. Both target greater than 1 Gb/s throughput, but while 802.11ac considers the traditional WLAN frequencies below 6 GHz, 802.11ad competes with the Wireless Personal Area Network Task Group (TG) 802.15.3c, standard ECMA 387, and the Wireless Gigabit Alliance on the 60 GHz frequency spectrum. Due to their premature stage, both TGs are still in the process of collecting input and specific proposals from their members. At the moment of writing this article, 802.11ad has already started defining some additional requirements regarding range (at least 10 m at 1 Gb/s), seamless session transfer of an active session from the 60 GHz band to the 2.4/5 GHz band and vice versa, coexistence with other systems in the band such as 802.15.3c, and support for uncompressed video requirements such as data rate, packet loss ratio, and delay.

802.11p: A Frequency Band for Vehicular Communication

Accepted in September 2003, 802.11p is specifically targeted at vehicular environments. It operates in the 5.85–5.925 GHz ITS band in the United States and the newly allocated 5.855–5.905 GHz band in Europe. Its PHY is identical to OFDM-based 802.11a. However, in addition to the traditional 20 MHz, 802.11p can optionally operate with reduced 10 MHz channel spacing in order to compensate for the increased delay spread in outdoor vehicular environments. With 10 MHz channel spacing, the maximum PHY data rate supported is halved to 27 Mb/s. To allow for longer communication distance, maximum radio output power may be increased up to 760 mW. Due to the harsh environmental conditions, 802.11p requires radios to be opera-

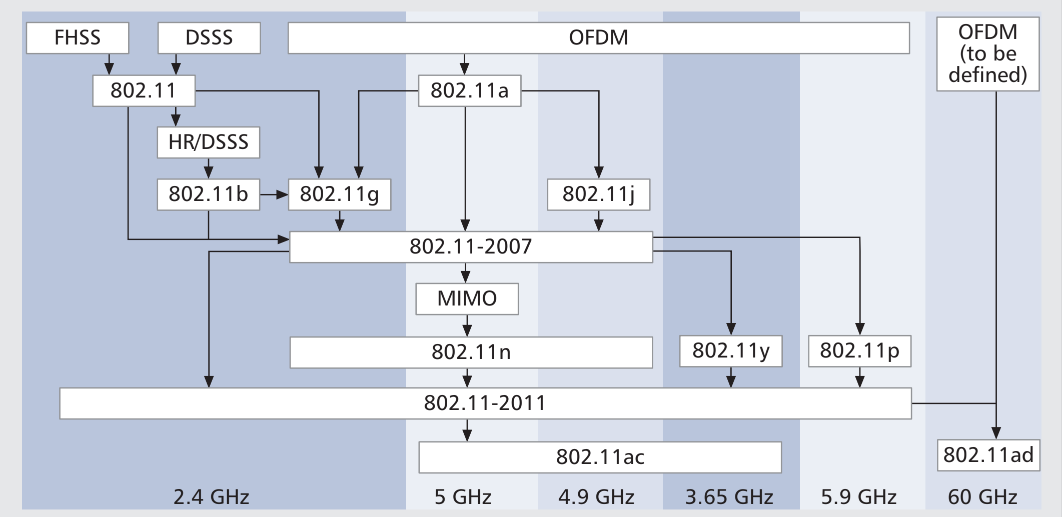

Figure 1. *The 802.11 PHY layer amendments and their dependencies.*

A key element to the 802.11 success is its simple MAC operation based on the DCF protocol. This scheme has proven to be robust and adaptive to varying conditions, able to cover most needs sufficiently well.

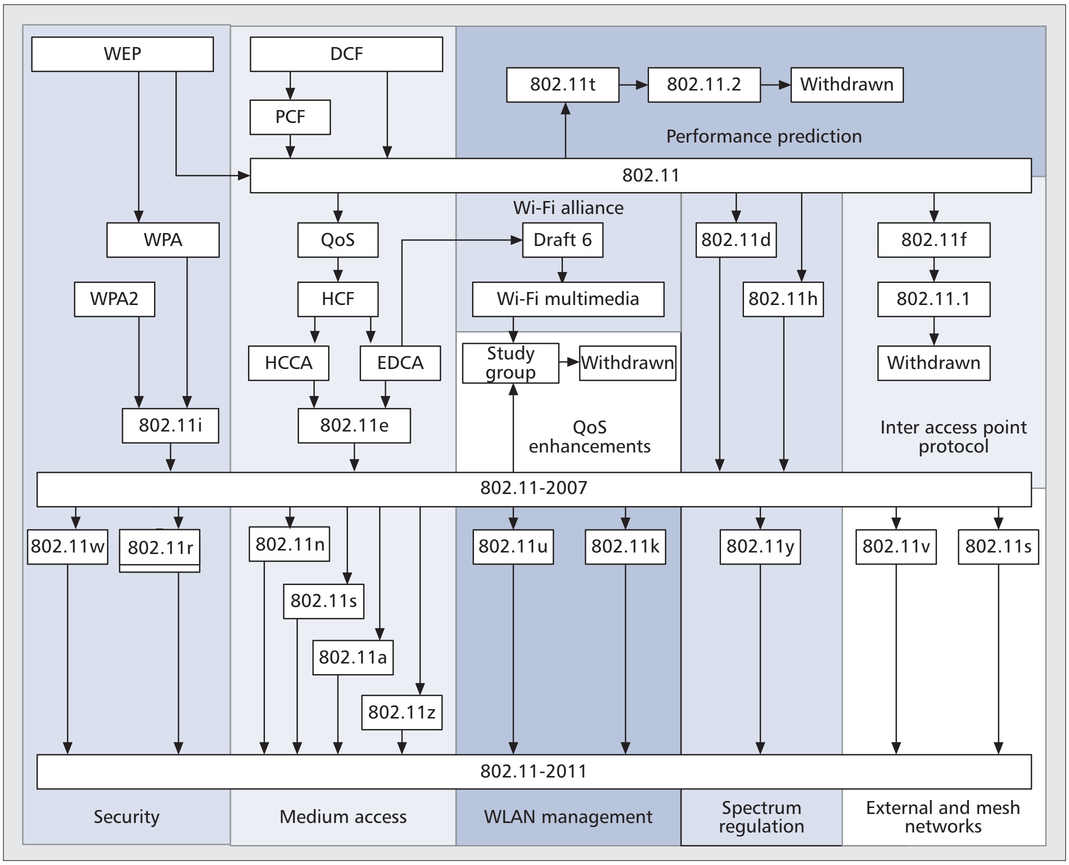

Figure 2. *The 802.11 MAC layer amendments.*

ble in an extended temperature range from –40°C to 85°C. In the MAC section we focus on the features necessary to meet specific needs that limit latency (e.g., for safety-related applications).

802.11y: Wide Area Coverage

In 2005 the FCC defined a new regulatory regime for systems that operate within 3.65–3.7 GHz [5]. With up to 20 W output power, systems applying a so-called contention-based -rotocol may provide wide-range coverage. Although the FCC offers licenses (at low cost), exclusive medium usage is not guaranteed. Instead, the FCC provides a central database where operators must give their base stations' positions. Due to possible location-dependent restrictions, an operator's signaling enables or disables the customers' equipment. We provide details on this in the MAC chapter. As 3.65 GHz has been targeted by WiMAX (802.16) vendors too, 802.11y caused intensive discussion in the 802.19 (Wireless Coexistence) WG.

MAC Related Amendments

A key element to the 802.11 success is its simple MAC operation based on the DCF protocol. This scheme has proven to be robust and adaptive to varying conditions, able to cover most needs sufficiently well. Following the trends visible from the wired Ethernet, 802.11's success is mainly based on overprovisioning of its capacity. The available data rate was sufficient to cover the original best effort applications, so complex resource scheduling and management algorithms were unnecessary. However, this may change in the future. Because of the growing popularity of 802.11, WLANs are expected to reach their capacity limits. Moreover, applications like voice and video streaming pose different demands for quality of service. Therefore, traffic differentiation and network management might become inevitable. In the following we explain 802.11 MAC related extensions of the amendments introduced in the previous section and those shown in Fig. 2.

802.11e: Support for QoS

The original project goal of 802.11e, approved at the end of March 2000, foresaw general enhancements of the WLAN standard. Efficiency improvements, support for quality of service (QoS), and security enhancements were its key elements. However, already in 2001, the 802.11 frame encryption algorithm WEP was broken by an attack. Thus, security enhancements were displaced to a new TG called 802.11i. After intensive discussions, 802.11e was finally approved in 2005 to support QoS. As a new medium access scheme, 802.11e provides the hybrid coordination function (HCF), where *hybrid* relates to HCF's two MAC protocol versions with centralized and distributed control, respectively [6]. The first is implemented by HCF controlled channel access (HCCA), an improved variant of the PCF requiring a central coordination instance that schedules medium access. Until today no device implementing HCCA is known to exist in the market. Enhanced distributed channel access (EDCA) is HCF's second MAC protocol. While DCF does not differentiate between traffic with different QoS needs, EDCA provides support for four traffic categories: voice, video, best effort, and background with different rules to access the wireless medium [6]. Accordingly, EDCA enables service differentiation. Both centralized and distributed MAC protocols change the medium sharing rules. Without 802.11e, a WLAN provides per packet fairness: regardless of the actual frame transmission duration, devices back off after every single frame. In contrast, duration of all HCCA and EDCA frame exchanges is bound by the transmission opportunity (TXOP) limit. Thus, devices share time slices of the wireless medium. Those that use faster MCSs may exchange multiple frames after a single successful contention and consequently achieve higher throughput.

Derived from EDCA, WFA has successfully branded and introduced to the market an EDCA variant called Wi-Fi multimedia (WMM). WMM incorporates a subset of functions from 802.11e draft 6 (November 2003). As the final 802.11e and WMM specifications differ, some members of the 802.11 initiated a QoS Enhancement Study Group (SG) in May 2007. Its intended goal was an adaptation of the 802.11e amendment to the WMM specification. However, a project could never be approved, and the SG was dissolved in November 2007.

802.11aa: Audio/Video Streaming

After one year of debating and several changes to its scope, 802.11aa came into life in March 2008. 802.11aa cooperates with the audio/video bridging TG 802.1AVB that develops the general principles for time-synchronized low-latency streaming services in 802 networks. Considering the adverse conditions of the wireless channel, 802.11aa adds MAC enhancements that enable differentiation of frames within the same 802.11e traffic category. For example, I-frames of an MPEG2 stream may receive higher precedence than their depending B-frames. Accordingly, 802.11aa allows for gracefully degrading the stream quality in case of insufficient channel capacity. As the latter may occur in densely populated homes where several WLANs overlap, 802.11aa will address this problem too.

802.11e, n: MAC Efficiency Enhancements

Block acknowledgments improve TXOP efficiency by allowing 802.11e devices to transmit consecutive frames without intermediate acknowledgment frames (ACKs) required by the receiver. Instead, the receiver sends a single block ACK to indicate success or failure of reception for each frame transmitted. Since gaps for transceiver turnaround can then be avoided, overhead can be saved. Unfortunately, WMM does not incorporate this efficiency enhancement. Additionally, 802.11n offers frame aggregation and reduced interframe spacing that eliminate or at least reduce the transmission idle periods between consecutive frames. As the maximum transmission size increases to 7955 B with 802.11n, several frames can be included in a single packet. Since fast MCSs lead to short frame transmission durations, 802.11n devices may use the Reverse Direction protocol to grant part of their TXOP to be used for frame reception. Thus, a previously receiving device may send in the reverse direction without the need for a backoff interval. This function appears useful to support higher-layer protocols like TCP sending back ACKs to the traffic source or VoIP conversations that have bidirectional traffic characteristics.

Pushed again by market demands, at the end of June 2007 WFA started a certification program based on draft 2.0 of 802.11n. Several vendors announced their devices as upgradeable to the final 802.11n standard and the respective WFA certification.

802.11e, z: Direct Link Setup

With WLANs that use an access point (AP), any traffic must be relayed through the AP. However, with 802.11 conquering the consumer electronics market, more and more devices need to exchange local traffic. The video stream of a Blu-Ray player placed below the HDTV display must be sent twice in the AP-based WLAN: from the player to the AP and from the AP to the HDTV. A direct frame exchange between adjacent devices would save half of the data transmission, and they could in addition benefit from a higher-rate MCS due to a shorter communication distance. 802.11e offers an optional solution, the Direct Link Setup (DLS) protocol, that requires a DLS-capable AP. However, DLS is not part of WFA's WMM certification; therefore, almost no DLS- capable APs are available in the market. Since existing APs may not be upgradeable, DLS-capable devices cannot benefit from non-relayed communication. Within 802.11z a remedy is under development by targeting the definition of an AP-independent DLS setup. To initiate a direct link connection, 802.11z-capable devices use a special Ethertype frame to tunnel setup messages through a legacy AP. Furthermore, the 802.11z TG allows for the possibility of frequency offloading, where devices use a power save indication to the AP to switch to an empty frequency channel for DLS frame exchanges.

802.11r: Support for Handoff

With a growing amount of highly mobile 802.11 devices, roaming support becomes increasingly important. Without the features of 802.11r, a device in motion sometimes loses connectivity, searches for a new AP, and finally needs to re-associate to a new AP. With 802.11r, devices may register in advance with neighbor APs. Thus, security and QoS-related settings can be negotiated before a device needs to switch to a new AP. Accordingly, the duration of connectivity loss can be substantially reduced.

802.11p: Interface for the 1609 Family

802.11p enables communication between devices moving at vehicular speed of up to 200 km/h. It is part of the Wireless Access in Vehicular Environments (WAVE) framework. Besides the PHY, 802.11p defines the lower part of the MAC layer, while the IEEE 1609 family of standards address the upper part of the MAC (1609.4), networking (1609.3), security (1609.2), resource management (1609.1), communication management (1609.5), and overall architecture (1609.0). With maximum communication range of 1 km, the time for data exchange between two moving devices is limited to a few seconds before connectivity is lost. As connectivity time is short, devices neither associ-

After one year of debating and several changes to its scope, 802.11aa came into life in March 2008. 802.11aa cooperates with the audio/video bridging TG 802.1AVB that develops the general principles for time-synchronized, low latency streaming services in 802 networks.

Although 802.11 has its roots in the worldwide license exempt band at 2.4 GHz, in June 1999 project 802.11d was approved which aimed at addressing regional requirements. Two years later, the regulatory framework was accepted as the third amendment.

ate nor authenticate before data exchange. Instead, devices join WAVE networks using an internal device procedure, without any frame exchange on the wireless medium. Lack of association/authentication exposes the data communication to security risks: this is handled by the dedicated security entity specified by 1609.2. As specified in 1609.4, the WAVE system works on a multi-frequency-channel basis consisting of a control channel for safety applications and service channels for non-safety applications. Thus, global synchronization is crucial to vehicular ad hoc networks for coordinating multichannel accesses. 802.11p enhances the timing synchronization function to facilitate global timing synchronization based on an external source like GPS. To meet vehicles' privacy requirements (e.g., to avoid being traceable along a journey), a device's randomly chosen MAC address is changed regularly.

802.11i, w: Security Enhancements

The initial 802.11 standard's encryption scheme WEP caused a lot of trouble in the market. Due to poor specification, products of different vendors were likely not to be interoperable. Thus, many networks operated non-encrypted. Early in 2001, the first reports on WEP's weaknesses occurred [7]. Additionally, its preshared keying concept did not allow for integration into enterprise networks, where each device should have its own unique key. Thus, companies required their employees to use IP-based virtual private networks (VPNs), and 802.11 became a synonym for insecurity. Although the establishment of 802.11i attracted many security experts, the market did not wait for a solution. Thus, WFA started its Wi-Fi Protected Access (WPA) certification program. To allow for *firmware-only, hardware-compatible* upgrades of existing devices, WPA does not rely on new encryption schemes. Like WEP, the so-called Temporal Key Integrity Protocol uses RC4 for encryption. However, many details of key initialization and renewal have been changed. WFA's WPA2 denotes the final 802.11i amendment that includes an additional encryption scheme designed from scratch. Most important, as the new scheme relies on the Advanced Encryption Standard (AES) defined by the U.S. National Institute of Standards and Technology (NIST), a higher degree of security is achieved. Old hardware, however, cannot be upgraded.

The most recent security related amendment was published in September 2009. 802.11w targets authenticated and encrypted management frames. Although management frames do not carry user data, fraud may cause disconnection and also opens the door for wireless denial of service attacks. Thus, 802.11w is extending the 802.11i framework to close the gap.

802.11d, h, y: Spectrum Regulatory Requirements

Although 802.11 has its roots in the worldwide license exempt band at 2.4 GHz, in June 1999 project 802.11d was approved, aimed at addressing regional requirements. Two years later, the regulatory framework was accepted as the third amendment. Besides country-specific information, an 802.11d AP broadcasts information on transmit power limits of permitted frequency channels. Initially, 802.11a did not meet the European requirements for WLAN operation at 5 GHz. Since 802.11a devices are secondary users in the 5 GHz band in Europe, they must avoid interference to weather radars in satellite uplinks. Finished in 2003, 802.11h adds the DFS and TPC that are required for operation in Europe. With 802.11h, an AP can quiet associated devices and even request them to perform measurements on other frequency channels.

According to the FCC regulation for the 3.65 GHz band, devices must be enabled by a network operator. Thus, mobile or fixed customer equipment must search for enabling messages transmitted by a provider's APs. It is the network operator's duty to ensure that within designated areas specified by the FCC (e.g., along the border to Canada and Mexico as well as in areas around satellite stations), interference is limited to some threshold, or APs do not transmit enable messages to customers at all. As 802.11y enables long-range communication, APs can instruct devices to change the default value of 1 μs for signal propagation over the wireless medium. 802.11y was approved in 2008.

802.11c, f, k, s, v: 802 Integration and Network Management

As a project within the IEEE 802 framework, 802.11 provides mechanisms for interoperability to other 802 standards. 802.11c defines the necessary means for the WLAN. After its final approval in 1998, 802.11c became part of the current 802.1D standard that defines the general 802 MAC bridging (layer 2 relaying) concept. To avoid confusion with full featured 802 bridges, 802.11 defines a device that connects an 802.11 with a non-802.11 network to be a portal. While the standard would allow for unconnected APs, almost all devices in the market include an Ethernet port. Accordingly, a WFA certified AP always implements the portal function.

With Ethernet being the typical backbone for WLAN APs, a solution for message exchange between APs became necessary. In 2000 802.11 TG f started to work on a recommended practice for an Inter-Access Point Protocol, today known as 802.11.1. It allows APs of different vendors to communicate over IP and TCP/UDP frames. With support for formation and maintenance of a network of several APs, context transfer, and caching of roaming devices, 802.11.1 foresaw some details that 802.11r integrates. However, the trial-use document was never really implemented. Accordingly, 802 withdrew 802.11.1 in 2006.

To become independent of the wired backbone, 802.11 approved a mesh networking project in 2004. Amendment 802.11s enables a multihop framework, where devices mutually serve as wireless routers. Since an 802.11s mesh transmits multihop transparently within the MAC layer, it integrates seamlessly with other 802 networks. During a ballot in May 2009, its third draft received a 79 percent approval rate.

With the increasing size of areas covered by WLANs, specifying a network management standard has become urgent. The 802.11k and 802.11v amendments provide a framework for radio resource and network management, respectively. The 2008 approved 802.11k provides radio channel information that goes beyond

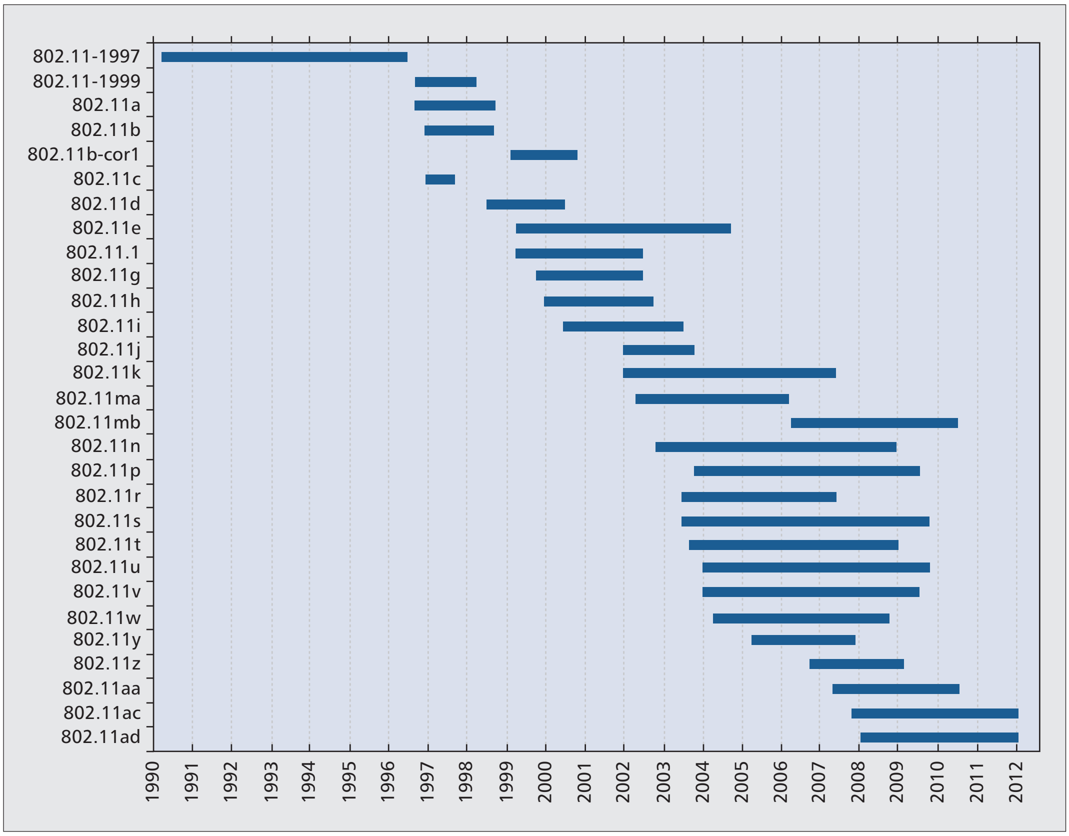

Figure 3. *Timeline of 802.11 and its amendments.*

With the increasing size of areas covered by WLANs, specifying a network management standard has become urgent. The 802.11k and 802.11v amendments provide a framework for radio resource and network management, respectively.

what 802.11h can deliver. 802.11k measurement reports include a channel load and noise histogram, provide location information, give details on a wireless link and assist APs by means of a detailed neighbor AP report. While many vendors already use device statistics for channel selection, 802.11k delivers the first standardized solution. With traffic filtering, diagnosis and event reporting, 802.11v centers on device and network management. The ninth amendment of 802.11 introduces new functionalities that allow an extended sleep time for stations. These, for instance, allow APs to proxy Address Resolution Protocol (ARP) requests for its associated devices, filter the traffic at the AP that wakes a specific station, and flexible broadcast/multicast services such that stations do not need to awake at each broadcast/multicast transmission period.

802.11u: Large-Scale Networks

Due to the convergence of WLAN and cellular in mobile phones, 802.11 needs a framework for interworking with external networks that is provided in 802.11u. It offers emergency call handling (911 over voice over IP [VoIP]), QoS adaptation, and support for handover and virtual networks. With GSM, operators have shared long base stations. Without 802.11u, an AP needs one MAC address and broadcast frame per operator that is to be announced. The 802.11u amendment allows the announcement of multiple network operators by an AP in one broadcast frame. Since user databases exist in other mobile radio networks, 802.11u integrates with their authentication and authorizing framework. Based on that, instead of proprietary solutions, network operators could finally offer a standardized solution for seamless worldwide roaming.

TG m: The Maintenance Task Group

TG m works on maintenance of the standard. It prepares the official replies to interpretation requests that anyone can send to the 802.11 WG. TG m also resolves problems noticed with the 802.11 standard and its finalized amendments. Besides technical corrections and clarifications, project 802.11ma foresaw the release of a new version of the 802.11 standard that integrates amendments a, b, d, e, g, h, i, and j into a single document. Its outcome was standard 802.11-2007 that defines the current baseline document [8]. Expected to finish in 2011, 802.11mb is 802.11's second maintenance group and will integrate k, n, r, w, y, and further amendments.

802.11.2: Wireless Performance Prediction

The Wireless Performance Prediction TG t aimed at the definition of a recommended practice for performance tests. Its latest draft, 802.11.2, defines a set of metrics, measurement methodologies, and test conditions. Devices under test are evaluated in line-of-sight and non-line-of-sight conditions. Indoor, outdoor, and shielded chambers can be used for testing. The measured metrics vary from overall results like throughput, over PHY related details such as adjacent channel interference, to packet loss and power consumption. Due to diminishing support, TG t was withdrawn in 2008.

Conclusion

The 802.11-2007 standard and its amendments provide a rich feature set for wireless communication. 5, 10, 20, and 40 MHz channel bandwidth in the 2.4, 3.65, and 4.9–5 GHz frequency bands support a wide range of regulatory domains. Furthermore, the 802.11 MAC has proven to be flexible enough to expand from its ancestral market segments. While 802.11n and mesh networks extend well-known applications, wide range (802.11y) and vehicular communication (802.11p) open new scenarios for WLAN. But the increasing amount of amendments also makes it more and more difficult to maintain a cohesive standard. As shown in Fig. 3, work on the latest amendments tends to take longer than those in the past. However, no alternative to the popular, cheap, and flexible 802.11 technology is visible yet. Quite the contrary, driven by customers' manifold needs, the 802.11 universe continues to expand.

Work on the latest amendments tends to take longer than those in the past. However, no alternative to the popular, cheap, and flexible 802.11 technology is visible yet. Quite the contrary, driven by customers' manifold needs, the 802.11 universe continues to expand.

References

[1] C. A. Rypinski, "Retrospective on Development of Radio and Wire Data Communication," IEEE 802.15 Wireless Next Generation (WNG) Task Group, Submission 06-0107, Mar. 2006; https://mentor.ieee.org/802.15/file/06/15-06-0107-00-wng0-retrospective-radio-wire-data-communication-short.pdf

[2] B. O'Hara and A. Petrick, *The IEEE 802.11 Handbook: A Designer's Companion*, 2nd ed., IEEE, Mar. 2005.

[3] A. Mercier *et al.*, "Adequacy between Multimedia Application Requirements and Wireless Protocols Features," *IEEE Wireless Commun.*, vol. 9, no. 6, Dec. 2002.

[4] L. Eastwood *et al.*, "Mobility Using IEEE 802.21 in a Heterogeneous IEEE 802.16/802.11-Based, IMT-Advanced (4G) Network," *IEEE Wireless Commun.*, vol. 15, no. 2, Apr. 2008.

[5] FCC, "Wireless Operations in the 3650–3700 MHz Band, Rules for Wireless Broadband Services in the 3650–3700 MHz Band," Mar. 2005; http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-56A1.pdf

[6] S. Mangold *et al.*, "Analysis of IEEE 802.11 for QoS Support in Wireless LANs," *IEEE Wireless Commun.*, vol. 10, no. 6, Dec. 2003.

[7] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," *Proc. 7th Int'l. Conf. Mobile Comp. Net.*, Rome, Italy, July 2001.

[8] IEEE P802.11-2007, "IEEE Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local And Metropolitan Area Networks — Specific Requirements — Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications," June 2007.

Additional Reading

[1] B. Walke, S. Mangold, and L. Berlemann, *IEEE 802 Wireless Systems: Protocols, Multi-Hop Mesh/Relaying, Performance and Spectrum Coexistence*, Wiley, Nov. 2006.

[2] S. Vaughan-Nichols, "Will the New Wi-Fi Fly?" *IEEE Computer*, vol. 39, no. 10, Oct. 2006.

Biographies

GUIDO R. HIERTZ (hiertz@ieee.org) received his Dipl.-Ing. degree in electrical engineering from RWTH Aachen University. Working toward his Ph.D. in the Department of Communication Networks, he contributed to various research projects and authored several papers at IEEE conferences. He is a voting member of IEEE 802.11 and a charter member of the industry forum Wi-Mesh Alliance that created the initial draft of IEEE 802.11s jointly with the industry group SEE-Mesh. Since 2009 he is head of research and development of the rental series department at Riedel Communications, Wuppertal, Germany.

DEE DENTENEER received an M.Sc. in statistics from the University of Utrecht and a Ph.D. in applied probability (queuing analysis) from Eindhoven University of Technology. In the period 1984–1988 he worked at the Dutch Central Statistical Office, where he designed the Blaise language: a language for questionnaire description. Since 1988 he is employed at Philips Research in Eindhoven, as of 2000 as a principal research scientist. In Philips he has worked on the application of mathematics in various industrial research projects such as MPEG encoding, speech recognition, secure biometrics, and data transmission systems. His current research interest is the performance analysis and standardization of wireless mesh networks.

LOTHAR STIBOR received his Dipl.-Ing. degree in electrical engineering from RWTH Aachen University. Working toward his Ph.D. in the Department of Communication Networks, he contributed to research projects related to vehicular communication (PReVENT, CoCar). His standardization work in the IEEE is focused on IEEE 1609 and IEEE 802.11p, where he made major contributions to wireless access in vehicular environments. His research interest is the design and performance analysis of vehicular ad hoc networks. Since 2008 he works at the Transport Telematics department of TÜV Rheinland InterTraffic GmbH, Cologne, Germany.

YUNPENG ZANG received his B.Eng. and M.Sc. from Beijing University of Posts and Telecommunications, China, in 1999 and 2002, respectively. From 2003 to 2009 he worked as a research assistant toward his Ph.D. degree in the Department of Communication Networks (ComNets), RWTH Aachen University, Germany. Since 2009 he is with Riedel Communications, Wuppertal, Germany, as a senior research scientist. His current research interests are performance analysis and protocol design for wireless vehicular communication networks, wireless personal area networks, and wireless mesh networks.

XAVIER PÉREZ COSTA is chief researcher at NEC Laboratories Europe, Heidelberg, Germany, where he is responsible for managing several projects related to wireless networks. In the wireless LAN area, he leads a project contributing to 3G/Wi-Fi mobile phones evolution and received NEC's R&D Award for his work on N900iL, NEC's first dual-mode phone. In the WiMAX area he manages a team researching NEC's WiMAX products' future enhancements. In the wireless multihop area he contributes to the EU FP7 project Carrier-Grade Mesh Networks (CARMEN). He has participated in IEEE standardization working groups as well as their corresponding certification bodies and has been included in the major contributor list of IEEE 802.11e and 802.11v. He has served on the program committees of several conferences, including IEEE ICC, WCNC, and INFOCOM, and holds eight patents. He received his M.Sc. and Ph.D. degrees in telecommunications from the Polytechnic University of Catalonia, and was the recipient of the national award for the best Ph.D. thesis on *Multimedia Convergence in Telecommunications* from the Official Association of Telecommunication Engineers (COIT).

BERNHARD H. WALKE is directing the Communication Networks (ComNets) Research Group at RWTH Aachen University, Germany, focusing on 4G air-interface design and performance evaluation as well as developing system-level simulation tools like openWNS. He contributed, together with his Ph.D. students, revolutionary concepts that are being used in standardized mobile radio networks, such as the packet data traffic channel of GPRS operated on a GSM traffic channel and the fast radio link establishment for GPRS (later named TBF), a concept also used in UMTS;the MAC frame applied in WiMAX and 3GPP LTE systems for radio resource allocation; and the concept of fixed decode-and-forward relays used in broadband cellular radio networks like WiMAX and 3GPP LTE/LTE-A. Besides that, his group has contributed a number of improvements now implemented in IEEE 802 standards. His work is published in six textbooks, and about 260 peer-reviewed conference and journal papers. Prior to joining academia, he worked for 18 years in industry at EADS AG. He holds a doctoral degree in information engineering from the University of Stuttgart, Germany.