SYBEX®

Certified Wireless Network Administrator (CWNA) PW0-106

Chapter 5
IEEE 802.11 Standards

Chapter 5 Overview

- Original IEEE 802.11 standard
- IEEE 802.11-2007 ratified amendments
- IEEE 802.11-2012 ratified amendments
- Post-2012 ratified amendments
- IEEE 802.11 draft amendments
- Defunct amendments
- 802.11m Task group

Original IEEE 802.11 Standard

- Published in June 1997
- IEEE Std. 802.11-1997
- Often referred to as 802.11 Prime
- Revised in 1999
- Reaffirmed in 2003 as IEEE Std. 802.11-1999 (R2003)
- March 2007 IEEE Std. 802.11-2007 approved
- March 2012 IEEE Std. 802.11-2012 approved

Original IEEE 802.11 Standard (continued)

- Defined technologies at:
  - Physical layer
  - MAC sublayer of the Data-Link layer
- Defined three Physical layer specifications:
  - Infrared (IR)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
- Radios used license-free 2.4 GHZ ISM band
- Data rates of 1 and 2 Mbps

IEEE 802.11-2007 Ratified Amendments

- IEEE Std 802.11-2007 includes
  - IEEE Std 802.11-1999 (R2003)
  - IEEE Std 802.11a-1999
  - IEEE Std 802.11b-1999
  - IEEE Std 802.11d-2001
  - IEEE Std 802.11g-2003
  - IEEE Std 802.11h-2003
  - IEEE Std 802.11i-2004
  - IEEE Std 802.11j-2004
  - IEEE Std 802.11e-2005

Certified Wireless Network Administrator: CWNA – PW0-106   5

802.11b - 1999

- Published by IEEE Task Group b (TGb)
- IEEE Std. 802.11b-1999/Cor1-2001
- Contained in clause 17 of 802.11-2012 Std.
- Backward compatible with 802.11 DSSS data rates of 1 and 2 Mbps
- Defined *High-Rate DSSS (HR-DSSS)*
- HR-DSSS added 5.5 and 11 Mbps
- 2.4 GHz to 2.4835 GHz ISM band

Certified Wireless Network Administrator: CWNA – PW0-106   6

SYBEX · ®WILEY

802.11b (continued)

- Used different spreading/coding technique called *Complementary Code Keying (CCK)*
- Used spreading technique called the Barker code
- Defined optional *Packet Binary Convolutional Code (PBCC)*

Certified Wireless Network Administrator: CWNA – PW0-106   7

SYBEX · ®WILEY

802.11a - 1999

- Published by IEEE Task Group a (TGa)
- IEEE Std. 802.11a-1999
- Contained in clause 18 of 802.11-2012 Std.
- Not backward compatible with 802.11
- Defined *Orthogonal Frequency Division Multiplexing (OFDM)*
- OFDM supported eight data rates; 6, 9, 12, 18, 24, 36, 48, and 54 Mbps

Certified Wireless Network Administrator: CWNA – PW0-106   8

SYBEX   **WILEY**

802.11a - 1999 (continued)

- Operated in less crowded 5 GHz bands
- Operated in three *Unlicensed National Information Infrastructure (UNII)* bands
- Total of 12 channels, 4 in each band
- Each band is 100 Mhz wide
- 802.11a devices were not readily available until almost two years after ratification
- OFDM chipsets were quite expensive

SYBEX   **WILEY**

802.11g - 2003

- Published by IEEE Task Group a (TGg)
- IEEE Std. 802.11g-2003
- Contained in clause 19 of 802.11-2012 Std.
- Backward compatible with 802.11 DSSS and 802.11b HR-DSSS
- Defined *Extended Rate Physical (ERP)*

SYBEX ®**WILEY**

802.11g -1999 (continued)

- ERP supported eight data rates; 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 2.4 GHz to 2.4835 GHz ISM band
- Heavily adopted in home, SOHO, and enterprise markets
- Introduced protection mechanism to coexist with earlier 802.11 technologies

Certified Wireless Network Administrator: CWNA – PW0-106   11

SYBEX ®**WILEY**

802.11d - 2001

- IEEE Std. 802.11d-2001
- Allowed 802.11 equipment to operate in areas not served by the original standard
- Country code information is delivered in fields in the beacon and probe response frames
- Ensures devices abide by a country's frequency and power regulations

Certified Wireless Network Administrator: CWNA – PW0-106   12

SYBEX **WILEY**

802.11h - 2003

- IEEE Std. 802.11h-2003
- Defined *dynamic frequency selection (DFS)*
- Defined *transmit power control (TPC)*
- Originally proposed to allow 5 GHz operation in Europe and to detect and avoid interference with 5 GHz satellite and radar
- Introduced new UNII-2 Extended band
- 11 additional channels

SYBEX **WILEY**

UNII Bands

Band Frequency range	Amendment	Channels
UNII-1 (lower) 5.150-5.250 GHz	802.11a	4
UNII-2 (middle) 5.250-5.350 GHz	802.11a	4
UNII-2 Extended 5.470-5.725 GHz	802.11h	11
UNII-3 (upper) 5.725-5.825 GHz	802.11a	4

Dynamic Frequency Selection (DFS)

- Required for radio cards in the UNII-2 and UNII-2 Extended bands
- Avoidance of radar systems mandated by *European Radiocommunications Committee (ERC)* and *Federal Communications Commission (FCC)*
- Essentially radar-detection and radar-interference avoidance technology
- Used to satisfy regulatory requirements

Transmit Power Control (TPC)

- Used to regulate the power levels used by OFDM radios in the 5 GHz frequency bands
- ERC mandates that radios use TPC to abide by a maximum regulatory transmit power
- DFS and TPC information is exchanged between clients and APs inside management frames

---

SYBEX   **WILEY**

802.11i - 2004

- IEEE Std. 802.11i-2004
- *Wired Equivalent Privacy (WEP)* was introduced with 802.11 in 1997
- Original standard defined two methods of authentication (neither was effective)
  - Open System authentication (allows all access)
  - Shared Key authentication (has security risks)
- WEP was cracked around 2001
- 802.11i finally defined stronger encryption and better authentication methods

Certified Wireless Network Administrator: CWNA – PW0-106   17

SYBEX   **WILEY**

802.11i - 2004 (continued)

- Major security enhancements addressed
  - Data Privacy using stronger encryption
    - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
    - Uses Advanced Encryption Standard (AES) algorithm
    - Optional support for Temporal Key Integrity Protocol (TKIP)
    - Uses RC-4 steam cipher algorithm (enhancement of WEP)
  - Authentication using 802.1X with *Extensible Authentication Protocol (EAP)* or preshared keys (PSKs)
  - Robust Security Network (RSN)

Certified Wireless Network Administrator: CWNA – PW0-106   18

802.11i (continued)

- *Wi-Fi Alliance's Wi-Fi Protected Access 2 (WPA2)* certification is a mirror of the 802.11i amendment
- *Wi-Fi Protected Access (WPA)* version 1 was a preview of 802.11i
  - Introduced in 2002
  - Used TKIP instead of CCMP/AES
  - Was designed as an interim solution until 802.11i was ratified

---

802.11j - 2004

- IEEE Std. 802.11j-2004
- Designed to obtain Japanese regulatory approval
- Enhanced 802.11 MAC and 802.11a PHY to operate in Japanese 4.9 GHz and 5 GHz bands
- 4.9 - 5.091 GHZ and 5.15 - 5.25 GHz
- Includes option of using 10 MHz wide OFDM channels instead of 20 MHz, resulting in data rates of 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps

802.11e - 2005

- IEEE Std 802.11e-2005
- Defines Layer 2 MAC methods need to meet quality of service (QoS) requirements
- *Hybrid Coordination Function (HCF)* was introduced with 802.11e
- HCF has two access methods to provide QoS
  - Enhanced Distributed Channel Access (EDCA) – An extension of DCF
  - Hybrid Coordination Function Controlled Channel Access (HCCA) – An extension of PCF
- Wi-Fi Alliance QoS certification is known as Wi-Fi Multimedia (WMM)

IEEE Std 802.11-2012

Includes the following
- IEEE 802.11-2007
- IEEE Std 802.11r-2008
- IEEE Std 802.11k-2008
- IEEE Std 802.11y-2008
- IEEE Std 802.11w-2009
- IEEE Std 802.11n-2009
- IEEE Std 802.11p-2010
- IEEE Std 802.11z-2010
- IEEE Std 802.11u-2011
- IEEE Std 802.11v-2011
- IEEE Std 802.11s-2011

Clause renumbering

IEEE Std 802.11-2007	IEEE Std 802.11-2012
Clause 1	Clause 1
Clause 2	Clause 2
Clause 3	Clause 3
Clause 4	Clause 3.3
Clause 5	Clause 4
Clause 6	Clause 5
Clause 10	Clause 6
802.11u: Clause 11B	Clause 6.4
Clause 12	Clause 7
Clause 13	Clause 7.4

Clause renumbering (cont)

IEEE Std 802.11-2007	IEEE Std 802.11-2012
Clause 7	Clause 8
Clause 9	Clause 9
Clause 11	Clause 10
Clause 8	Clause 11
802.11w: Clause 11A	Clause 12
802.11s: Clause 11C	Clause 13
Clause 14	Clause 14
Clause 16	Clause 15
Clause 15	Clause 16
Clause 18	Clause 17
Clause 17	Clause 18
Clause 19	Clause 19
802.11n: Clause 20	Clause 20

SYBEX **WILEY**

802.11r - 2008

- IEEE Std. 802.11r-2008
- Known as *fast basic service set transition (FT)*
- Commonly referred to as fast secure roaming
- Defines faster handoffs between APs using *robust secure network (RSN)*
- Proposed due to time restraints of roaming for applications such as VoWiFi

SYBEX **WILEY**

802.11k - 2008

- IEEE Std. 802.11k-2008
- Provides a means of *radio resource measurement (RRM)*
- Defines mechanism in which client station resource data is gathered and processed by an AP or controller
- Client can also request information
- Key radios resource measurements
  - Transmit Power Control (TPC)
  - Client Statistics
  - Channel Statistics
  - Neighbor Reports
- Most features are not yet supported on clients

SYBEX ⊛WILEY

802.11y - 2008

- IEEE Std. 802.11y-2008
- Allows high-powered operations in 3650 MHz to 3700 MHz licensed band in the U.S.
- Requires content-based protocol mechanisms to avoid interference between devices (CSMA/CA can normally provide this)
- If CSMA/CA is insufficient, *dynamic STA enablement (DSE)* procedures can be used

Certified Wireless Network Administrator: CWNA – PW0-106   27

SYBEX ⊛WILEY

802.11w - 2009

- IEEE Std. 802.11w-2009
- Designed to deliver management frames in a secure manner
- 802.11w frames are referred to as *robust management frames*
- Goal is to prevent management frames from being spoofed and prevent *denial-of-service attacks (DoS attacks)*
- Provides protection for unicast, broadcast, and multicast management frames

Certified Wireless Network Administrator: CWNA – PW0-106   28

802.11n - 2009

- IEEE Std. 802.11n-2009
- Designed to increase throughput in both the 2.4 GHz and 5 GHz frequency bands
- Defines *High Throughput (HT)*
- Provides PHY and MAC enhancements
- Data rates up to 600 Mbps
- Defined as clause 20
- Uses MIMO technology

802.11p - 2010

- 802.11p
    - Define enhancements to support *Intelligent Transportation Systems (ITS)* applications
    - Licensed 5.9 GHz ITS band
    - Speeds up to 200 kph (124 mph)
    - 1000 meter range
    - Known as *Wireless Access in Vehicular Environments (WAVE)*

802.11z - 2010

- IEEE Std. 802.11z-2010
- Designed to establish and standardize a *Direct Link Setup (DLS)* mechanism
- Historically all inter-client traffic had to traverse an AP
- DLS allows clients to communicate directly with other clients
- Slow to be implemented

802.11u - 2011

- IEEE Std. 802.11u-2011
- Addresses interworking issues between 802.11 network and external networks
- Referred to a *Wireless Interworking with External Networks (WIEN)*
- Defines functions and procedures for aiding network discovery and selection by STAs, information transfer from external networks using QoS mapping, and a general mechanism for the provision of emergency services

---

802.11v - 2011

- IEEE Std. 802.11v-2011
- Provides the ability to configure client stations wireless from a central management point
- Defines *Wireless Network Management (WNM)*
- Clients and APs use WNM to exchange operational data, making clients more cognizant of the state and topology of the network
- Devices can exchange location information, support multiple BSSIDs, and offers new WNM-Sleep mode

802.11s - 2011

- IEEE Std. 802.11s-2011
- Designed to standardize mesh networking
- Mesh devices include
  - Mesh point (MP)
  - Mesh access point (MAP)
  - Mesh point portal (MPP)
- Uses mesh routing protocol call *Hybrid Wireless Mesh Protocol (HWMP)*
- Vendors can also use proprietary routing protocols and metrics

9/28/2015

802.11s - 2011

Certified Wireless Network Administrator: CWNA – PW0-106 35
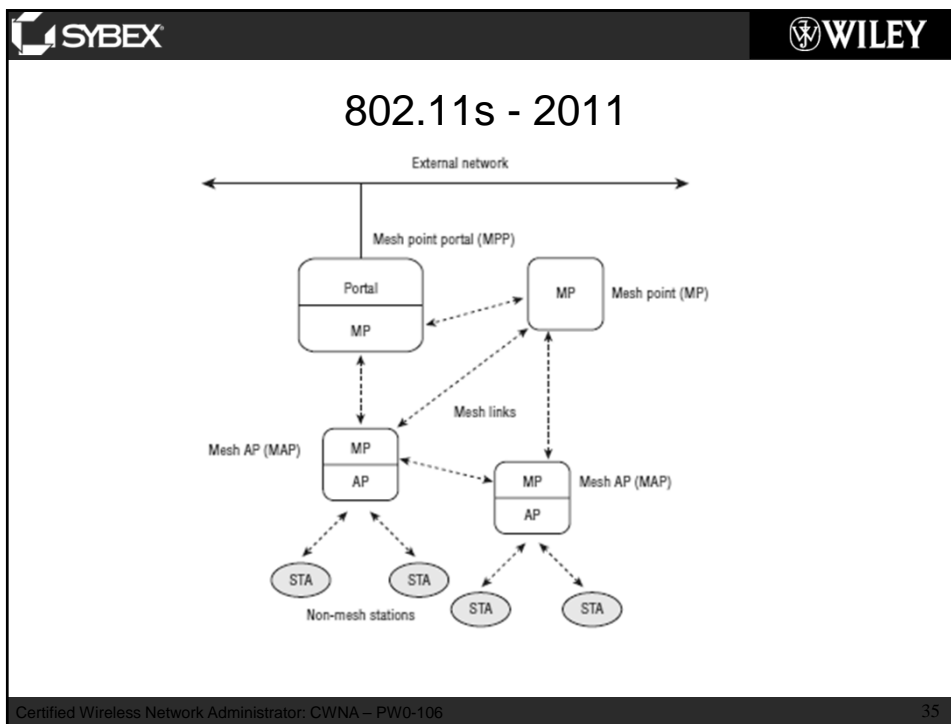
Post 2012 Ratified Amendments

- 802.11ae - 2012
  – Specifies enhancement to QoS management
- 802.11aa - 2012
  – Specifies enhancements to the MAC for robust audio video streaming while coexisting with other traffic.
- 802.11ad - 2012
  – Defines *Very High Throughput (VHT)* enhancements
  – Using higher frequency 60 GHz band
  – Potentially up to 7 Gbps
  – Significantly less range
  – May also require new encryption mechanisms due to higher data rates

Certified Wireless Network Administrator: CWNA – PW0-106 36

SYBEX ®WILEY

Post 2012 Ratified Amendments (continued)

- 802.11ac
  - Goal of throughput above 1 Gbps
  - Will define *Very High Throughput (VHT)*
  - Uses 5 GHz bands
  - Wider channels – 80 MHz and 160 MHz
  - New modulation – 256-QAM
  - More spatial streams – up to 8
  - Improved MIMO and beamforming – uses mu-MIMO and null data packet beamformimg

Certified Wireless Network Administrator: CWNA – PW0-106   37

SYBEX ®WILEY

Post 2012 Ratified Amendments (continued)

- 802.11af
  - Allows the use of Wi-Fi in the newly opened TV whitespace frequencies between 54 MHz and 790 MHz
  - Lower frequencies would require lower data rates
  - Potential for long-distance outdoor transmissions

Certified Wireless Network Administrator: CWNA – PW0-106   38

IEEE 802.11 Draft Amendments

- 802.11ah
  - Defining the use of Wi-Fi in frequencies below 1 GHz
  - Would have greater range
  - Can enhance Internet-of-things (IoT) or Machine – to-Machine (M2M) communication
- 802.11ai
  - Goal is to provide a fast initial link setup (FILS). This technology could allow a STA to establish a secure link setup in less than 100 ms.

IEEE 802.11 Draft Amendments

- 802.11aj
  - Provides modifications to the IEEE 802.11ad-2012 amendment's PHY and MAC layer to provide support for operating in the Chinese Milli-Meter Wave (CMMW) frequency bands
- 802.11ak
  - also referred to as General Link (GLK).
  - enhancement to 802.11 links for use in bridged networks
  - aims to simplify the use of 802.11 between access points and wireless stations,
  - allowing the stations to provide bridging services.

IEEE 802.11 Draft Amendments

- 802.11aq - enables delivery of network service information prior to the association of stations on an 802.11 network. This amendment hopes to be able to allow advertisement of services to stations prior to the stations' actual association to the network.

Defunct Amendments

- IEEE Std 802.11F-2003
  - Never ratified, withdrawn in February 2006
  - Attempt to standardize roaming mechanisms
  - Addressed "vendor interoperability" for AP-to-AP roaming.
  - Recommended *Inter-Access Point Protocol (IAPP)*
- IEEE Std 802.11T
  - Tasked to develop performance metrics, measurement methods, and test conditions to measure the performance of wireless equipment
  - Also called Wireless Performance Prediction (WPP)

SYBEX ⊛**WILEY**

802.11m Task Group

- Started in 1999
- Initiative for internal maintenance of the 802.11 standard's technical documentation
- Often referred to as *802.11 housekeeping*
- Also responsible for "rolling up" ratified amendments into a published document

Certified Wireless Network Administrator: CWNA – PW0-106   43

SYBEX ⊛**WILEY**

Chapter 5 Summary

- Original IEEE 802.11 standard
- IEEE 802.11-2007 ratified amendments
- IEEE 802.11-2012 ratified amendments
- Post-2012 ratified amendments
- IEEE 802.11 draft amendments
- Defunct amendments
- 802.11m Task group

Certified Wireless Network Administrator: CWNA – PW0-106   44