Self Organizing Networks

WLAN IEEE 802.11

Max Riegel

Lectures overview

June 25th

- Wi-Fi deployments
- Standardization environment
- Wi-Fi system architecture
- Wi-Fi security

July 2nd

- Medium access functions
- MAC layer management frame formats
- Quality of Service

July 9th

- Wi-Fi roaming and Hotspot 2.0
- WLAN management
- Spectrum and wireless channel characteristics

July 16th

- Wi-Fi radio for 2.4 GHz and 5 GHz bands
- WiGig extension for 60 GHz bands
- HaLow extension for below 1GHz bands

WLAN IEEE 802.11

PROLOG

About my person

Max Riegel

<maximilian.riegel@nokia.com>

Dipl.-Ing. (TU)

Nokia Bell Labs - IEEE Standardization

- Job positions
  - prior to 1998
    - Various positions regarding HW and SW development at PKI and TPS
  - 1998 - 2007
    - Responsible for IETF and IEEE Standardization at Siemens Communications
  - since 2007
    - Responsible for IEEE related standardization at NSN/Nokia Networks/Nokia Bell Labs
- Involvement in IEEE 802.11 Standardization since 2000
- Currently voting member of IEEE 802.1 and IEEE 802.11
- Engagement in Wi-Fi Alliance and Wireless Broadband Alliance
- Chaired IEEE 802.1CF project of OmniRAN Task Group

WLAN IEEE 802.11

TABLE OF CONTENT

Topics covered in lecture of June 25th

- Introduction
- WLAN deployments
  - Networking aspects
  - IEEE 802.1CF Architecture
  - WLAN for access to Internet
  - Q&A
- Standardization environment
  - IEEE 802.11 Standardization
  - Standards reference
  - Wi-Fi Alliance certification
- WLAN System architecture
  - WLAN Configurations
  - Protocol architecture
  - Q&A

=== short break ===

- Security
  - List of topics on next slide
  - Q&A

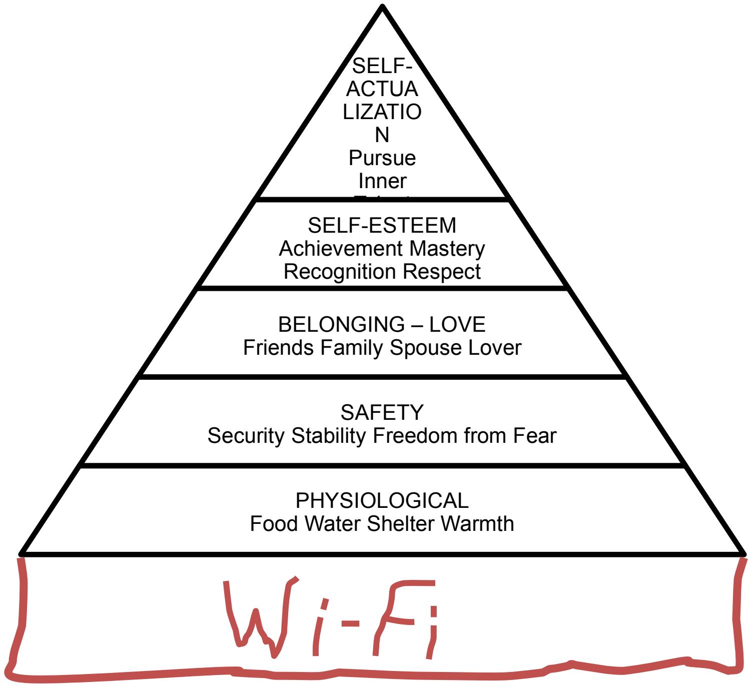
Topics covered in IEEE 802.11 security section

- IEEE 802.11 Security
  - Security evolution
  - Robust security network
    - Configuration
    - PSK/SAE Authentication
    - IEEE 802.1X Authentication
    - Key management
    - Data protection
    - Summary
  - Protected management frames,
  - Fast transition

WLAN IEEE 802.11

INTRODUCTION

Consumer expectations on Wi-Fi (aka 'WLAN' in Europe)



The hierarchy of human needs

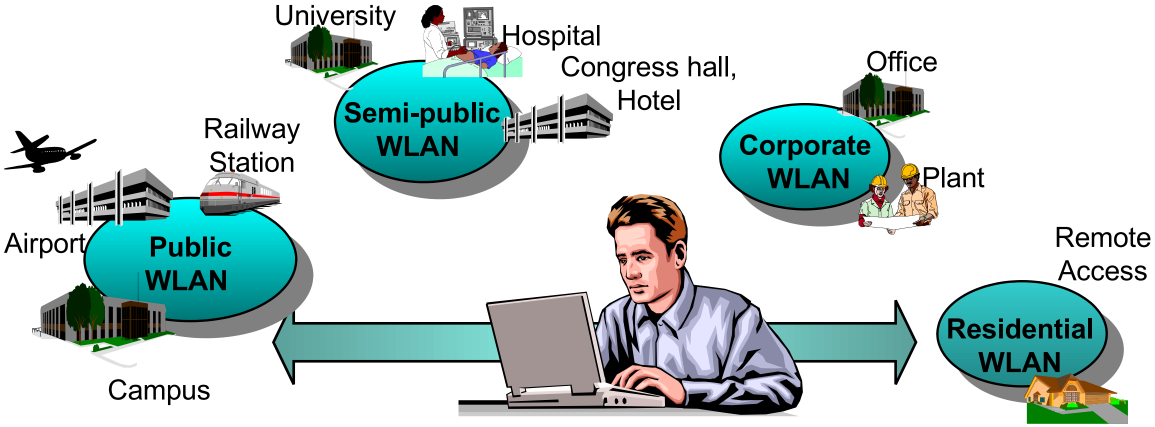
- Wi-Fi is becoming considered a basic need like food, water, shelter and warmth
  - In a couple of years all households will have Wi-Fi
- Free-of-charge Wi-Fi access is expected in public venues, hotels, coffee shops, shopping malls, airports, stations, trains, busses,…
  - Charged access may still be accepted for premium locations or premium services
- Quality of 'free-of-charge' Wi-Fi access is becoming a differentiator for selecting goods and services
  - e.g. customers will avoid to stay in hotels with bad 'free' Wi-Fi

WLAN IEEE 802.11

WLAN DEPLOYMENTS

The ubiquitous WLAN

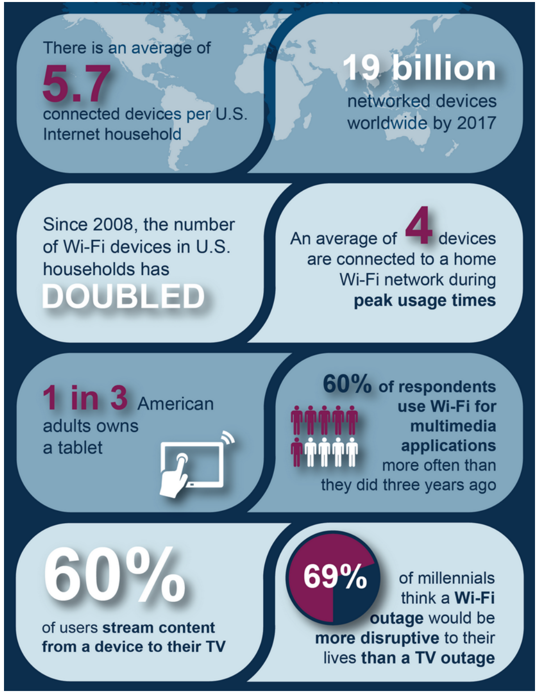
- Today everybody requires access to the Internet everywhere.
- Wi-Fi is more than just cable replacement, it provides hassle-free broadband Internet access everywhere.



- Coverage in ‘hot-spots’ is mostly sufficient.
- Wi-Fi meets the expectations for easiness, cost and bandwidth.

Diversity of Wi-Fi terminals and access infrastructure

Wi-Fi is predominantly deployed in homes and indoors



There is an average of **5.7** connected devices per U.S. Internet household

19 billion networked devices worldwide by 2017

Since 2008, the number of Wi-Fi devices in U.S. households has **DOUBLED**

An average of **4** devices are connected to a home Wi-Fi network during **peak usage times**

1 in 3 American adults owns a tablet

60% of respondents **use Wi-Fi for multimedia applications** more often than they did three years ago

60% of users **stream content from a device to their TV**

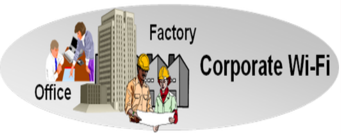
69% of millennials think a **Wi-Fi outage** would be **more disruptive** to their lives than a **TV outage**

Source: WFA, Cisco, Pew Research Center, Wakefield Research

~90%*

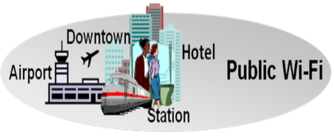
- Currently managed by millions of ‘hobby’ operators
- Most heavy growth of Wi-Fi devices and data traffic
- Public co-use feasible but requires strict separation from privately operated part.

~10%*



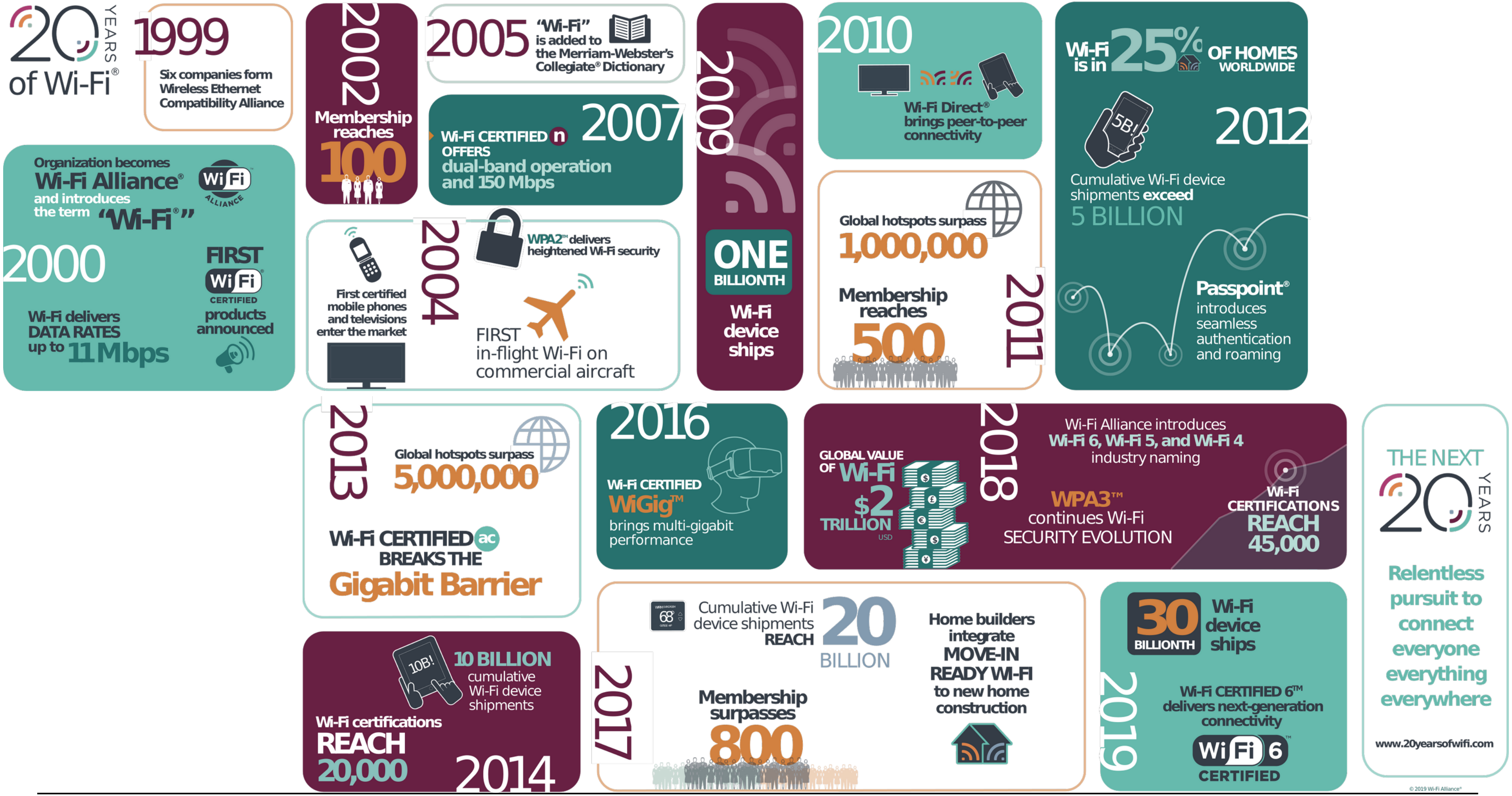
- Managed by corporate IT departments
- Mission critical service with strict security policies in place
- Public access overlays for allowing employees to bring their own devices

<1%*



- Managed by public communication service providers or WISPs
- Cumbersome security and usability due to open Wi-Fi and portals
- Very good business potential in dense deployments

* Percentage of APs in segment; Source: ABIresearch 2010, Femtocells, Operator, Access Point and Chipset Market Analysis



20 YEARS of Wi-Fi®

1999
Six companies form Wireless Ethernet Compatibility Alliance

2000
Organization becomes Wi-Fi Alliance® and introduces the term "Wi-Fi®"

Wi-Fi delivers DATA RATES up to 11 Mbps

FIRST Wi-Fi CERTIFIED products announced

2002
Membership reaches 100

2004
First certified mobile phones and televisions enter the market

WPA2™ delivers heightened Wi-Fi security

FIRST in-flight Wi-Fi on commercial aircraft

2005
"Wi-Fi" is added to the Merriam-Webster's Collegiate® Dictionary

2007
Wi-Fi CERTIFIED n OFFERS dual-band operation and 150 Mbps

2009
ONE BILLIONTH Wi-Fi device ships

2010
Wi-Fi Direct® brings peer-to-peer connectivity

2011
Global hotspots surpass 1,000,000

Membership reaches 500

2012
Wi-Fi is in 25% OF HOMES WORLDWIDE

Cumulative Wi-Fi device shipments exceed 5 BILLION

Passpoint® introduces seamless authentication and roaming

2013
Global hotspots surpass 5,000,000

Wi-Fi CERTIFIED ac BREAKS THE Gigabit Barrier

2014
10 BILLION cumulative Wi-Fi device shipments

Wi-Fi certifications REACH 20,000

2016
Wi-Fi CERTIFIED WiGig™ brings multi-gigabit performance

2017
Cumulative Wi-Fi device shipments REACH 20 BILLION

Membership surpasses 800

Home builders integrate MOVE-IN READY Wi-Fi to new home construction

2018
GLOBAL VALUE OF Wi-Fi $2 TRILLION USD

Wi-Fi Alliance introduces Wi-Fi 6, Wi-Fi 5, and Wi-Fi 4 industry naming

WPA3™ continues Wi-Fi SECURITY EVOLUTION

Wi-Fi CERTIFICATIONS REACH 45,000

2019
30 BILLIONTH Wi-Fi device ships

Wi-Fi CERTIFIED 6™ delivers next-generation connectivity

Wi-Fi 6 CERTIFIED

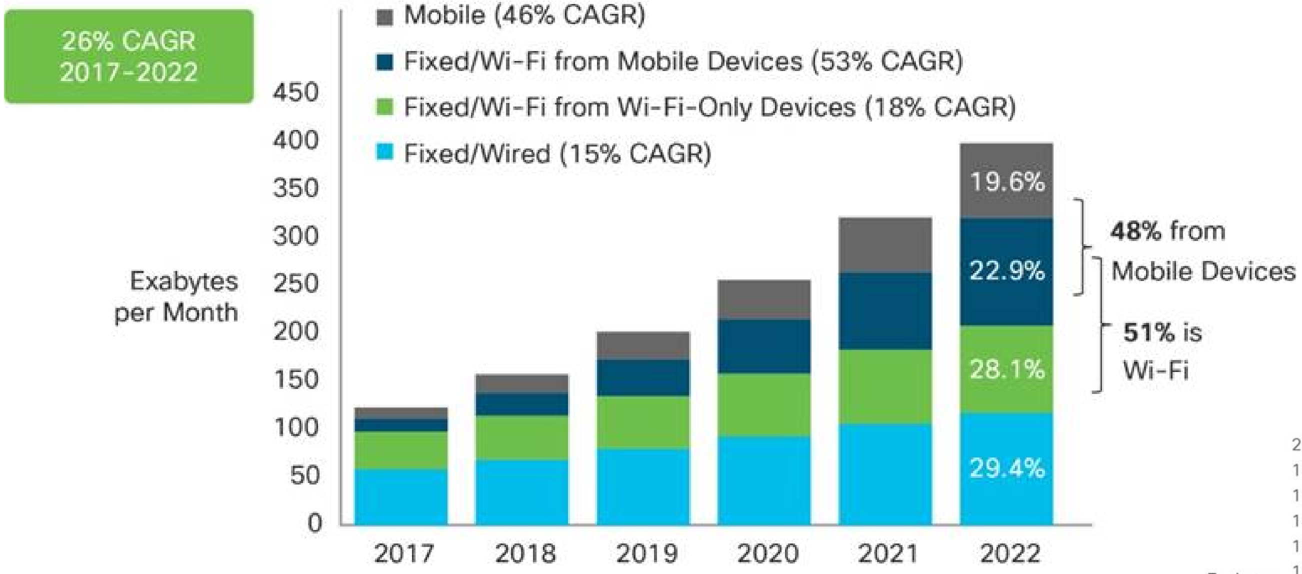
THE NEXT 20 YEARS

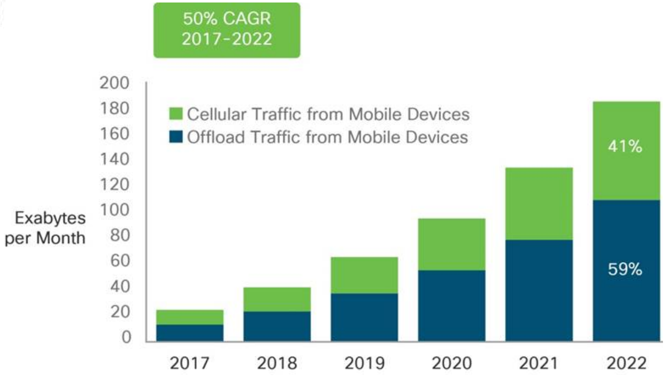
Relentless pursuit to connect everyone everything everywhere

www.20yearsofwifi.com

Wi-Fi is the dominant interface for Internet traffic

… and is serving more data to mobiles than cellular





https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html

Segmenting the Wi-Fi device ecosystem

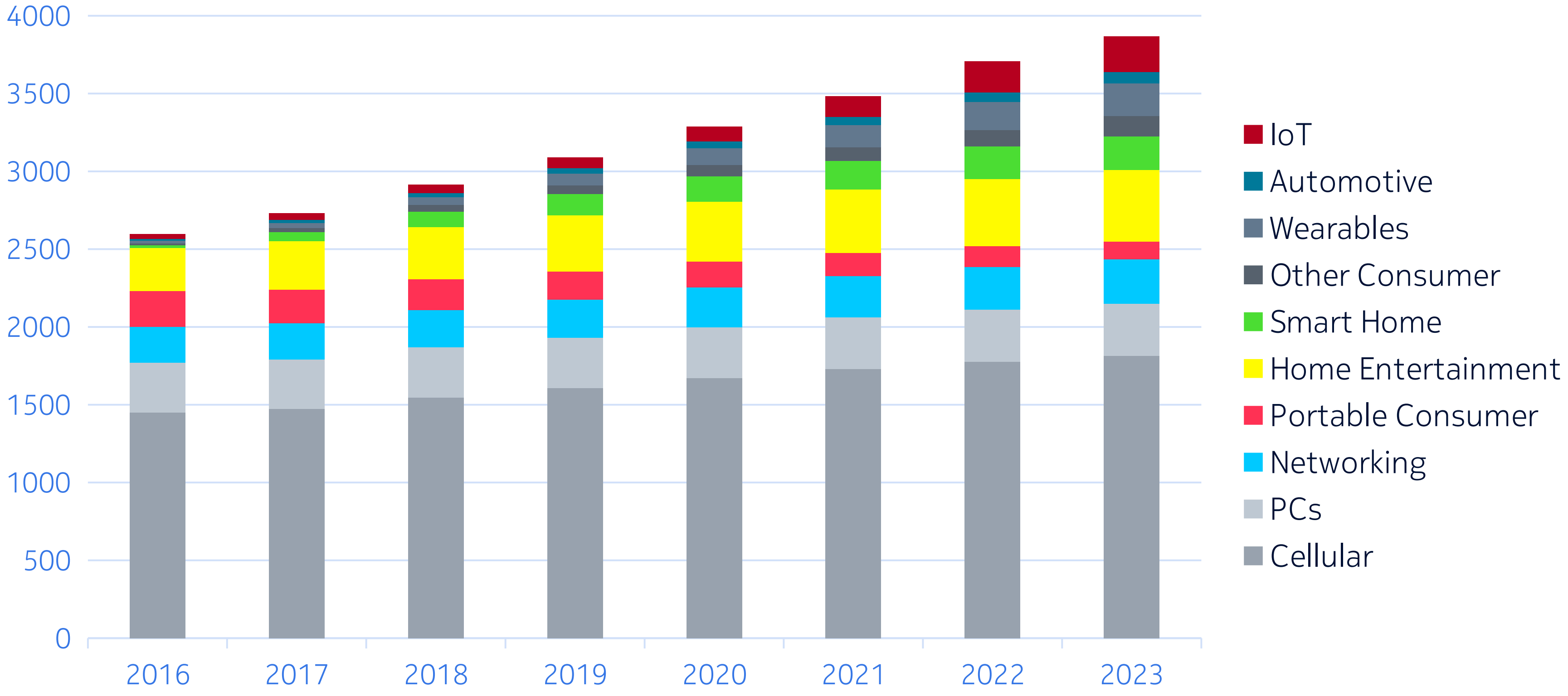
Source: ABI research ‘Wireless Connectivity ICs’ 2018

- Cellular (1474)
  - Smartphones
  - Feature Phones
- PCs (313)
  - Desktop PCs
  - Compute Sticks
  - Traditional Notebooks
  - Ultrabooks
  - Chromebooks
  - PC Accessories
  - Printers
- Networking (235)
  - Consumer APs
  - Consumer External Adapters
  - Enterprise APs
  - Carrier Wi-Fi APs
  - Mobile Hotspot Routers
  - Residential Wi-Fi Mesh Systems
- Portable Consumer (214)
  - Media Tablets
  - White Box Tablets
  - Handheld Gaming
  - Portable Media Players
  - Digital Cameras/ Camcorders
  - eBook Readers
- Home Entertainment (313)
  - Flat Panel TVs
  - DVD/Blu-Ray Players
  - UHD Blu-Ray Players
  - Set-Top Boxes
  - Media Streaming Adapters
  - OEM Remote Controls
  - Gaming Consoles
  - Speakers
  - Digital Photo Frames
- Other Consumer (25)
  - Consumer Robotics
  - Other Consumer Electronics Devices
- Smart Home (59)
  - Home Automation Control
  - Home Automation Devices
  - Residential Smart Lighting
  - Smart Appliances
  - Voice-Control Front Ends
- Wearables (33)
  - Smartwatches
  - Smart Glasses
  - Sports, Fitness, and Wellness Trackers
  - Virtual Reality
  - Wearable Cameras
  - Wearable Scanners
- Automotive (19)
  - In-Car Infotainment
- IoT (43)
  - Smart Cities
  - Healthcare
  - Energy Management
  - Asset Management
  - Video Surveillance
  - Location/Tracking
  - Monitoring/Status
  - Other Value-Added Applications

(Figures) reflect millions shipped Wi-Fi connectivity ICs in 2017

Yearly Wi-Fi device shipments

Source: ABI research ‘Wireless Connectivity ICs’ 2018

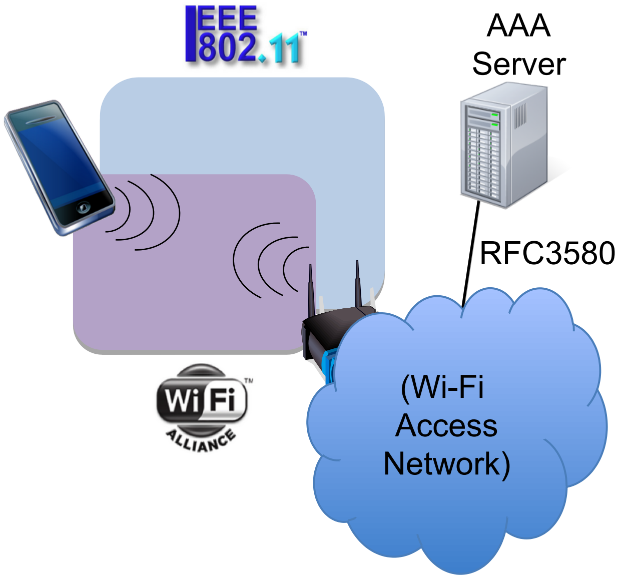


WLAN Deployments

NETWORKING ASPECTS

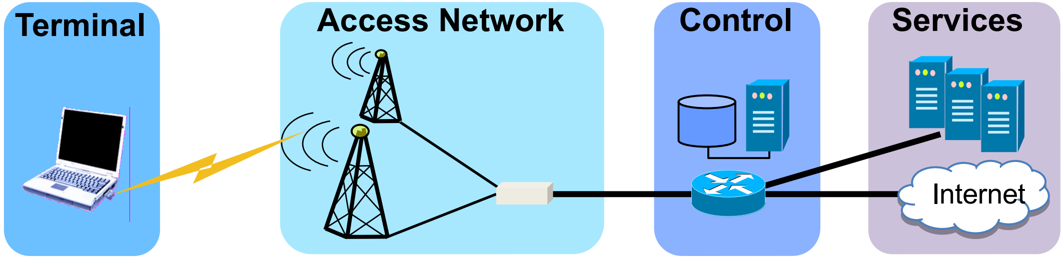
Specification of the Wi-Fi access network

Certified Air Interface, but hardly any standards for network compliance



- The air interface is specified by IEEE 802.11 standards
- Wi-Fi Alliance ensures compliance on the air interface by certification
- IETF RFC3580 (IEEE 802.1X RADIUS usage Guidelines) defines the interface between the WLAN Access Point and the AAA server.
- There is no normative architecture specification for the WLAN access network
  - But IEEE 802.1CF provides a good description.

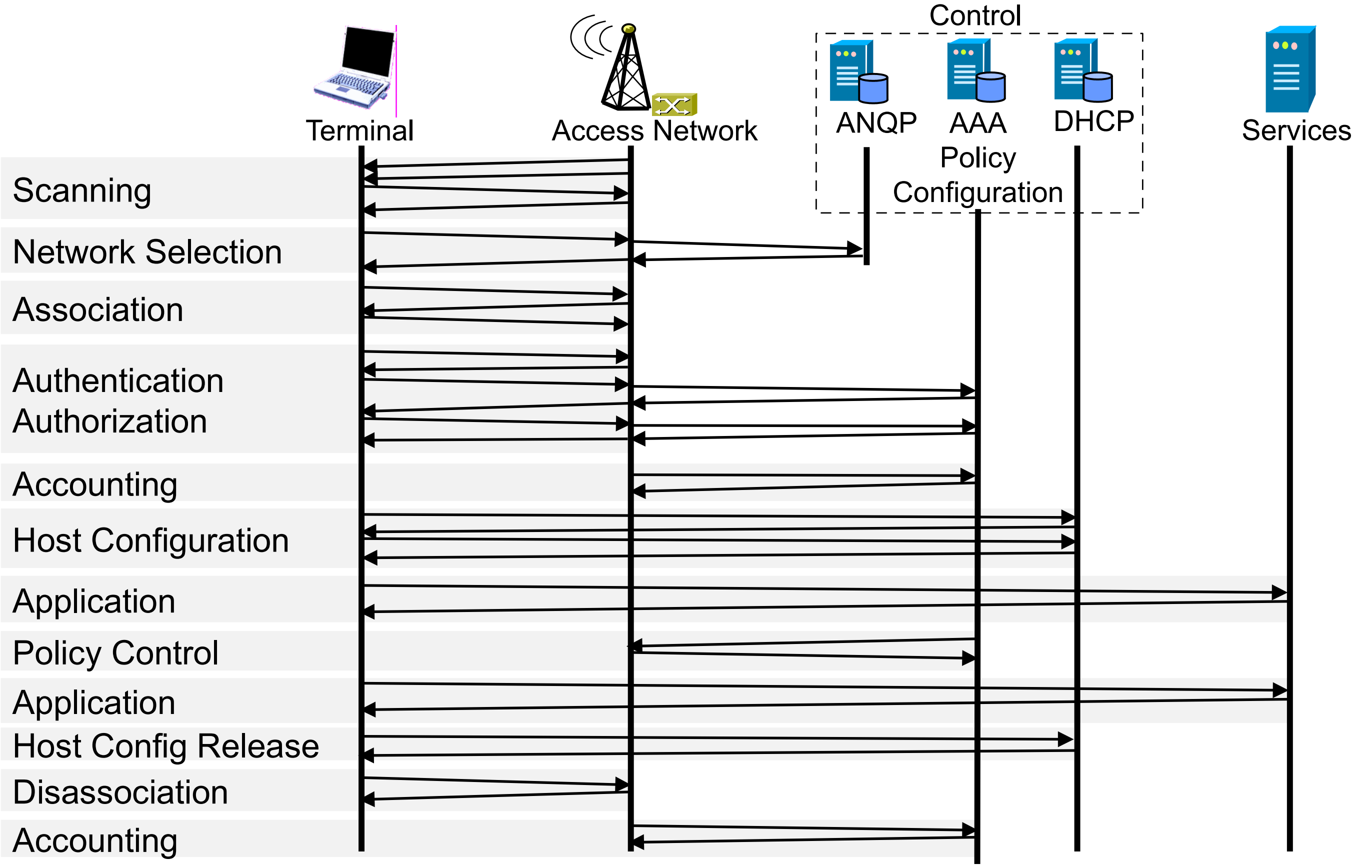
Wireless communication network structure



Communication networks supporting dynamic attachment of terminals are usually structured into

- Terminal
  - Communication endpoint towards the consumer and subscriber of communication services
- Access Network
  - Distributed infrastructure for aggregation of multiple network access interfaces into a common interface
- Control and IP connectivity
  - Infrastructure for control and management of network access and end-to-end IP connectivity
- Services
  - Infrastructure for providing services over IP connectivity

Access network control plane functions



Functional decomposition of wireless network access

Access Network

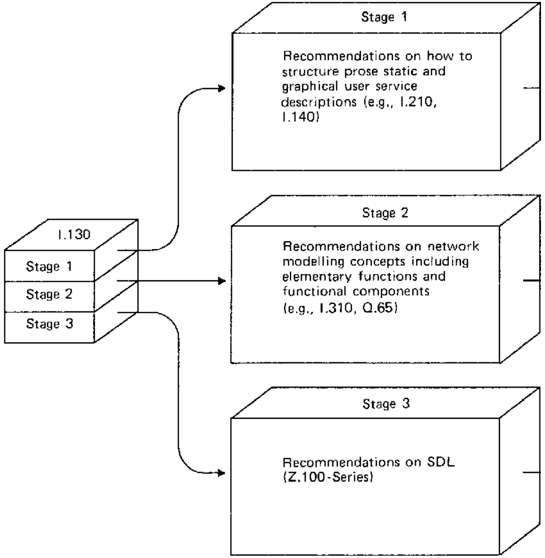
- Network advertisement
- Pre-association signaling
- Authentication, authorization and accounting client
- L2 session establishment
  - w/ QoS and Policy Enforcement
- L2 mobility management inside access networks
- Traffic forwarding to core based on L2 addresses

Control and IP connectivity

- Subscription management
- Terminal provisioning
- Authentication, authorization and accounting server
- IP address management
- IP connectivity establishment to Internet and services
- Policy & QoS management server (policy decision)
- Mobility Anchor
- Roaming support to other cores

Network protocol specification in 3 stages

- ITU-T defined in its Rec. I.130 a sequential 3 stage process for the specification of the Integrated Services Digital Network (ISDN)
- It is nowadays commonly used for telecommunication network standardization.



Stage 1

Recommendations on how to structure prose static and graphical user service descriptions (e.g., I.210, I.140)

Stage 2

Recommendations on network modelling concepts including elementary functions and functional components (e.g., I.310, Q.65)

Stage 3

Recommendations on SDL (Z.100-Series)

Specify requirements
from the user's perspective;

⬇

Develop a logical/functional model
to meet those requirements;

⬇

Develop a detailed specification
of the protocols and attributes.

More Information:
ETSI: *Making Better Standards*
http://docbox.etsi.org/MTS/MTS/10-PromotionalMaterial/MBS-20111118/protocolStandards/stagedApproach.htm

WLAN Deployments

IEEE 802.1CF ARCHITECTURE

IEEE 802.1CF: Specification of IEEE 802 access network

- IEEE Std 802.1CF-2019 provides an access network model for IEEE 802:
  - ‘External’ requirements from the service/deployment perspective

    ⇕ ?

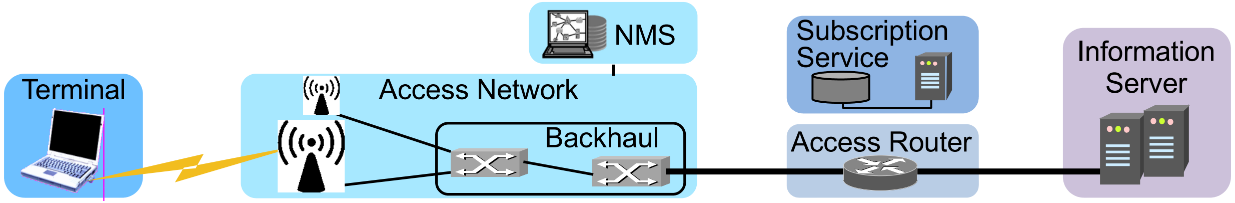
  - Develop a logical/functional model for evaluation of those requirements;

    ↑

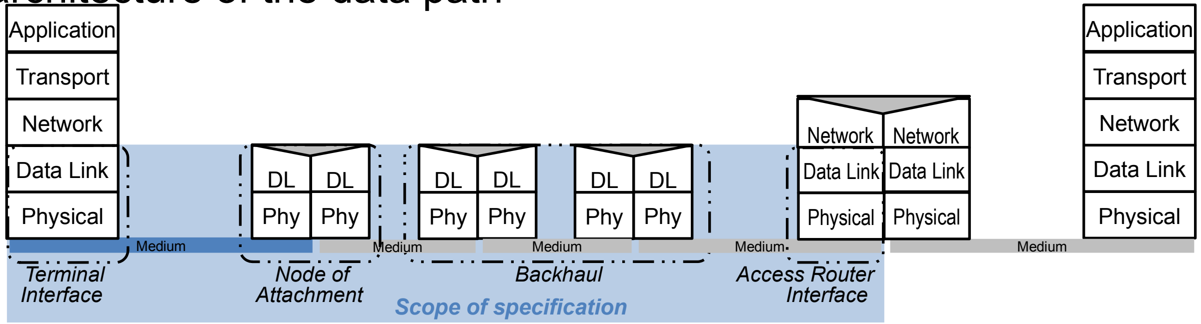
  - Available IEEE 802 specifications of protocols and attributes.
- A functional network specification based on an abstract network model enables evaluation and better understanding of existing IEEE 802 protocols for deployment in access networks.
- It illustrates commonalities among IEEE 802 access technologies while supporting specifics of individual technologies.
- The access network model facilities broader deployment of IEEE 802 specifications.

Network Reference Model

- Core functional entities were identified from a common topology figure of an access infrastructure



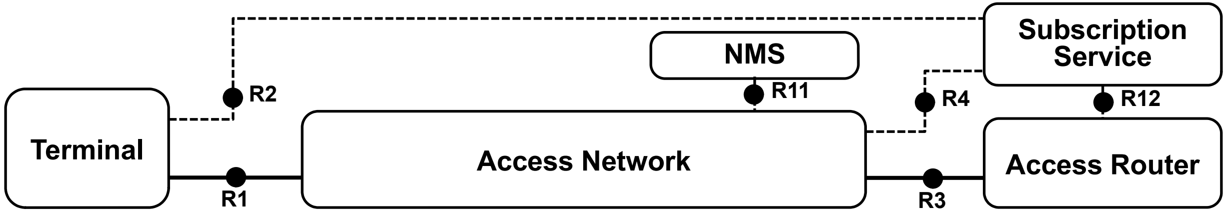
- The portion of the access infrastructure in scope of IEEE 802 was defined according to the protocol layer architecture of the data path



- IEEE 802 access network describes the layer 2 network between terminal and access router implemented through IEEE 802 technologies.

Network Reference Model basics

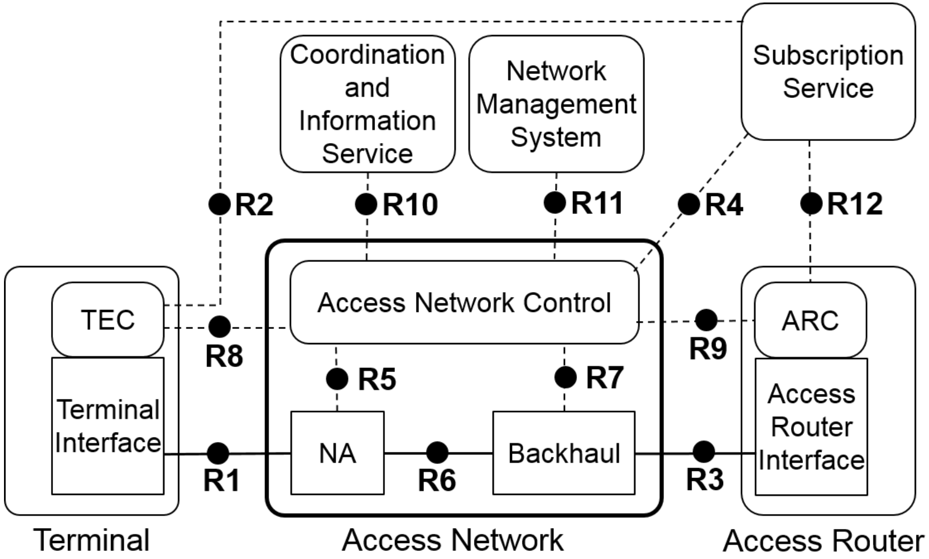
- The NRM denotes the functional entities and their relation to each others



- Functional entities represented by rounded rectangles
- Relations are shown by reference points indicating interfaces
  - Reference points are denoted through R…
    - Total of 12 reference points in the model
  - Two different kind of reference points
    - Forwarding path of Ethernet frames
      - Represented by solid lines
    - Control interfaces
      - Represented by dotted lines

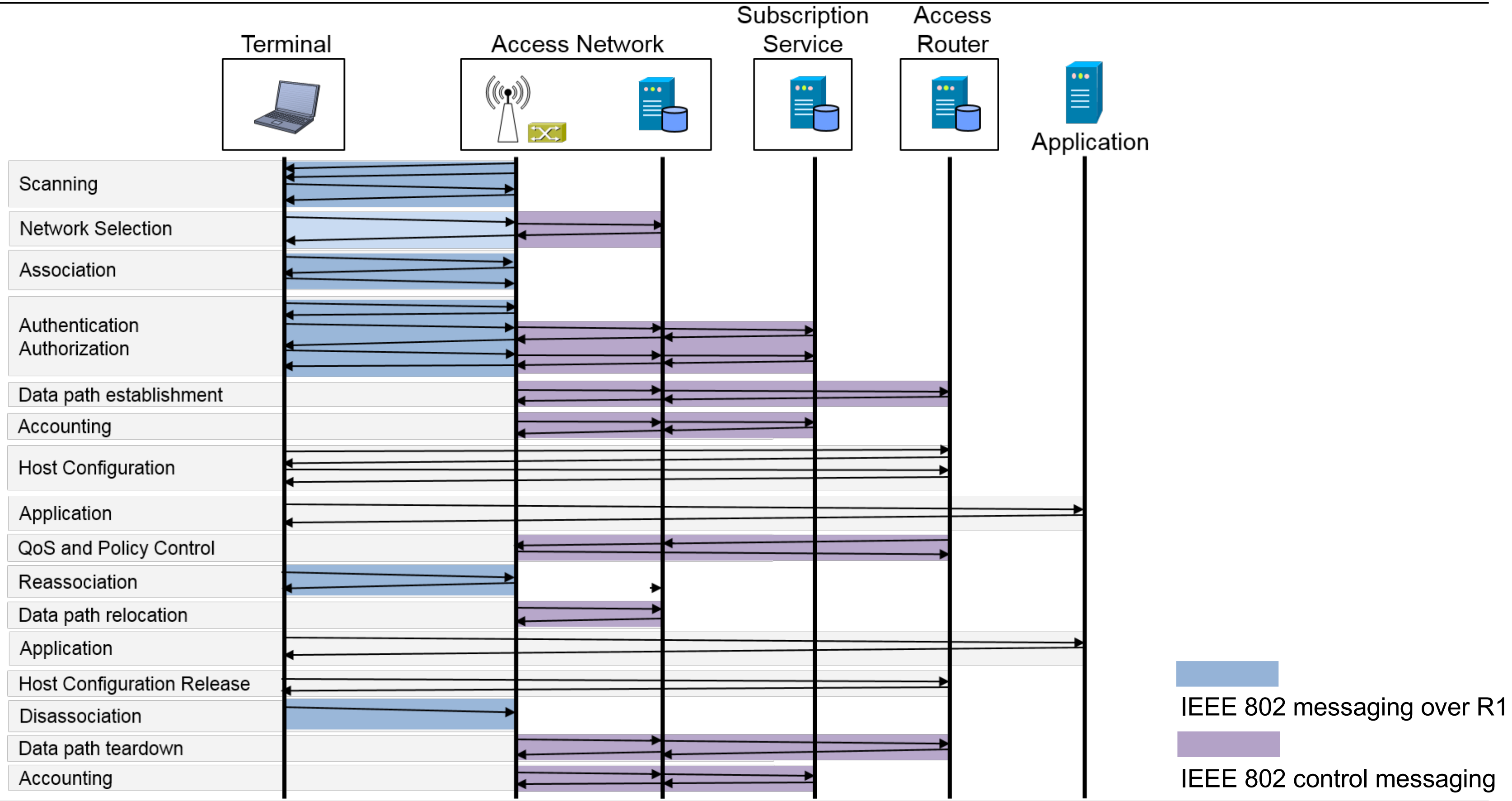
IEEE 802 Access Network Reference Model

- Comprehensive NRM shows highest level of details

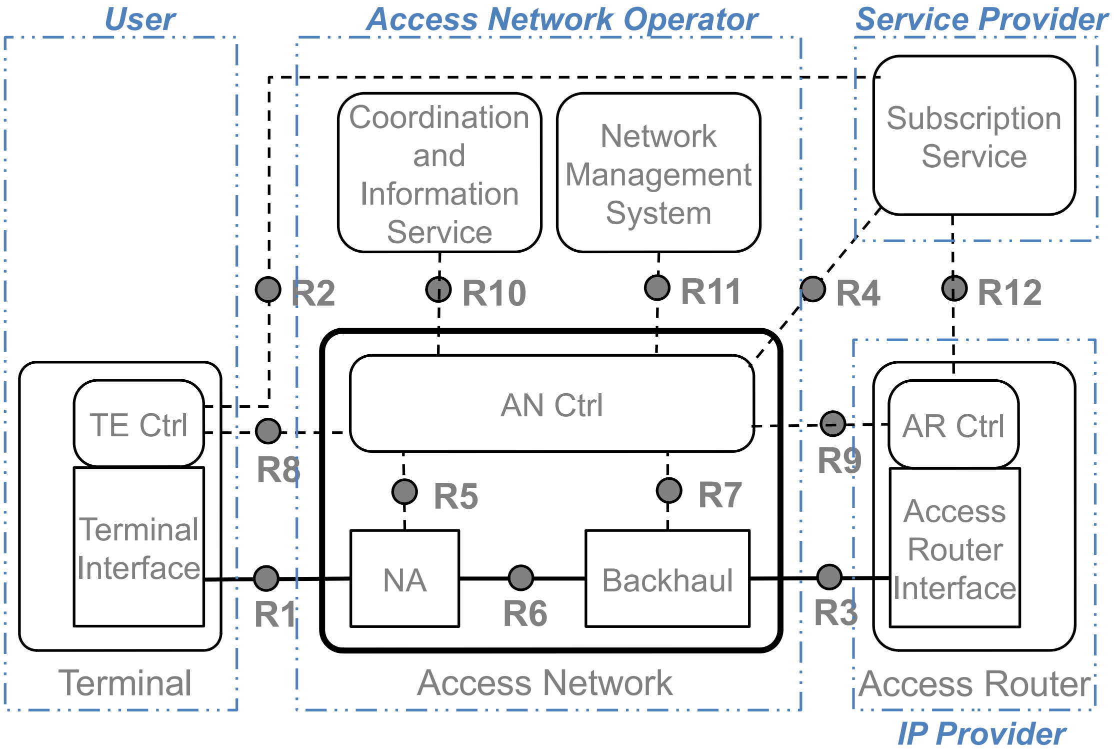


- NRM represents an abstract view on an access network
  - For the purpose to define interfaces
- Control interfaces cover only attributes related to IEEE 802
  - Protocol details on control interfaces are out of scope

The life-cycle of an IEEE 802 session

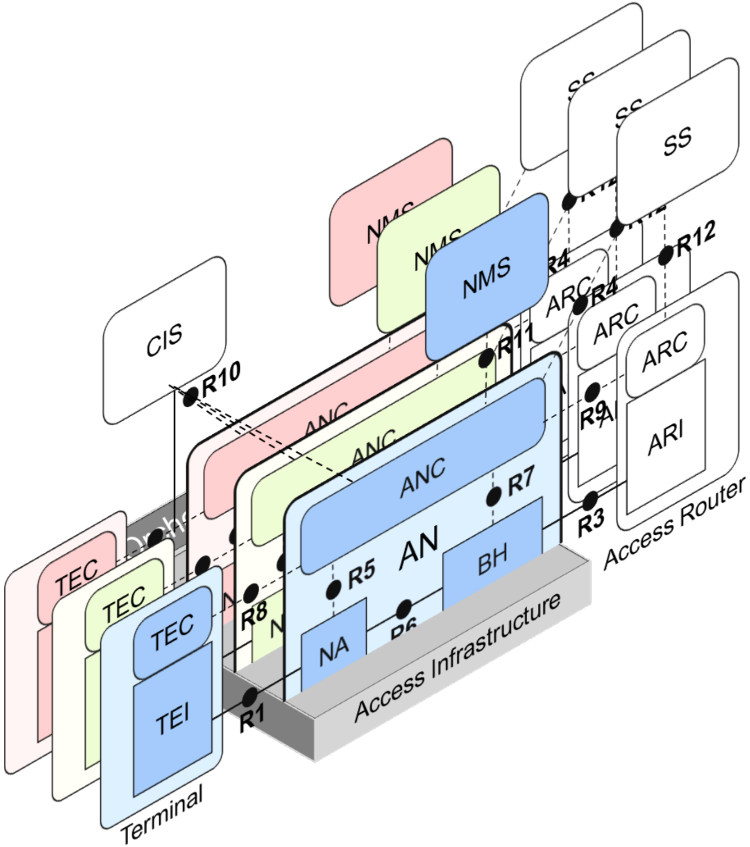


Generic operational roles of IEEE 802 access network



- Operational roles define independent security and privacy domains

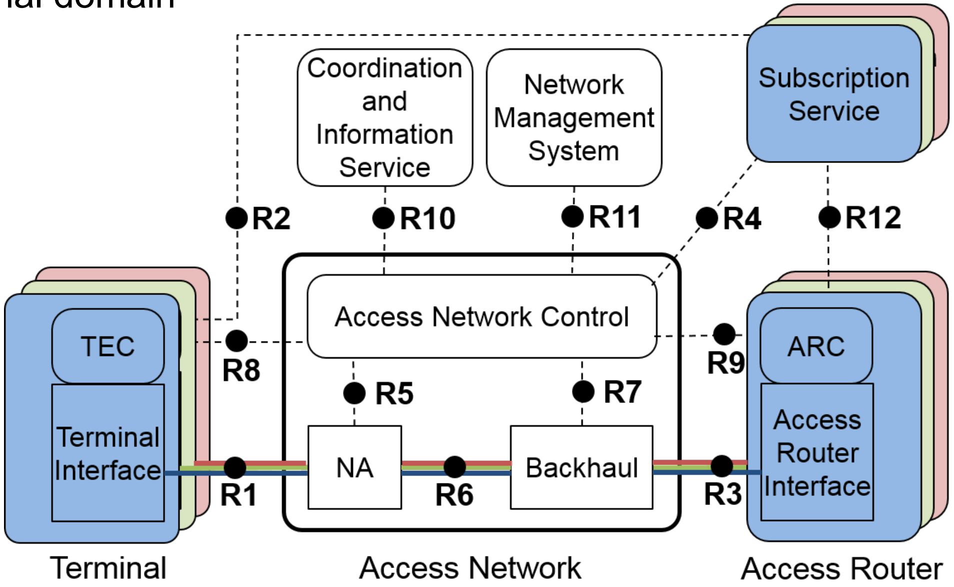
Network virtualization: Virtualized networks



- The NRM provides the foundation to specify virtualized access networks.
  - The NRM defines a single, independent instance
  - Multiple instances coordinate themselves via CIS
  - CIS is a function owned by the orchestrator of the access infrastructure
  - Each instance builds its own operational domain
- Virtualization is a common functionality of IEEE 802 access network

The lesser virtualization: Virtual Networks aka Network Slicing

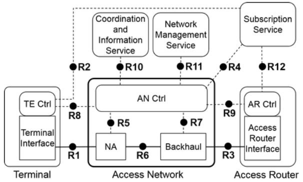
- VLANs provide separate datapaths under a common control
  - Single operational domain

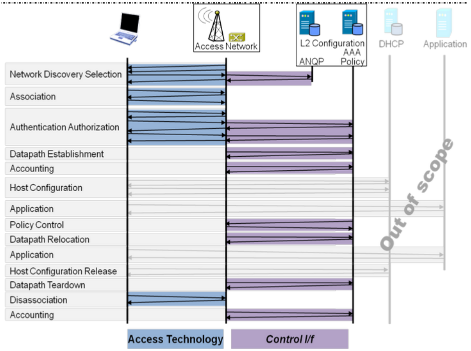


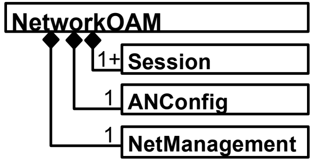
  - BTW: ‘5G network slicing’ is more like virtual networks
    - Service differentiation through separate datapaths

IEEE Std 802.1CF-2019 table of content

- Overview
- References, definitions, acronyms and abbreviations
- Conformance
- Network Reference Model
  - Basic concepts and terminology
  - Overview of NRM
  - Basic, enhanced and comprehensive NRM
  - Deployment scenarios
- Functional Design and Decomposition
  - Access Network Setup
  - Network Discovery and Selection
  - Association and Disassociation
  - Authentication and Trust Establishment
  - Datapath establishment, relocation and teardown
  - Authorization, QoS and policy control
  - Monitoring and statistics
  - Fault diagnostics and maintenance
- Information model
- Annex:
  - Information model notation
  - SDN abstraction
  - Network Function Virtualization



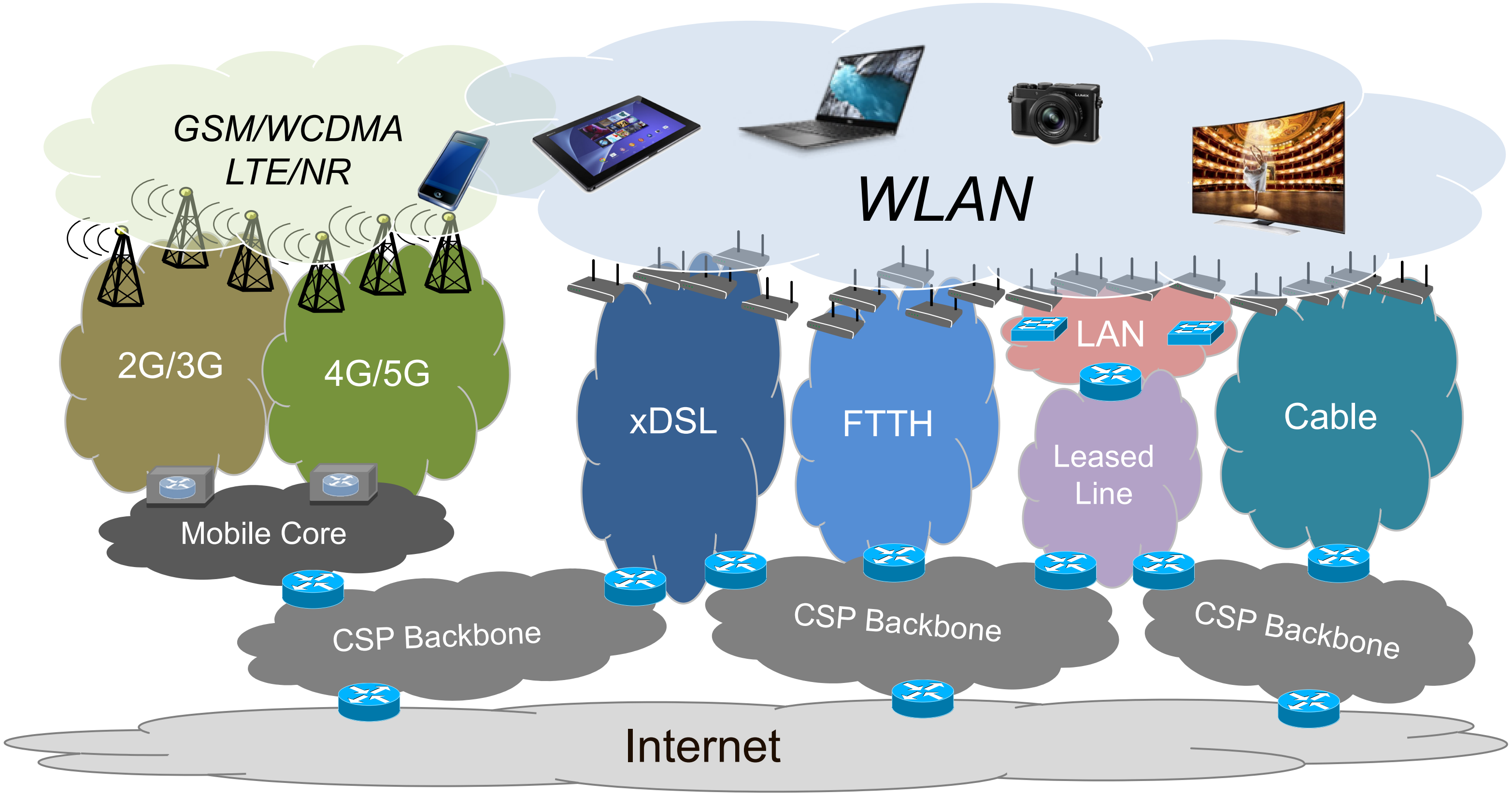




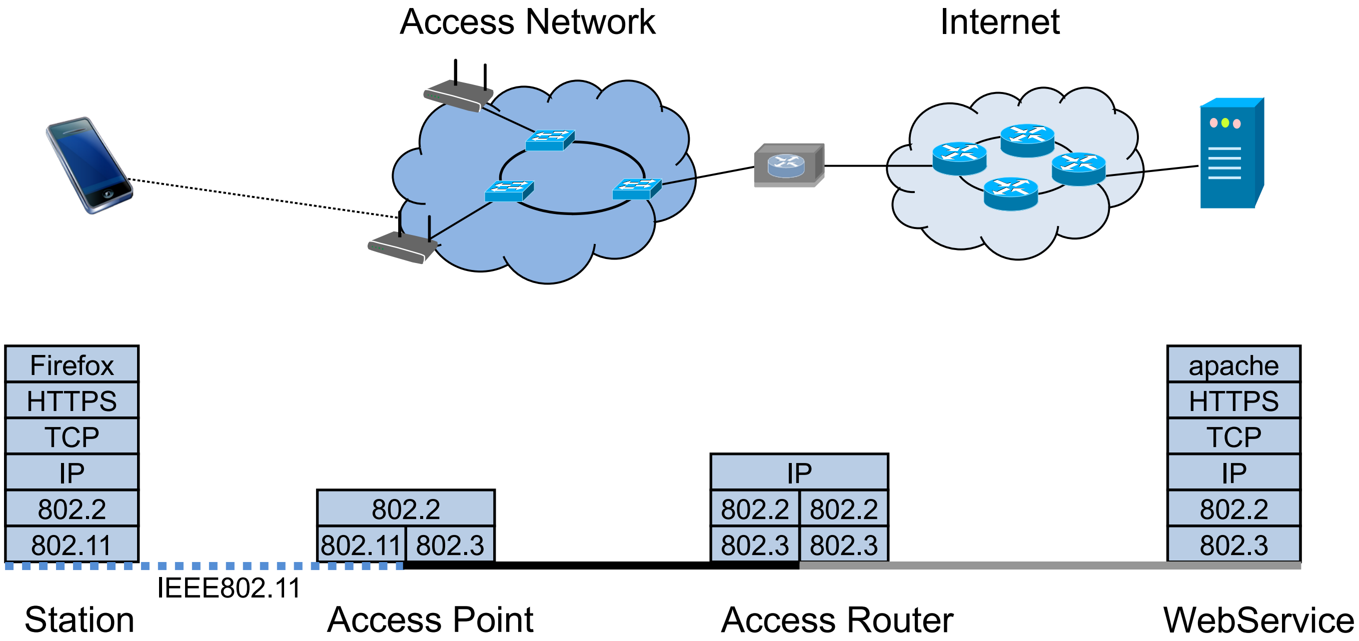
WLAN Deployments

WLAN ACCESS TO THE INTERNET

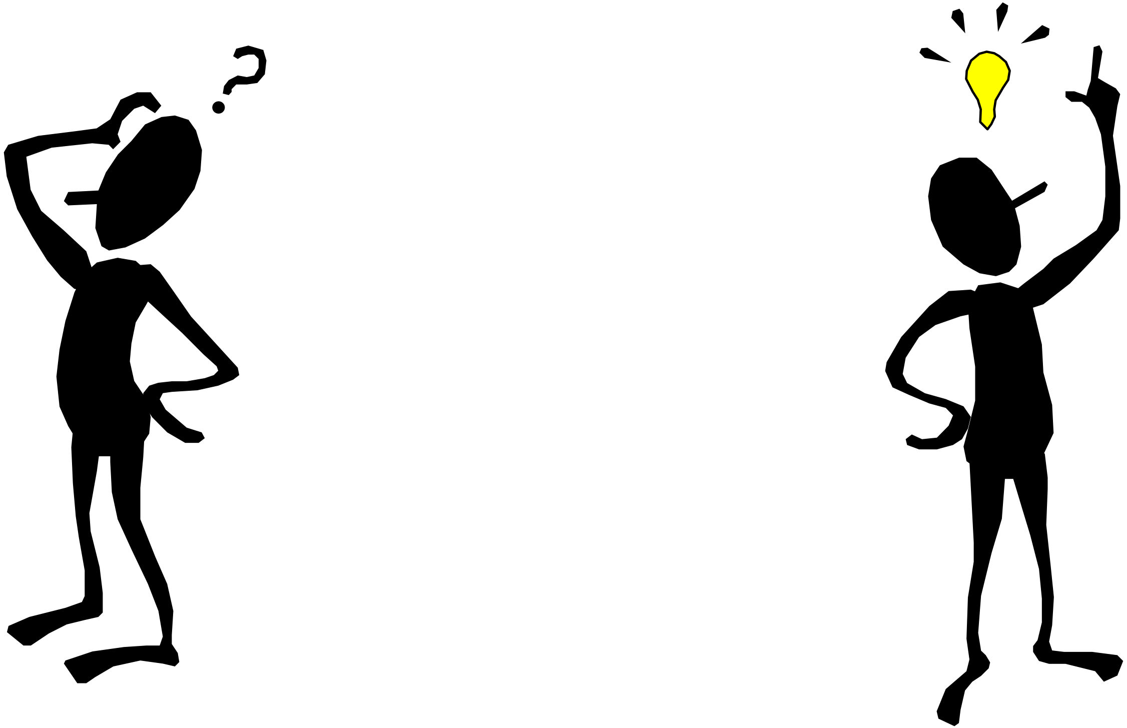
WLAN is the terminal interface for the fixed access networks



WLAN Access protocol architecture for the Internet



Questions and answers



Questions…

WLAN Deployments

1) What is the rough percentage of distribution of WLAN APs between residential, corporate and public?
2) What are the 4 components of a wireless communication network?
3) What are the main functions of the control and IP connectivity part of a wireless communication network?
4) Which control plane functions of a WLAN session setup are executed before of the host configuration?
5) What are the 3 stages of the 3-stage network specification method?
6) What is the purpose of the 802.1CF network reference model?
7) Which operational role belongs to the subscription service?
8) What is the difference between virtualized networks and virtual networks?
9) Which part of the link between Station and Access Router is realized by IEEE 802.11?

WLAN IEEE 802.11

STANDARDIZATION ENVIRONMENT

IEEE 802.11 and Wi-Fi Alliance

IEEE 802.11™

The IEEE 802.11 provides comprehensive technical specifications

Standards Framework

Wi Fi™ ALLIANCE

The Wi-Fi Alliance defines profiles for deployments and certification of products

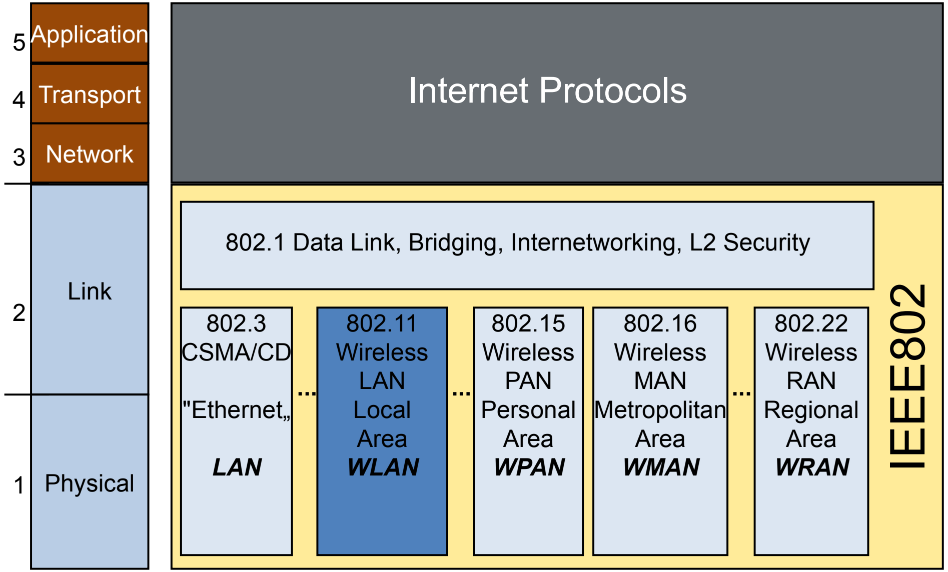
Compatibility Conformance

Standards environment

IEEE 802.11 STANDARDIZATION

IEEE 802 LAN/MAN Standardization Committee

Wireless LAN became topic in IEEE 802 LMSC ten years after its foundation.

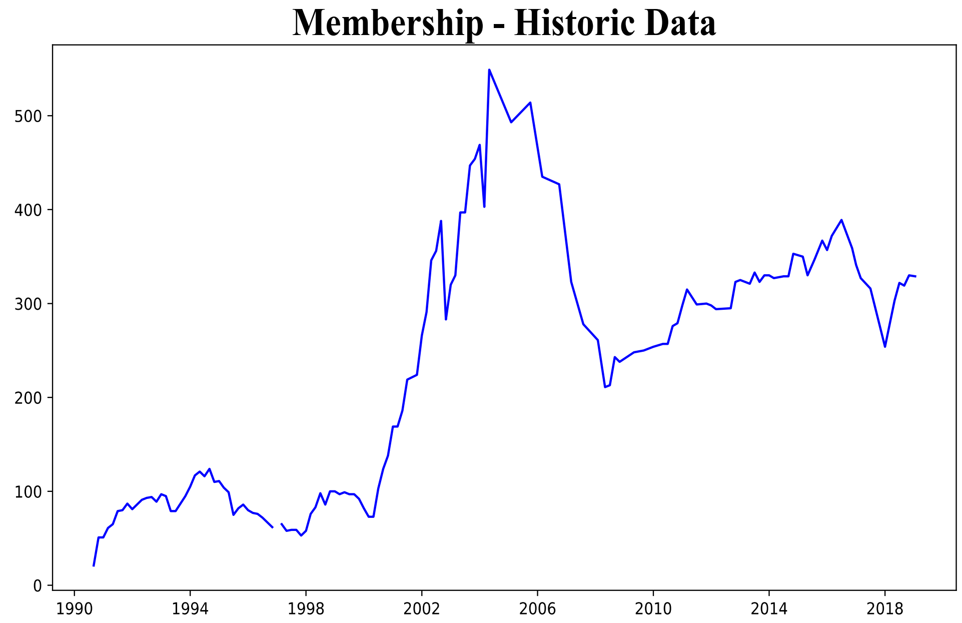

5 Application
4 Transport
3 Network
2 Link
1 Physical
Internet Protocols
802.1 Data Link, Bridging, Internetworking, L2 Security
802.3 CSMA/CD "Ethernet„ LAN
...
802.11 Wireless LAN Local Area WLAN
...
802.15 Wireless PAN Personal Area WPAN
802.16 Wireless MAN Metropolitan Area WMAN
...
802.22 Wireless RAN Regional Area WRAN
IEEE802

Specifies only Physical and Link Layer.
Complete set of standards for carrying IP

- Start of IEEE Computer Society Project 802 in February 1980.
  - Later renamed to “LMSC”: LAN/MAN Standardization Committee
- Initial work on “Ethernet”
  - With 1 to 20 Mbps!
- IEEE 802.11 started in 1990
  - Initially aimed for cash registers!
  - Challenging regulatory!
- Further MAC and PHY groups added, e.g. 802.15, 802.16
- Unifying themes
  - common upper interface to the Data Link Control
  - common data framing

Standardization Process of IEEE 802

- Process is based on Individual Membership – open to everybody
- Working group defines approach to create specification
  - Usually multiple specification stages
  - Call for specific contributions
    - To be discussed at the next f2f meeting
  - Individuals submit written contributions
  - Discussion and debate at meetings
    - Conclusion by 75% vote
  - Initial working group draft
- Working Group Ballot
  - Ballot Responses:
    - "Approve" or "Disapprove”
    - Indicate required changes
  - All submitted comments have to be resolved by working group
- IEEE "Sponsor Ballot“
  - same as above, but with open group



IEEE 802.11 Specifications

IEEE 802.11-1997	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications	Jul 1997
IEEE 802.11	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	Sep 1999
IEEE 802.11a	High-speed Physical Layer in the 5 GHz Band (54 Mbps in 5GHz)	Sep 1999
IEEE 802.11b	Higher-Speed Physical Layer Extension in the 2.4 GHz Band (11 Mbps in 2.4 GHz)	Sep 1999
IEEE 802.11c	Support of the Internal Sublayer Service to cover bridge operations with 802.11 MAC => IEEE 802.1D	Oct 1998
IEEE 802.11d	Specification for operation in additional regulatory domains	Jun 2001
IEEE 802.11e	Medium Access Control (MAC) Quality of Service Enhancements	Nov 2005
IEEE 802.11F	Inter-Access Point Protocol => Withdrawn February 2006	Jul 2003
IEEE 802.11g	Further Higher Data Rate Extension in the 2.4 GHz Band (54 Mbps in 2.4 Ghz)	Jun 2003
IEEE 802.11h	Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe	Oct 2003
IEEE 802.11i	Medium Access Control (MAC) Security Enhancements	Jul 2004
IEEE 802.11j	4.9 GHz–5 GHz Operation in Japan	Oct 2004
IEEE 802.11-2007	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	Jun 2007

IEEE 802.11 Specifications, continuation

IEEE 802.11-2007	***Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) spec***	***Jun 2007***
IEEE 802.11k	Radio Resource Measurement of Wireless LANs	Jun 2008
IEEE 802.11n	Enhancements for Higher Throughput (4x 150 Mbps in 2.4/5GHz)	Oct 2009
IEEE 802.11p	WAVE—Wireless Access for the Vehicular Environment	Jul 2010
IEEE 802.11r	Fast Basic Service Set (BSS) Transition	Jul 2008
IEEE 802.11s	Mesh Networking	Sep 2011
IEEE 802.11T	Wireless Performance Prediction (WPP) => Cancelled	
IEEE 802.11u	Interworking with External Networks	Feb 2011
IEEE 802.11v	IEEE 802.11 Wireless Network Management	Feb 2011
IEEE 802.11w	Protected Management Frames	Sep 2009
IEEE 802.11y	3650–3700 MHz Operation in USA	Nov 2008
IEEE 802.11z	Extensions to Direct Link Set-up (DLS)	Oct 2010
IEEE 802.11-2012	***Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications***	***Mar 2012***

IEEE 802.11 Specifications, continuation

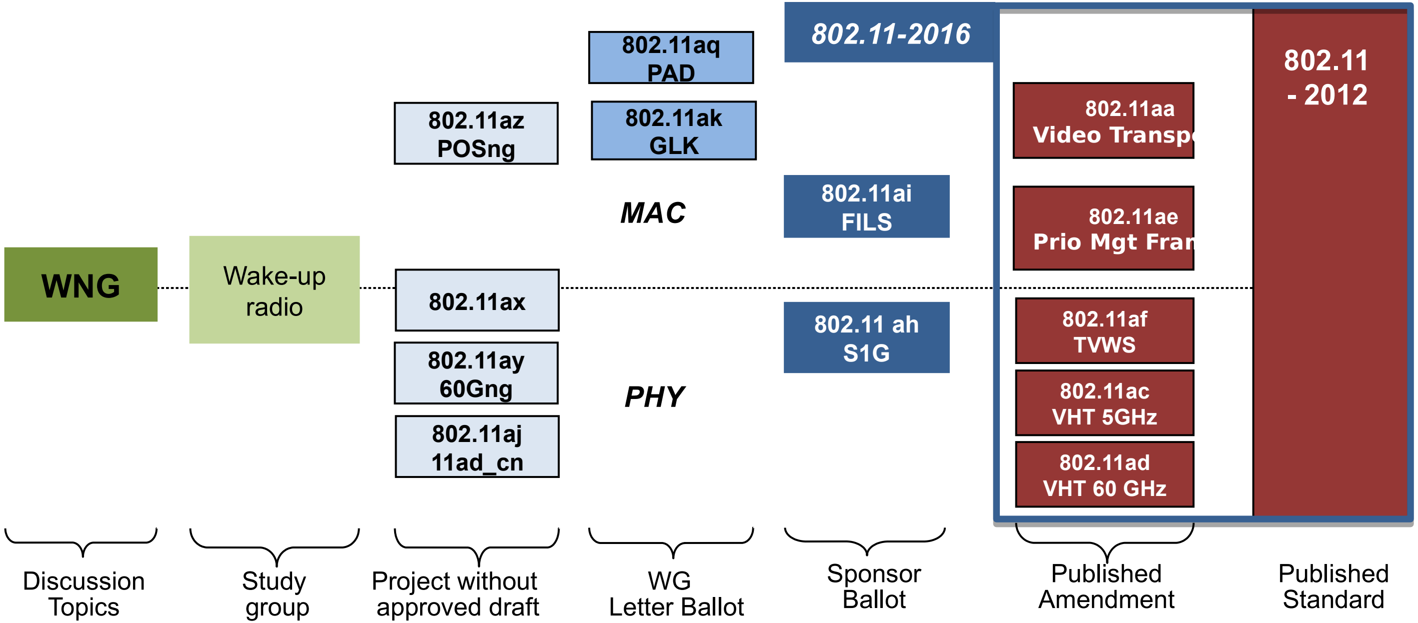
IEEE 802.11-2012	**Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) spec**	**Mar 2012**
IEEE 802.11aa	MAC Enhancements for Robust Audio Video Streaming	May 2012
IEEE 802.11ad	Enhancements for Very High Throughput in the 60 GHz Band	Dec 2012
IEEE 802.11ae	Prioritization of Management Frames	Apr 2012
IEEE 802.11ac	Enhancements for Very High Throughput for Operation in Bands below 6 GHz	Dec 2013
IEEE 802.11af	TV White Spaces Operation	Dec 2013
IEEE 802.11-2016	**Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) spec**	**Dec 2016**
IEEE 802.11ah	Sub 1 GHz license-exempt operation	Dec 2016
IEEE 802.11ai	Fast Initial Link Set-up	Dec 2016
IEEE 802.11aj	China Milli-Meter Wave (CMMW)	Feb 2018
IEEE 802.11ak	Enhancements For Transit Links Within Bridged Networks	Jun 2018
IEEE 802.11aq	Pre-Association Discovery (PAD)	Sep 2018
P802.11md	***Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) spec***	***~ 11/2020***

IEEE 802.11 ongoing standardization projects

P802.11md	***Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) spec***	***~ 11/2020***
P802.11ax	High Efficiency WLAN	~ 11/2020
P802.11ay	Enhanced Throughput for Operation in License-Exempt Bands above 45 GHz	~ 12/2020
P802.11az	Next Generation Positioning	~ 03/2021
P802.11ba	Wake Up Radio (WUR)	~ 12/2020
P802.11bb	Light Communication (LC)	~ 07/2022
P802.11bc	Enhanced Broadcast Service	~ 04/2022
P802.11bd	Enhancements for Next Generation V2X	~ 12/2021
P802.11be	Extreme High Throughput	~ 05/2024

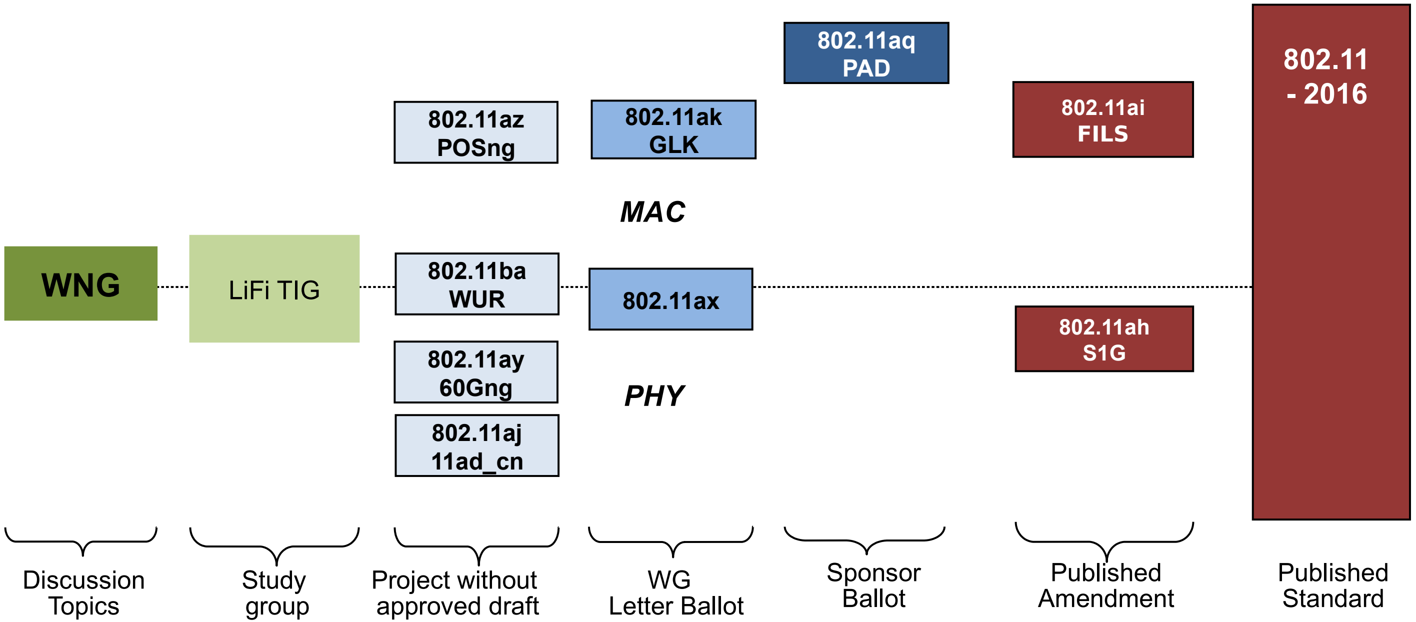
IEEE 802.11 standards evolution (from 09/2016 …)

The working group concurrently operates in different standardization phases



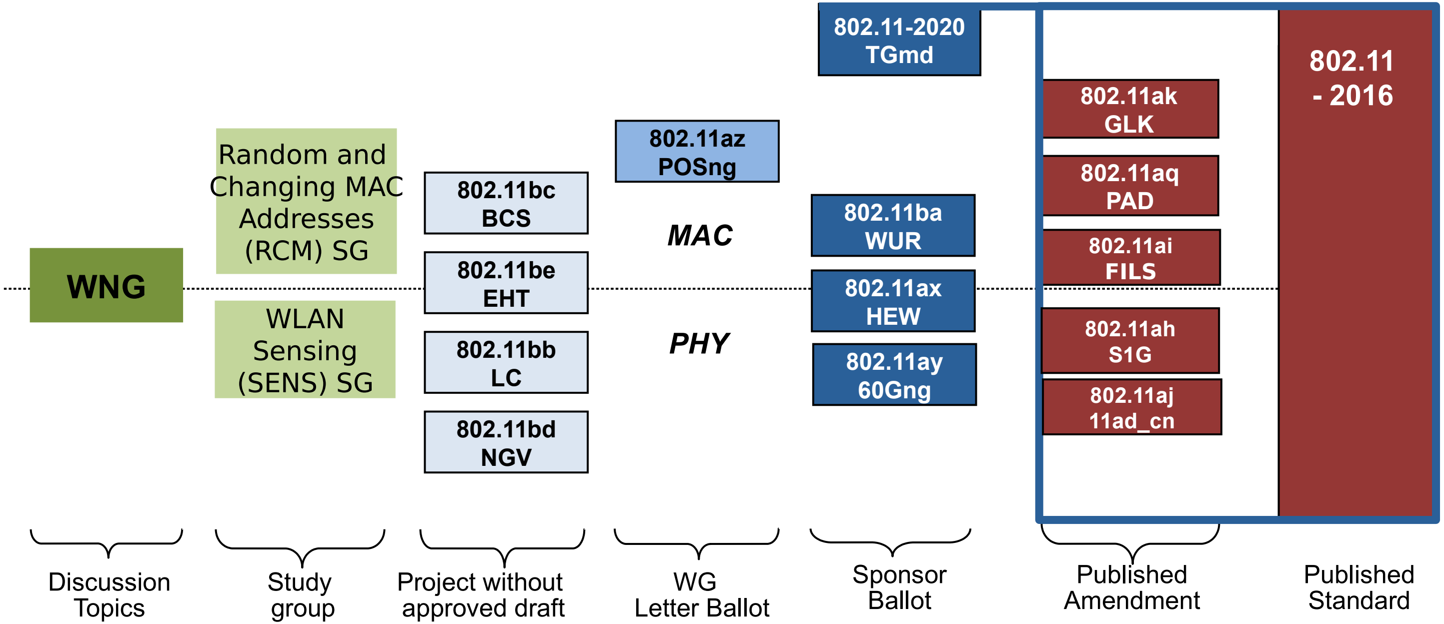
IEEE 802.11 standards evolution (.. to 03/2017)

The working group concurrently operates in different standardization phases



IEEE 802.11 standards evolution (.. to 05/2020)

The working group concurrently operates in different standardization phases



IEEE802.11 WLAN radio standards evolution

Std	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate outdoor range (m)
	Jun 1997	2.4	20	1, 2	1	DSSS	40	150
a	Sep 1999	5	20**	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	40	150
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	40	150
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM (DSSS)	40	150
n	Oct 2009	2.4 5	20/40	up to 72.2/150	4	OFDM	60 40	200 150
y	Nov 2008	3.7	5/10/20	up to 13.5/27/54	1	OFDM	-	5 000
ac	Dec 2013	5	20/40/ 80/160	up to 87/200/433/867	8	OFDM	40	150
ad	Oct 2012	60	2160	up to 6 700	1	SC // OFDM	line of sight	line of sight
af	Dec 2013	TV WS	1,2,4x 6/7/8	up to 1,2,4x 26.7/26.7/35.5	4	OFDM	100	1000
ah	Dec 2016	< 1	1/2/4/8/16	0.15 … up to 4.4/9/20/43/87	4	OFDM	100	1000
ax	~ 2020*	1…6	2.5/5/10/20/ 40/80/160	up to 15/30/63/143/287/600/1201	8	OFDMA	80	300
ay	~ 2020*	60	1..4 x 2160	N_{cb}x 8.6 // 8.3/18.2/28.1/37.9 Gbps	8	SC // OFDM	line of sight	line of sight

* Preliminary information; specifications still in early phases of development.
** Half-clocked and quarter clocked variants available for 10 MHz and 5 MHz channel bandwidth, as used by IEEE 802.11p
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power

Standards environments

STANDARD REFERENCE

IEEE Std 802.11™-2016

IEEE Standard for Information technology—
Telecommunications and information exchange between systems
Local and metropolitan area networks—
Specific requirements

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

IEEE Computer Society

- *Can be downloaded at no charge by IEEE Get Program*
  - [*http://standards.ieee.org/getieee802/download/802.11-2016.pdf*](http://standards.ieee.org/getieee802/download/802.11-2016.pdf)
- *No all the features specified in the standard are available in real Wi-Fi products*
- *This lecture presents behavior of real Wi-Fi products as specified by Wi-Fi Alliance in its certification programs*
  - [*https://www.wi-fi.org/discover-wi-fi/specifications*](https://www.wi-fi.org/discover-wi-fi/specifications)

IEEE Standard for Information technology

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

- Revision of IEEE Std 802.11-2012
  - Revision of IEEE Std 802.11-2007
    - Revision of IEEE Std 802.11-1999
      - First IEEE 802.11 standard release in 1997
- Comprises initial IEEE Std 802.11-1999 together with all amendments IEEE 802.11a-1999 … IEEE 802.11af-2013
  - *i.e.:* a, b, d, e, g, h, I, j, k, n, p, r, s, u, v, w, y, z, aa, ac, ad, ae, af

Standards environments

WI-FI ALLIANCE CERTIFICATION

The Wi-Fi Alliance

Wi-Fi CERTIFIED™ makes it Wi-Fi.

To overcome interoperability issues experienced with early IEEE 802.11 products, the Wireless Ethernet Compatibility Alliance (WECA) was founded in 1999 with the completion of IEEE 802.11b.

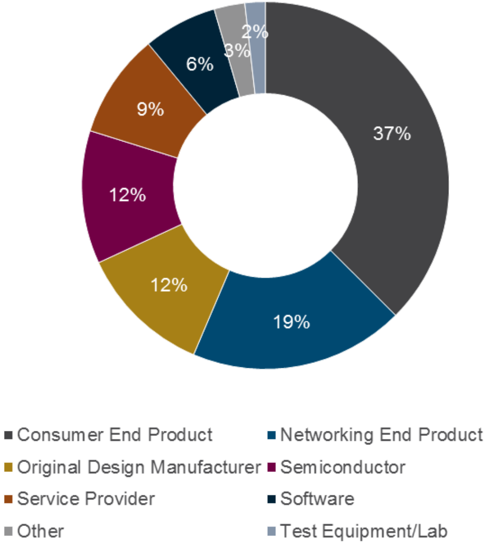
'Wi-Fi' was introduced as brand-name for interoperable IEEE 802.11 WLAN.

In 2001, WECA became the

Wi-Fi Alliance

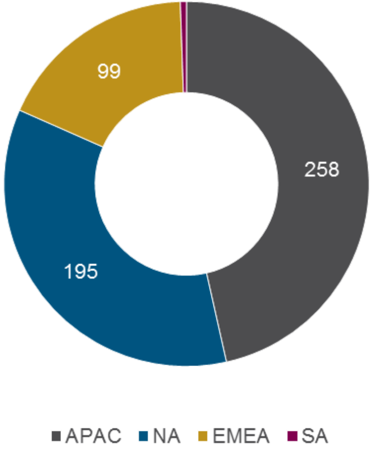
Members by Segment

(June 2013)



Members by Regions

(June 2013)



The Wi-Fi Alliance Approach to Certification

Wi-Fi CERTIFIED products have to demonstrate that they can perform well in networks with other Wi-Fi CERTIFIED products, running common applications, in situations similar to those encountered in everyday use.

Interoperability

Rigorous test cases are used to ensure that products from different equipment vendors can interoperate in a wide variety of configurations.

Backward Compatibility

Backward compatibility protects investments in legacy Wi-Fi products and enables users to gradually upgrade and expand their networks.

Innovation

Timely introduction of new certification programs as the latest technology and specifications come into the marketplace. Equipment vendor can differentiate in areas that are not covered by certification testing.

The Wi-Fi Alliance Certification Process

Wi Fi CERTIFIED

Compatibility

Certified equipment has been tested for connectivity with other certified equipment. It involves tests with multiple devices from different equipment vendors and ensures that devices purchased today will work with Wi-Fi CERTIFIED devices already owned or purchased in the future.

Conformance

The equipment conforms to specific critical elements of the IEEE802.11 standard. Conformance testing usually involves standalone analysis of individual products and establishes whether the equipment responds to inputs as expected and specified.

Performance

The equipment meets the performance levels required to meet end-user expectations in support of key applications. Performance tests verify that the product meets the minimum performance requirements for a good user experience. Specific performance tests results are not released by the Wi-Fi Alliance.

The base Wi-Fi Alliance certification programs

Program	Description	Remarks
IEEE 802.11a IEEE 802.11b IEEE 802.11g	Wi-Fi products based on IEEE radio standards - 802.11a, 802.11b, 802.11g in single, dual mode (802.11b and 802.11g) or multi-band (2.4GHz and 5GHz) products.	Required by CTIA for Wi-Fi enabled handsets seeking CTIA certification
WPA2™ (Wi-Fi Protected Access 2)	Wi-Fi wireless network security - offer government-grade security mechanisms for personal and enterprise	
EAP (Extensible Authentication Protocol)	An authentication mechanism used to validate the identity of network devices (for enterprise devices)	Includes mandatory support for EAP-SIM
Protected Management Frames	Extends WPA2 protection to unicast and multicast management action frames	
Wi-Fi CERTIFIED n	Based on the IEEE 802.11n ratified standard.	Includes also Wi-Fi Multimedia (WMM) testing
Wi-Fi CERTIFIED ac	Based on IEEE 802.11ac	Requires devices to pass all certified n tests

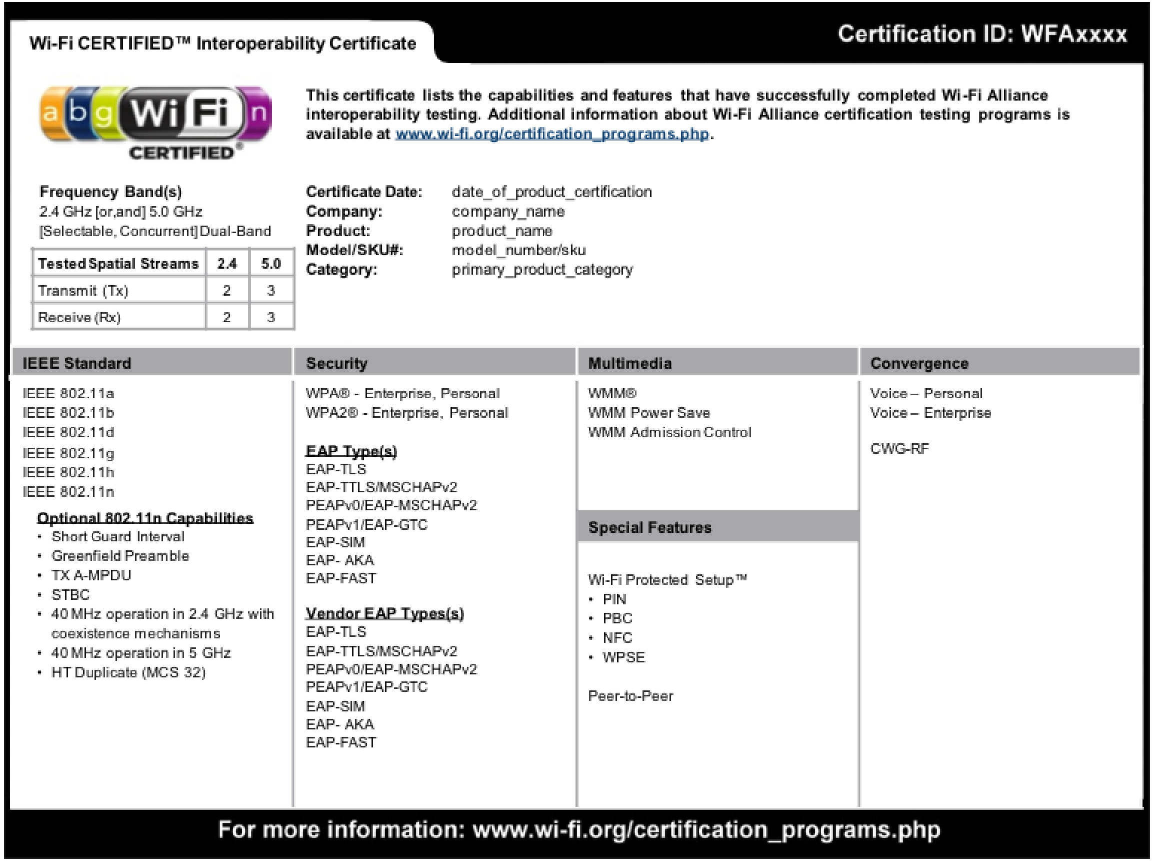
Optional certification programs

Program	Description	Remarks
Miracast™	Provides seamless display of content between devices, regardless of brand, without cables or a network connection. Miracast	“Wi-Fi Display Technical Specification”
TDLS (Tunneled Direct Link Setup)	Allows network-connected devices to create a secure, direct link to transfer data more efficiently	
Passpoint™	Enables mobile devices to automatically discover and connect to Wi-Fi networks. Passpoint also automatically configures industry-standard WPA2™ security protections without user intervention.	“Wi-Fi Alliance Hotspot 2.0 Technical Specification”
Wi-Fi Direct™	Allows Wi-Fi client devices that connect directly without use of an access point, to enable applications such as printing, content sharing, and display.	“Wi-Fi Alliance Peer-to-Peer Technical Specification”
Wi-Fi Protected Setup™	Facilitates easy set-up of security features using a Personal Identification Number (PIN) or other defined methods within the Wi-Fi device.	“Wi-Fi Simple Configuration Technical Specification”
WMM® (Wi-Fi Multimedia™)	Support for multimedia content over Wi-Fi networks enabling Wi-Fi networks to prioritize traffic generated by different applications using Quality of Service (QoS) mechanisms.	“WMM Technical Specification”

Further optional certification programs

Program	Description	Remarks
WMM-Power Save	Power savings for multimedia content over Wi-Fi networks - helps conserve battery life while using voice and multimedia applications by managing the time the device spends in sleep mode	
WMM-Admission Control	Enhanced bandwidth management tools to optimize the delivery of voice and other traffic in Wi-Fi® networks.	“WMM Technical Specification”
Voice-Personal	Voice over Wi-Fi - extends beyond interoperability testing to test the performance of products and help ensure that they deliver good voice quality over the Wi-Fi link	
Voice-Enterprise	Supports a good experience with voice applications over Wi-Fi with fast transitions between access points and providing management.	Builds on Voice-Personal certification features
CWG-RF	For converged handsets with both Wi-Fi and cellular technology - provides detailed information about the performance of the Wi-Fi radio, as well as about the coexistence of the cellular and Wi-Fi radios.	Mandatory for Wi-Fi enabled handsets seeking CTIA certification.
IBSS with Wi-Fi Protected Setup	Enables ad-hoc connections between devices to complete tasks such as file printing or sharing. Designed to ease setup of connection for devices with limited user interface.	“IBSS with Wi-Fi Protected Setup Specification”

Documentation of a Wi-Fi CERTIFIED Product



Wi-Fi CERTIFIED™ Interoperability Certificate

Certification ID: WFAxxxx

This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification testing programs is available at www.wi-fi.org/certification_programs.php.

Frequency Band(s)
2.4 GHz [or,and] 5.0 GHz
[Selectable, Concurrent] Dual-Band

Tested Spatial Streams	2.4	5.0
Transmit (Tx)	2	3
Receive (Rx)	2	3

Certificate Date: date_of_product_certification
Company: company_name
Product: product_name
Model/SKU#: model_number/sku
Category: primary_product_category

IEEE Standard

IEEE 802.11a
IEEE 802.11b
IEEE 802.11d
IEEE 802.11g
IEEE 802.11h
IEEE 802.11n

Optional 802.11n Capabilities

- Short Guard Interval
- Greenfield Preamble
- TX A-MPDU
- STBC
- 40 MHz operation in 2.4 GHz with coexistence mechanisms
- 40 MHz operation in 5 GHz
- HT Duplicate (MCS 32)

Security

WPA® - Enterprise, Personal
WPA2® - Enterprise, Personal

EAP Type(s)
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP- AKA
EAP-FAST

Vendor EAP Types(s)
EAP-TLS
EAP-TTLS/MSCHAPv2
PEAPv0/EAP-MSCHAPv2
PEAPv1/EAP-GTC
EAP-SIM
EAP- AKA
EAP-FAST

Multimedia

WMM®
WMM Power Save
WMM Admission Control

Special Features

Wi-Fi Protected Setup™

- PIN
- PBC
- NFC
- WPSE

Peer-to-Peer

Convergence

Voice – Personal
Voice – Enterprise

CWG-RF

For more information: www.wi-fi.org/certification_programs.php

Generational Wi-Fi

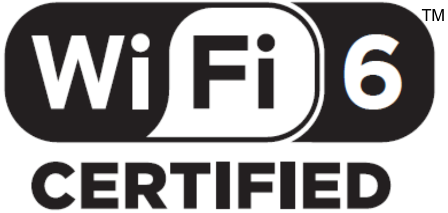
- Up to now Wi-Fi radio technologies were identified through the project acronym of the related IEEE 802.11 standardization project.
  - 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac
- It led to ambiguous communication and slow adoption of new Wi-Fi radio technologies through the market.

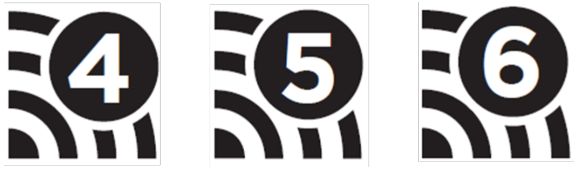
- Aligned to the much better perceived notation of radio technologies in the cellular market, Wi-Fi Alliance moved forward and introduced a similar notation for Wi-Fi radio technologies.
  - E.g. cellular communications: 1G -> 2G -> 3G -> 4G -> 5G
- The next Wi-Fi radio technology based on IEEE 802.11ax will be denoted ‘Wi-Fi 6’.
  - Wi-Fi certified products are identified through ‘Wi-Fi CERTIFIED™ 6’

Visualization of Wi-Fi generations

- Identification and visualization of various Wi-Fi radio technologies:

If the most advanced technology a device supports is …	Then it shall be identified as generation
802.11ax	Wi-Fi 6
802.11ac	Wi-Fi 5
802.11n	Wi-Fi 4





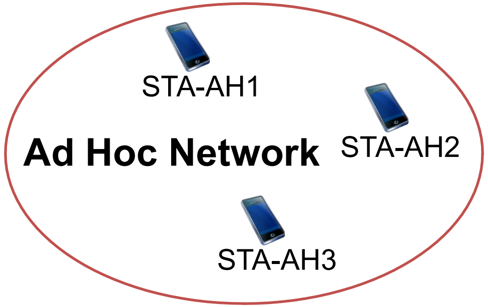
- A simple and clear identification allows the user to distinct the radio technology supported by the equipment and used for a connection.
  - The main intention is the faster market adoption of new Wi-Fi technologies by creating more evident demand of users and operators.

WLAN IEEE 802.11

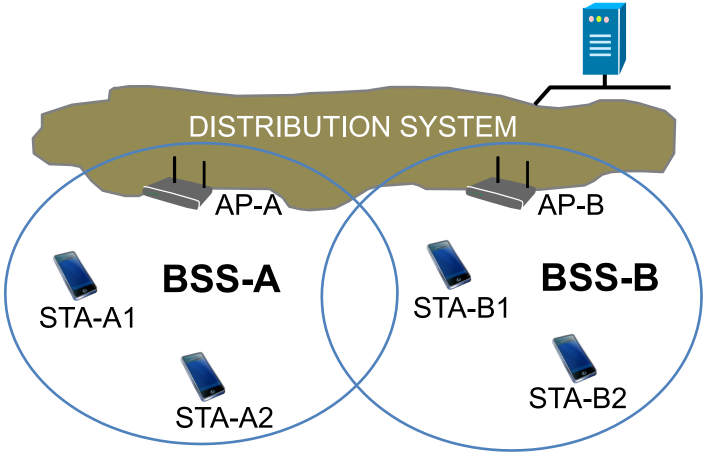
WLAN SYSTEM ARCHITECTURE

IEEE802.11 Configurations

- Independent
  - one “Basic Service Set”, BSS
  - “Ad Hoc” network
  - direct communication
  - limited coverage area



- Infrastructure
  - Access Points and Stations
  - Distribution System interconnects Multiple Cells via Access Points to form a single Network.
    - extends wireless coverage area

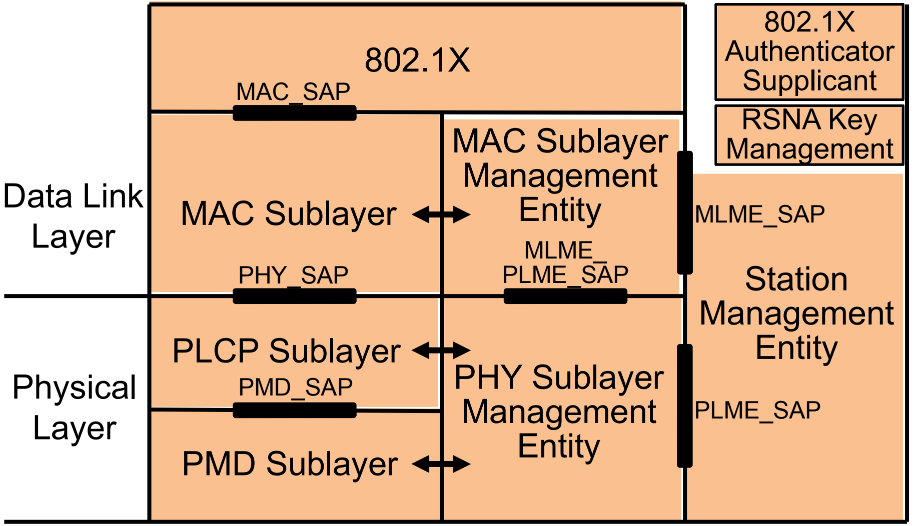


IEEE802.11 Architecture overview

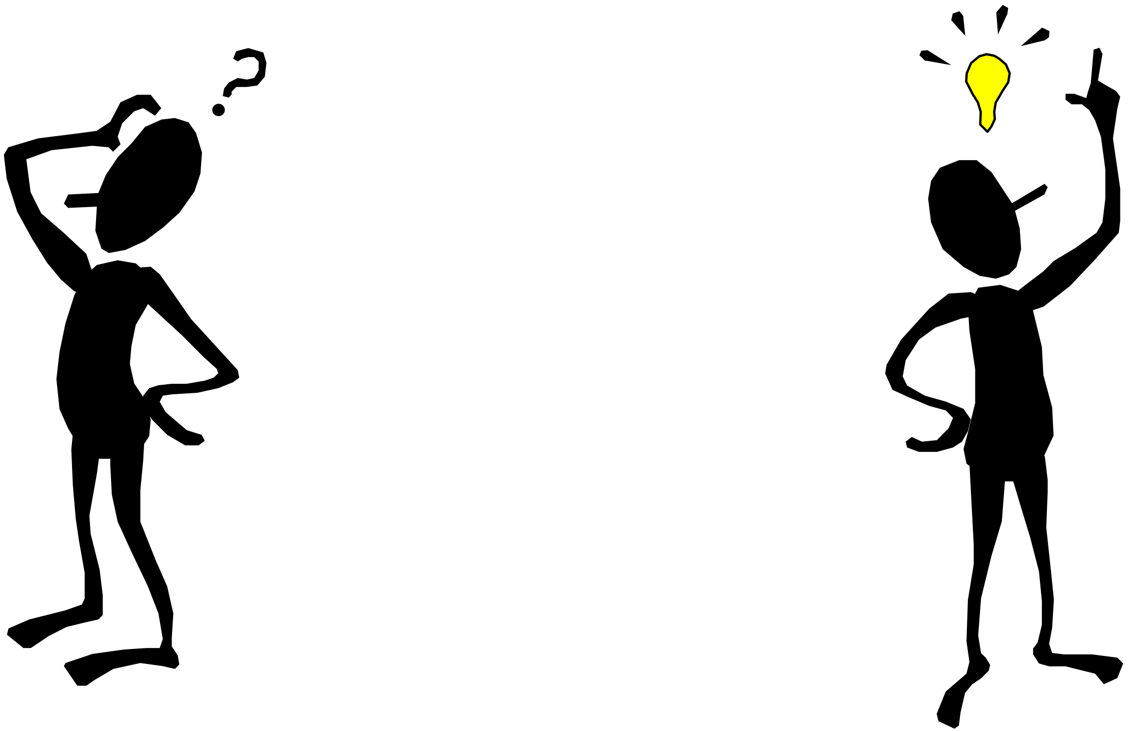
- One common MAC supporting multiple PHYs
- Two configurations
  - “Independent” (ad hoc) and “Infrastructure”
- CSMA/CA (collision avoidance) with optional “point coordination”
- Connectionless Service
  - Transfer data on a shared medium without reservation
  - data comes in bursts
  - user waits for response, so transmit at highest speed possible
  - is the same service as used by Internet
- Robust against noise and interference (ACK)
- Hidden Node Problem (RTS/CTS)
- Mobility (Hand-over mechanism)
- Security (WPA2, WPA3)
- Power savings (Sleep intervals)

IEEE802.11 Protocol architecture

- 802.1X
  - Port Access Entity
  - Authenticator/Supplicant
- RSNA Key Management
  - Generation of Pair-wise and Group Keys
- Station Management Entity (SME)
  - interacts with both MAC and PHY Management
- MAC Sublayer Management Entity (MLME)
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- MAC Sublayer
  - basic access mechanism
  - fragmentation
  - encryption
- PHY Sublayer Management Entity (PLME)
  - channel tuning
  - PHY configuration and monitoring
- Physical Sublayer Convergence Protocol (PLCP)
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- Physical Medium Dependent Sublayer (PMD)
  - modulation and encoding



Questions and answers



Questions…

Standards Environment

1) What part of a Wi-Fi access network is specified by IEEE 802.11?
2) What is the purpose of the Wi-Fi Alliance?
3) To which standardization organization belongs IEEE 802.11?
4) Which IEEE 802.11 standards and amendments are comprised in IEEE 802.11-2016
5) What layers of the ISO-OSI model are covered by IEEE 802.11?
6) What aspects are covered through the Wi-Fi Alliance certification process?
7) Which Wi-Fi Alliance certification program addresses direct connectivity between Wi-Fi clients without the use of an access point?
8) What does ‘WMM’ stand for?

WLAN System Architecture

9) What are the two IEEE 802.11 Configurations?
10) What function provides the Distribution System of the Infrastructure configuration?
11) Which sublayer provides the convergence protocol between the PMD Sublayer and the MAC sublayer in the protocol architecture?

WLAN IEEE 802.11

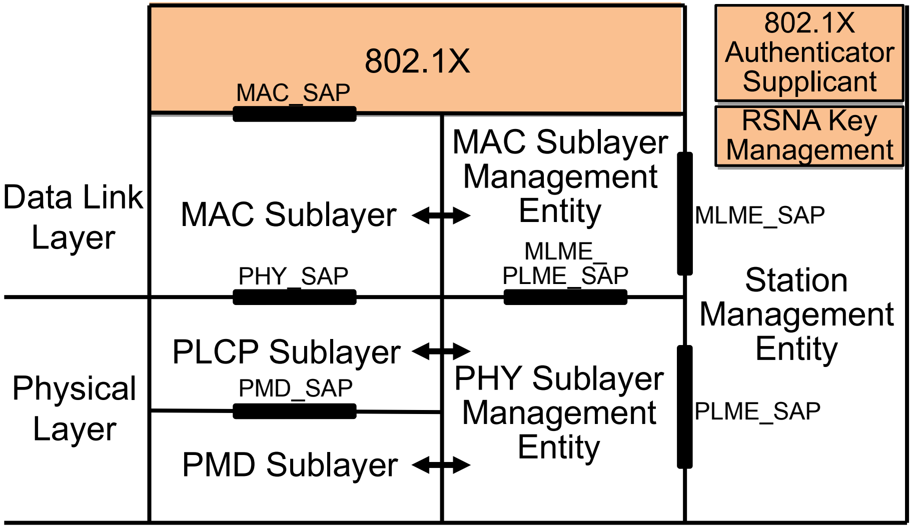
IEEE 802.11 SECURITY

Topics covered in this section

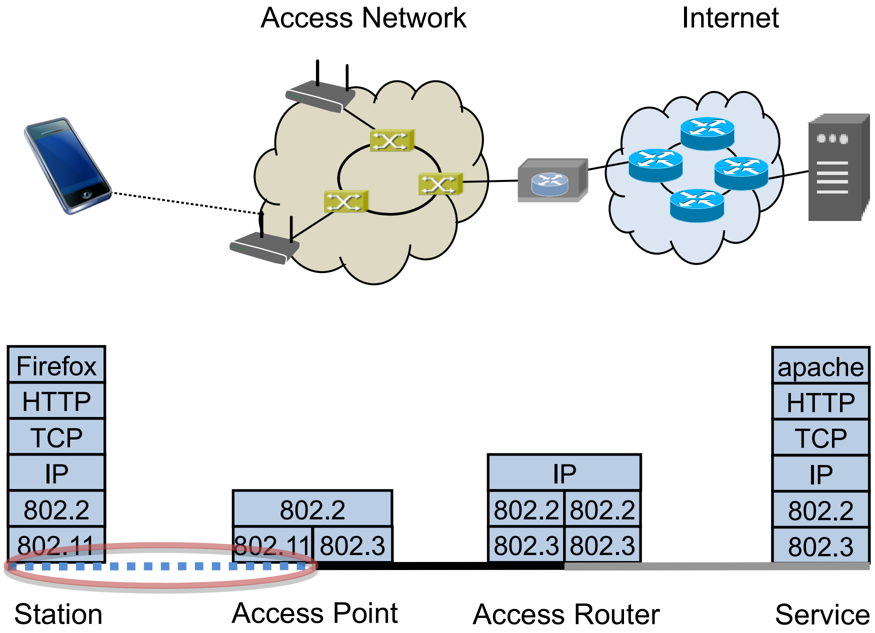
- IEEE 802.11 Security
  - Security evolution
  - Robust security network
    - Configuration
    - PSK/SAE Authentication
    - IEEE 802.1X Authentication
    - Key management
    - Data protection
    - Summary
  - Protected management frames,
  - Fast transition

IEEE802.11 Protocol architecture

- 802.1X
  - Port Access Entity
  - Authenticator/Supplicant
- RSNA Key Management
  - Generation of Pair-wise and Group Keys
- Station Management Entity (SME)
  - interacts with both MAC and PHY Management
- MAC Sublayer Management Entity (MLME)
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- MAC Sublayer
  - basic access mechanism
  - fragmentation
  - encryption
- PHY Sublayer Management Entity (PLME)
  - channel tuning
  - PHY configuration and monitoring
- Physical Sublayer Convergence Protocol (PLCP)
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- Physical Medium Dependent Sublayer (PMD)
  - modulation and encoding

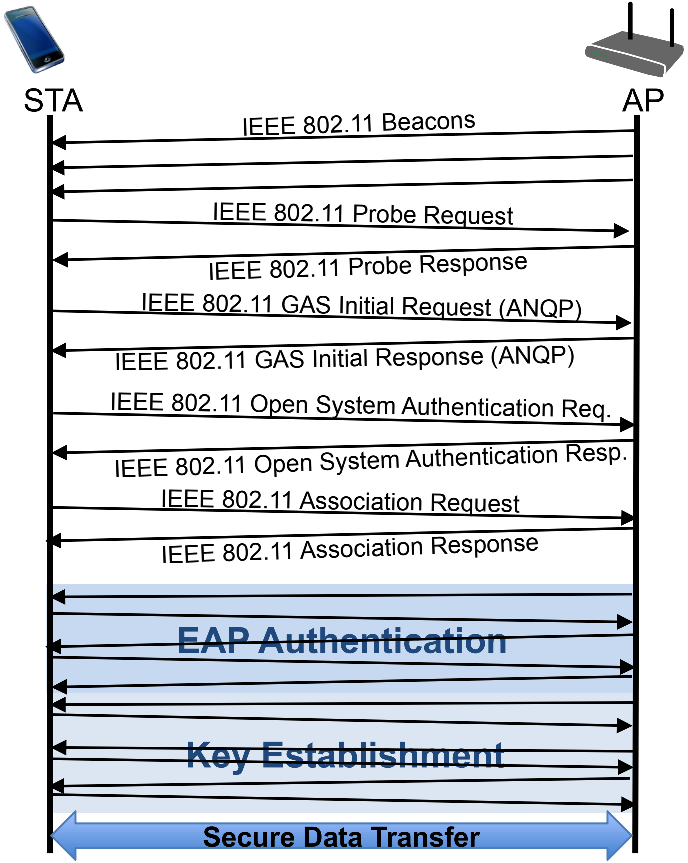


Wireless LAN IEEE802.11 Security



- Wireless portion of the network is open to sniffing and injection
- IEEE 802.11 security addresses authentication, confidentiality and replay protection.
  - Various authentication methods supported.
- Ciphering works on both unicast and multicast messages

IEEE 802.11 Security Establishment


STA
AP
IEEE 802.11 Beacons
IEEE 802.11 Probe Request
IEEE 802.11 Probe Response
IEEE 802.11 GAS Initial Request (ANQP)
IEEE 802.11 GAS Initial Response (ANQP)
IEEE 802.11 Open System Authentication Req.
IEEE 802.11 Open System Authentication Resp.
IEEE 802.11 Association Request
IEEE 802.11 Association Response
EAP Authentication
Key Establishment
Secure Data Transfer

- Scanning
  - Beacon
  - Probe Request/Response
- Network Selection
  - GAS (ANQP Request/Response)
- Authentication
  - Open System Authentication
- Association
  - Association Request/Response
- Authentication/Authorization
  - IEEE 802.1X EAPoL follows association message exchange
    - Starts with controlled port blocked and uncontrolled port used for exchange of authentication messages
    - EAP protocol carries authentication method
  - Authorization comprises configuration of data path and master key delivery to AP
- Key establishment
  - Four-way handshake for pair-wise keys
  - Additional groups keys for broadcasts
- Secure data transfer
  - Secure data transfer over controlled port starts once encryption keys are established

IEEE 802.11 Security

SECURITY EVOLUTION

History of IEEE 802.11 Security

- Initial goal of P802.11 security was to provide “Wired Equivalent Privacy”
  - Usable worldwide as there was strict export regulation at that time for any ‘strong’ security with more than 40bits keys
- IEEE 802.11-1997 provided shared key authentication based on WEP privacy mechanism
  - RC4 algorithm with 40 bit secret key
- WEP was completely insufficient
  - WEP unsecure at any key length
  - No user authentication
  - No mutual authentication
  - Missing key management protocol
- IEEE 802.11i-2004 fixed weak security by “Robust Security Network” (RSN)
  - Transitional solution w/ TKIP for fixing bugs in existing hardware
  - Conclusive solution w/ CCMP (AES) for new hardware
    - Also known by WFA terms WPA (TKIP) and WPA2 (CCMP)
- WPA2 supported by all Wi-Fi hardware since about 2005

Wi-Fi Security Algorithms

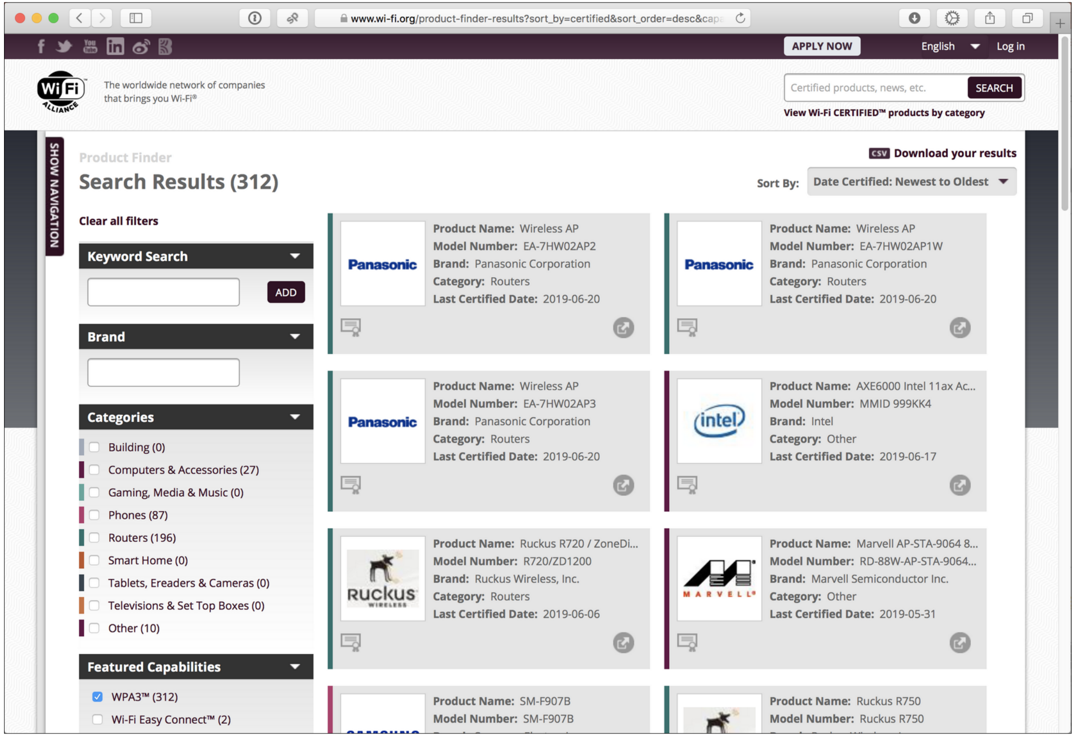
Security Feature	Manual WEP	Dynamic WEP	TKIP (RSN)	CCMP (RSN)
Core cryptographic algorithm	RC4	RC4	RC4	AES
Key sizes	40bit or 104bit (encryption)	40bit or 104bit (encryption)	128bit (encryption) 64bit (integrity protection)	128bit (encryption and integrity protection)
Per-packet key	Created through concatenation of WEP key and 24bit IV	Derived from EAP authentication	Created through TKIP mixing function	Not needed; temporal key is sufficiently secure
Integrity protection	Enciphered CRC-32	Enciphered CRC-32	Michael message integrity check (MIC) with countermeasures	CCM
Header protection	None	None	Src and Dest addresses protected by MIC	Src and Dest addresses protected by CCM
Replay protection	None	None	Enforce IV sequencing	Enforce IV sequencing
Authentication	Open system or shared key	EAP method with IEEE 802.1X	PSK or EAP method with IEEE 802.1X	PSK or EAP method with IEEE 802.1X
Key distribution	Manual	IEEE 802.1X	manual or IEEE 802.1X	manual or IEEE 802.1X

IEEE 802.11, WPA, WPA2 and WPA3

IEEE 802.11	WPA	WPA2	WPA3
IEEE 802.1X	▨	▨	▨
PSK	▨	▨	
SAE			▨
Data privacy protocols			
TKIP	▨		
CCMP		▨	▨
GCMP			▨
Further functions			
Basic Service Set	▨	▨	▨
IBSS		▨	▨
Pre-authentication		▨	▨
Key hierarchy	▨	▨	▨
Key management	▨	▨	▨
Cipher & authentication negotiation	▨	▨	▨
Protected Management Frames		option	▨

- WPA (Wi-Fi Protected Access) has been legacy stop-gap solution to address WEP issues (~ 2003 !)
  - WPA could be realized as firmware upgrade to existing products
- WPA2 covers full IEEE 802.11i amendment
- WPA w/ TKIP now depreciated
  - Selecting WPA limits maximum speed to 54 Mbps
  - 11n, 11ac mandate WPA2 AES encryption
- WPA3 replaces direct derivation from PSK through SAE key generation and provides more secure cypher modes for Enterprise deployments
  - Support of Protected Management Frames is mandatory for WPA3 certification.

WPA3 product support



www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&cap

APPLY NOW English Log in

The worldwide network of companies that brings you Wi-Fi®

Certified products, news, etc. SEARCH

View Wi-Fi CERTIFIED™ products by category

SHOW NAVIGATION

Product Finder

Search Results (312)

CSV Download your results

Sort By: Date Certified: Newest to Oldest

Clear all filters

Keyword Search

ADD

Brand

Categories

- □ Building (0)
- □ Computers & Accessories (27)
- □ Gaming, Media & Music (0)
- □ Phones (87)
- □ Routers (196)
- □ Smart Home (0)
- □ Tablets, Ereaders & Cameras (0)
- □ Televisions & Set Top Boxes (0)
- □ Other (10)

Featured Capabilities

- ☑ WPA3™ (312)
- □ Wi-Fi Easy Connect™ (2)

Product Name: Wireless AP
Model Number: EA-7HW02AP2
Brand: Panasonic Corporation
Category: Routers
Last Certified Date: 2019-06-20

Product Name: Wireless AP
Model Number: EA-7HW02AP1W
Brand: Panasonic Corporation
Category: Routers
Last Certified Date: 2019-06-20

Product Name: Wireless AP
Model Number: EA-7HW02AP3
Brand: Panasonic Corporation
Category: Routers
Last Certified Date: 2019-06-20

Product Name: AXE6000 Intel 11ax Ac...
Model Number: MMID 999KK4
Brand: Intel
Category: Other
Last Certified Date: 2019-06-17

Product Name: Ruckus R720 / ZoneDi...
Model Number: R720/ZD1200
Brand: Ruckus Wireless, Inc.
Category: Routers
Last Certified Date: 2019-06-06

Product Name: Marvell AP-STA-9064 8...
Model Number: RD-88W-AP-STA-9064...
Brand: Marvell Semiconductor Inc.
Category: Other
Last Certified Date: 2019-05-31

Product Name: SM-F907B
Model Number: SM-F907B

Product Name: Ruckus R750
Model Number: Ruckus R750

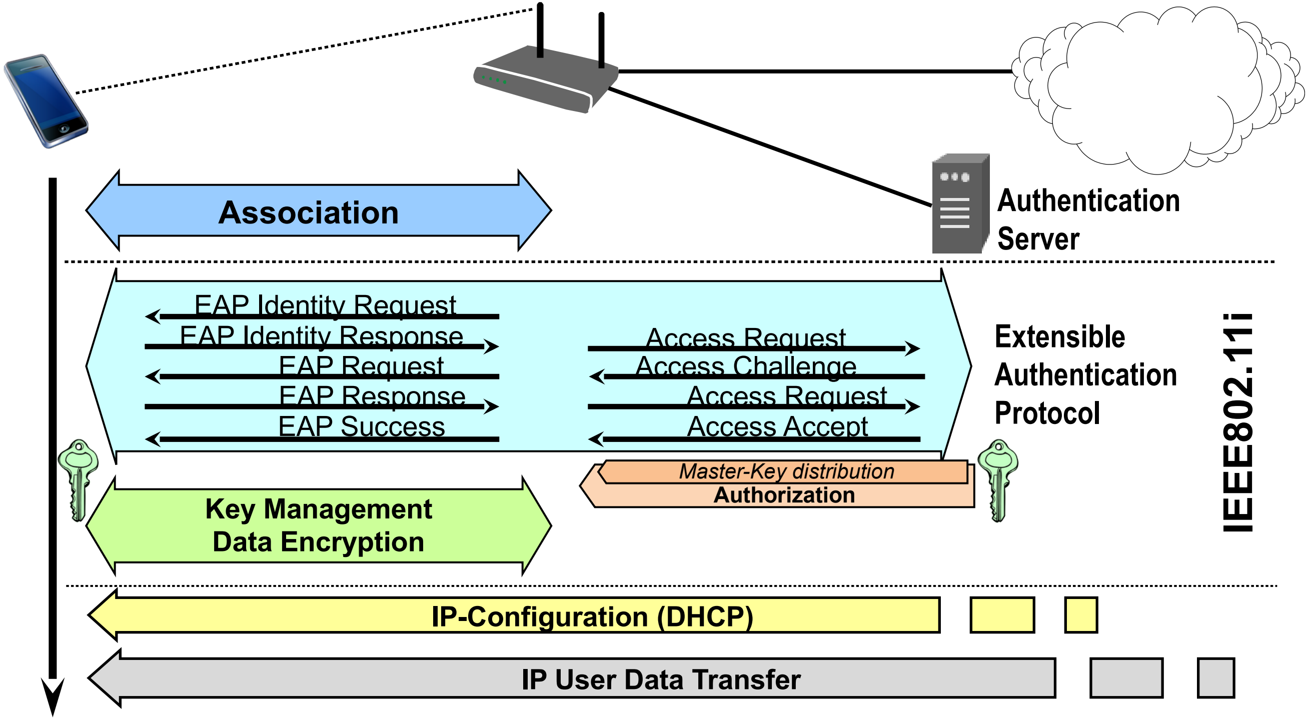
- https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc provides overview of WPA3 certified products.

IEEE 802.11 Security

ROBUST SECURITY NETWORK

IEEE 802.11 Robust Security Network (RSN)

RSN was introduced by IEEE 802.11i-2004



Robust Security Network Components

- Establishes Robust Security Network Associations (RSNAs)
- Comprises:
  - Configuration
  - IEEE 802.1X authentication
  - Key distribution by RADIUS
  - Key management
  - Data protection
    - CCMP (CTR/CBC-MAC Protocol)
      - Counter mode/Cipher Block Chaining Message Authentication Code of AES
      - Achieves both confidentiality and integrity
- Amendment to RSN
  - Protected Management Frames

RSNA establishment

WPA2/3-Personal	**WPA2/3-Enterprise**
RSN Capability identification from Beacon or Probe Response frames	
Open System authentication.	
Cipher suite negotiation during the association process	
Case of STA and AP supporting	
PSK/SAE	802.1X Authentication
Derive Pairwise Master Key from Pre-Shared Key	IEEE Std 802.1X-2004 Authentication Derive Pairwise Master Key
Establish temporal keys by executing 4-way key management algorithm for pairwise keys and group key management for broadcast keys	
Protect the data link by operation of ciphering and message authentication with keys generated above.	
If Protected Management Frame (PMF) is enabled, the temporal keys and pairwise cipher suite is used for protection of individually addressed robust management frames	

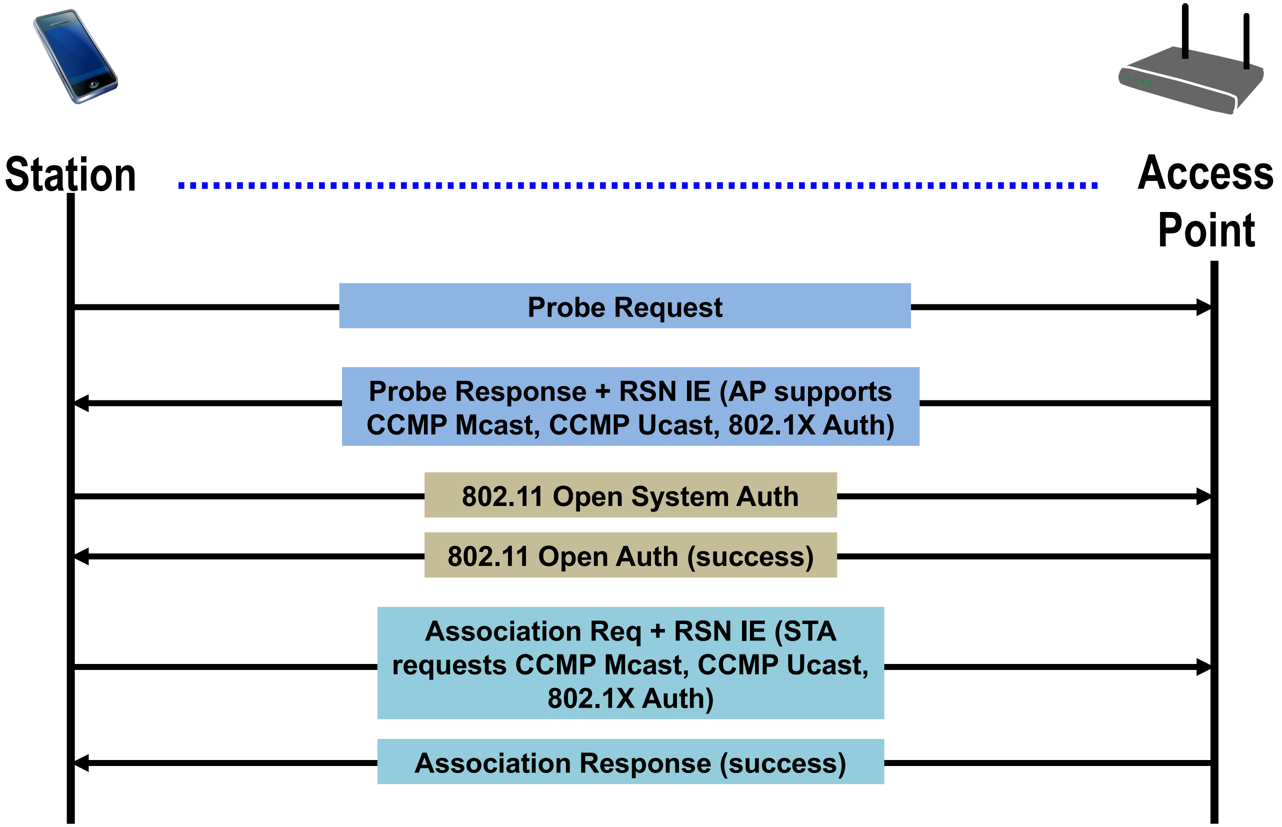
Robust Security Network

CONFIGURATION

Configuration

- Security requires networks with “right” characteristics
- AP advertises capabilities in Beacon, Probe Response
  - SSID in Beacon, Probe provides hint for right authentication credentials
  - RSN Information Element advertises all enabled authentication suites, all enabled unicast cipher suites and multicast cipher suites
- At the end of discovery STA knows
  - SSID of the network
  - Authentication and cipher suites of the network
  - The preferred choice of authentication and cipher suites
- STA selects authentication suite and unicast cipher suite in Association Request
  - STA and AP have an established Ethernet link
  - STA and AP are ready to authenticate by 802.1X

Configuration process

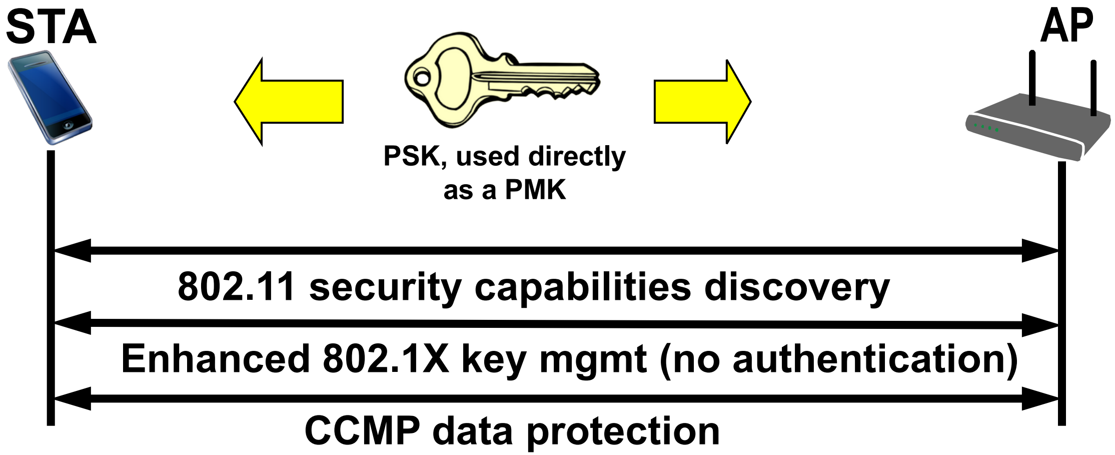


Station
Access Point
Probe Request
Probe Response + RSN IE (AP supports CCMP Mcast, CCMP Ucast, 802.1X Auth)
802.11 Open System Auth
802.11 Open Auth (success)
Association Req + RSN IE (STA requests CCMP Mcast, CCMP Ucast, 802.1X Auth)
Association Response (success)

Robust Security Network

PSK/SAE AUTHENTICATION (WPA2/3-PERSONAL)

PSK Authentication

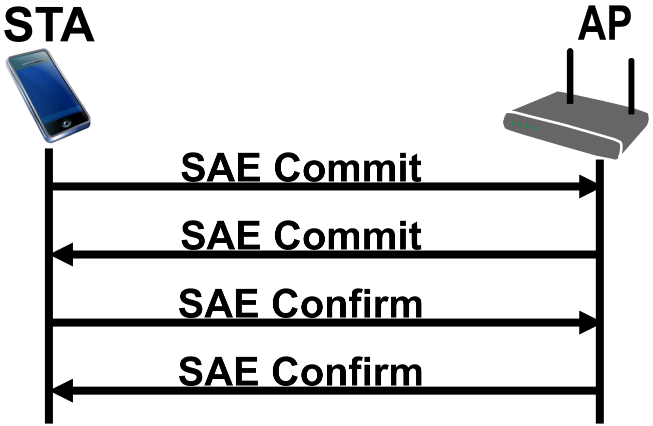

STA
AP
PSK, used directly as a PMK
802.11 security capabilities discovery
Enhanced 802.1X key mgmt (no authentication)
CCMP data protection

- Password-to-Key Mapping
  - Uses PKCS #5 v2.0 PBKDF2 (RFC2898; Public Key Cryptography Specification #5 v2.0, Password Based Key Derivation Function #2), to generate a 256-bit PSK from an ASCII password
  - Quality of PSK depends on quality of ASCII password!
- Reason to provide PSK-Mode:
  - Home users might configure passwords, but will never configure keys

WPA3-Personal deploys SAE for key generation

- Replacement of PSK through Simultaneous Authentication of Equals (SAE)
  - SAE is available in IEEE 802.11 through IEEE 802.11s amendment for authentication and encryption among mesh partners.
  - Resistant to offline dictionary attacks to determine the network password
    - Requires repeated active attacks for each guess of the password
  - Provides forward secrecy
    - Even if the password is compromised at some point in the future, data sent prior to the compromise is protected
  - Retains the ease-of-use and system maintenance associated with WPA2-Personal
- WPA3-Personal Transition Mode allows for gradual migration while maintaining interoperability with WPA2-Personal devices

Simultaneous Authentication of Equals



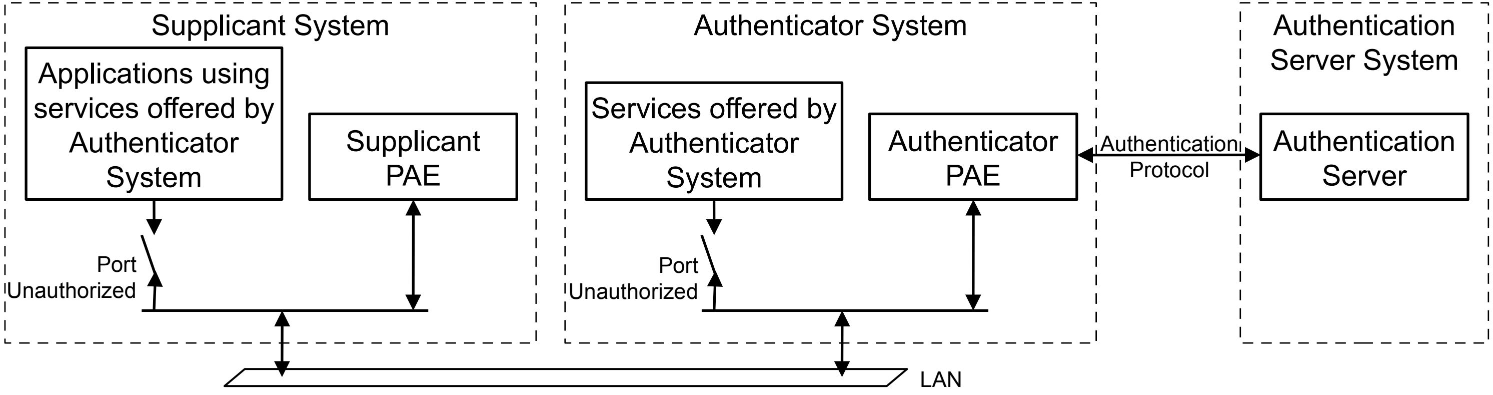
- SAE is based on a Dragonfly handshake as defined in RFC 7664
- Authenticates two peers using only a password, resulting in a shared secret between the two peers that can subsequently be used for secret communication.
- The SAE handshake negotiates a fresh Pairwise Master Key (PMK) per client, which is then used in a traditional Wi□Fi four-way handshake to generate session keys.
- It provides a secure alternative to using certificates or when a centralized authority is not available.
- Neither the PMK nor the password credential used in the SAE exchange can be obtained by a passive attack, active attack, or offline dictionary attack.

Robust Security Network

802.1X AUTHENTICATION (WPA2/3-ENTERPRISE)

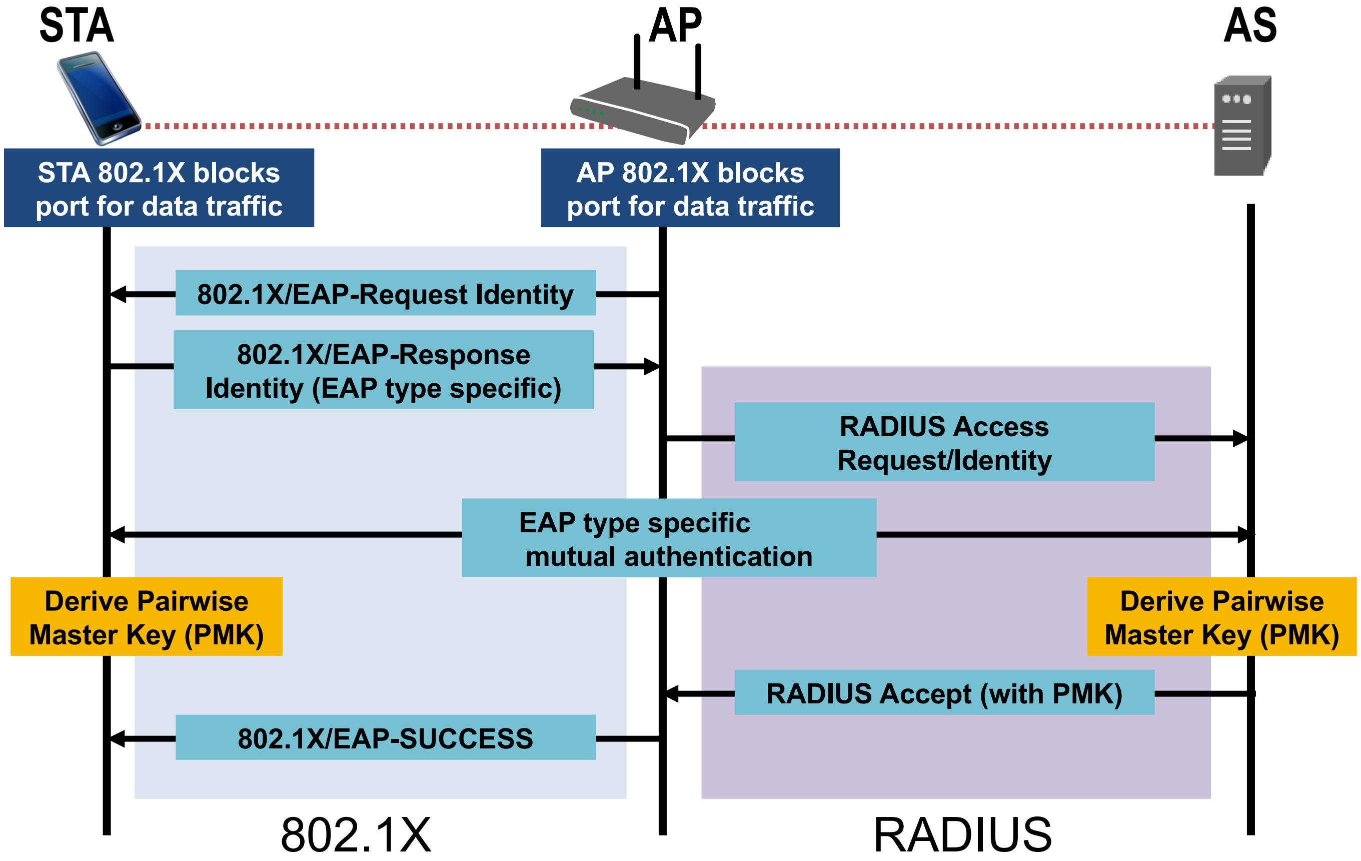
IEEE 802.1X aka EAPoL (EAP over LAN)

- Inherits EAP architecture (RFC 3748, RFC 5247)
  - “Authenticator” located in AP, “Supplicant” located in STA
  - Transport for EAP messages over IEEE 802 LANs



- Deploys Port Authentication Entity (PAE) with uncontrolled port and controlled port.
- IEEE 802.1X/EAP provides no cryptographic protections
  - No defense against forged EAP-Success, relies on EAP method to detect all attacks
  - “Mutual” authentication and binding must be inherited from EAP method

802.1X Message flow


STA
AP
AS
STA 802.1X blocks port for data traffic
AP 802.1X blocks port for data traffic
802.1X/EAP-Request Identity
802.1X/EAP-Response Identity (EAP type specific)
RADIUS Access Request/Identity
EAP type specific mutual authentication
Derive Pairwise Master Key (PMK)
Derive Pairwise Master Key (PMK)
RADIUS Accept (with PMK)
802.1X/EAP-SUCCESS
802.1X
RADIUS

802.1X Authentication

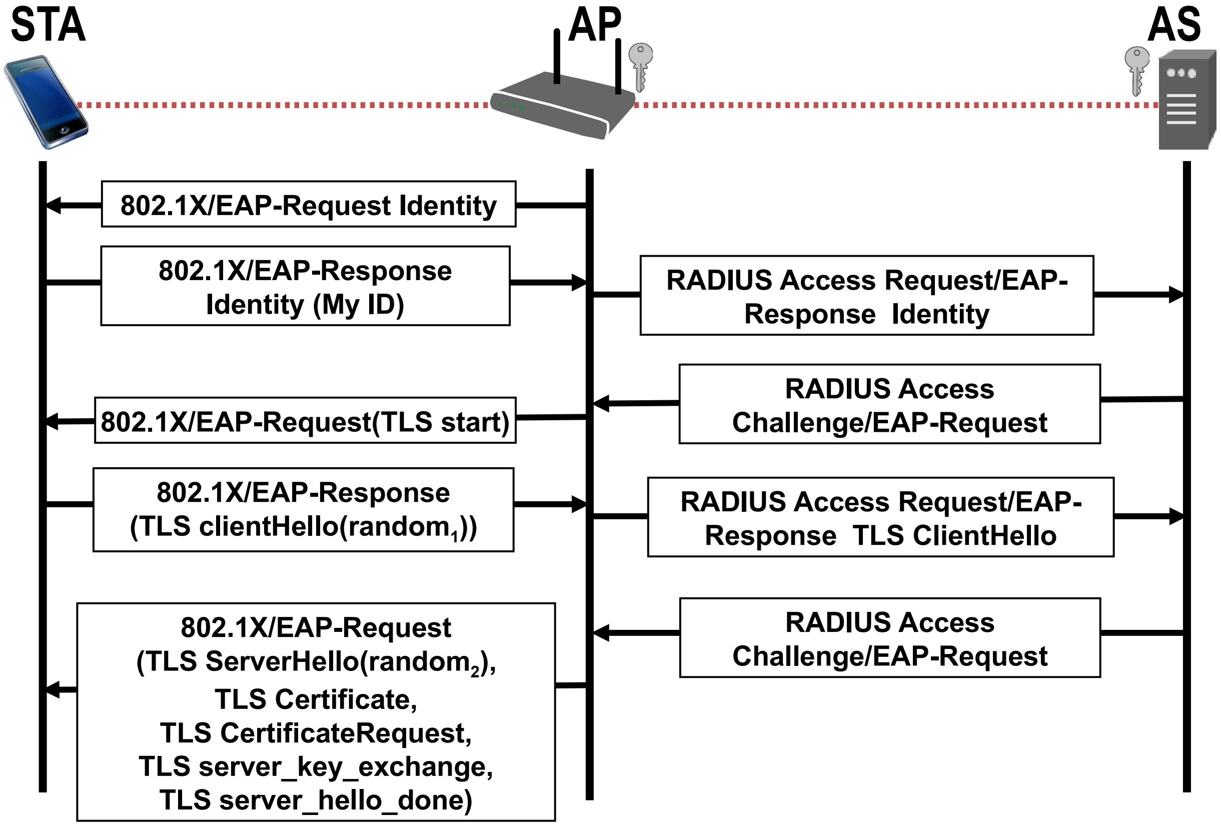
- Establishment of a mutually authenticated session key between Authentication Server (AS) and STA
  - Session ⇒ key is fresh
  - Mutually authenticated ⇒ bound only to AS and STA
- Authentication method defends against eavesdropping, man-in-the-middle attacks, forgeries, replay, dictionary attacks against either party

- At the end of authentication:
  - The AS and STA have established a session bound to a mutually authenticated Master Key
  - Delivered by EAP method
    - AS has forwarded PMK to the AP
- Identity protection not a goal
  - MAC addresses are not hidden
  - However, identities can protected by random MAC addresses and tunneled EAP methods

EAP Menthods, e.g. EAP-TLS

- EAP-TLS is not part of 802.11i;
  - neither is any other specific authentication method
- But EAP-TLS is the initial solution of an EAP method for IEEE 802.11
  - Can meet all IEEE 802.11 requirements
    - Other widely deployed methods do not
- EAP-TLS = TLS Handshake over EAP
  - EAP-TLS defined by RFC 5216, TLS defined by RFC 2246
  - Must have the capability to verify the identity of the peer
    - Requires deployment of public key infrastructure
    - Mutual authentication requires X.509 certificates for both, STA and Authentication Server

802.1X Authentication with EAP-TLS (1)



802.1X/EAP-Request Identity

802.1X/EAP-Response Identity (My ID)

RADIUS Access Request/EAP-Response Identity

RADIUS Access Challenge/EAP-Request

802.1X/EAP-Request(TLS start)

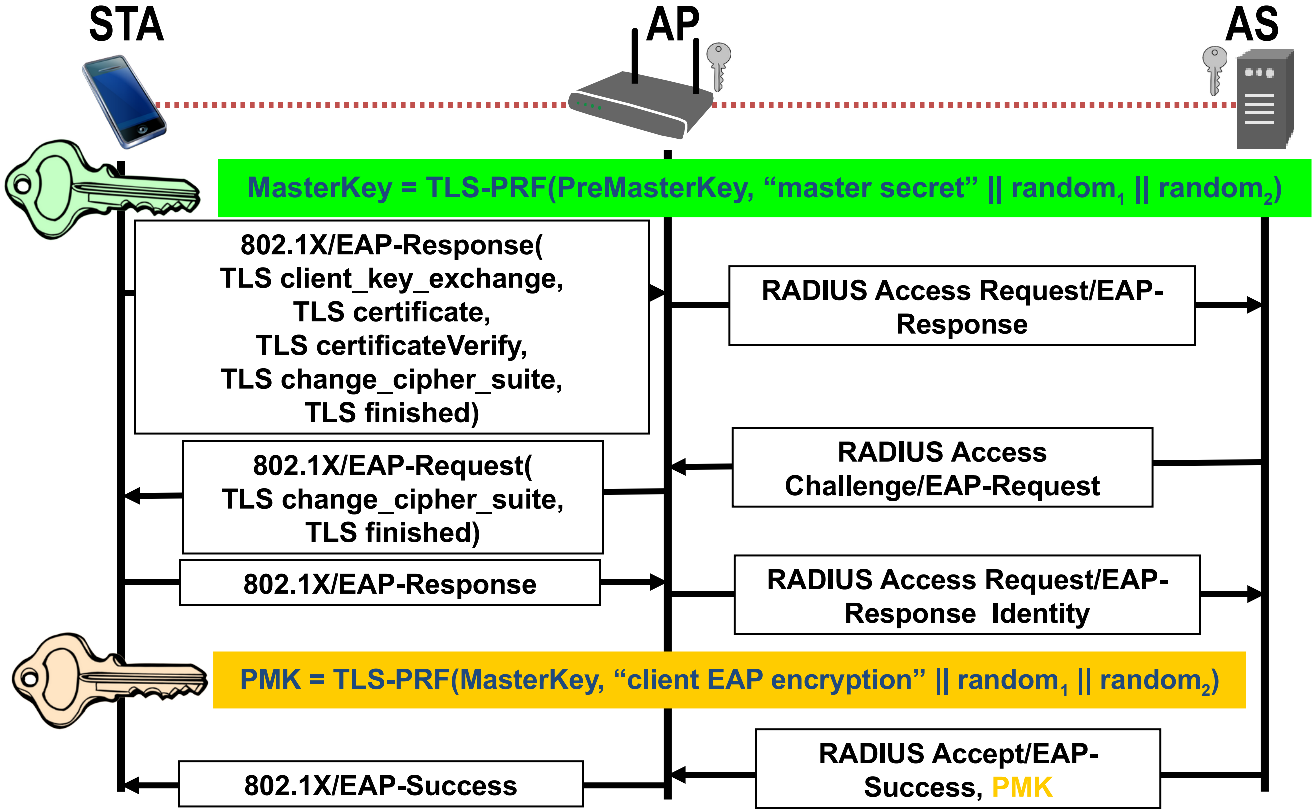
802.1X/EAP-Response (TLS clientHello(random$_1$))

RADIUS Access Request/EAP-Response TLS ClientHello

RADIUS Access Challenge/EAP-Request

802.1X/EAP-Request
(TLS ServerHello(random$_2$),
TLS Certificate,
TLS CertificateRequest,
TLS server_key_exchange,
TLS server_hello_done)

802.1X Authentication with EAP-TLS (2)



STA

AP

AS

MasterKey = TLS-PRF(PreMasterKey, “master secret” || random$_1$ || random$_2$)

802.1X/EAP-Response(
TLS client_key_exchange,
TLS certificate,
TLS certificateVerify,
TLS change_cipher_suite,
TLS finished)

RADIUS Access Request/EAP-Response

802.1X/EAP-Request(
TLS change_cipher_suite,
TLS finished)

RADIUS Access Challenge/EAP-Request

802.1X/EAP-Response

RADIUS Access Request/EAP-Response Identity

PMK = TLS-PRF(MasterKey, “client EAP encryption” || random$_1$ || random$_2$)

802.1X/EAP-Success

RADIUS Accept/EAP-Success, PMK

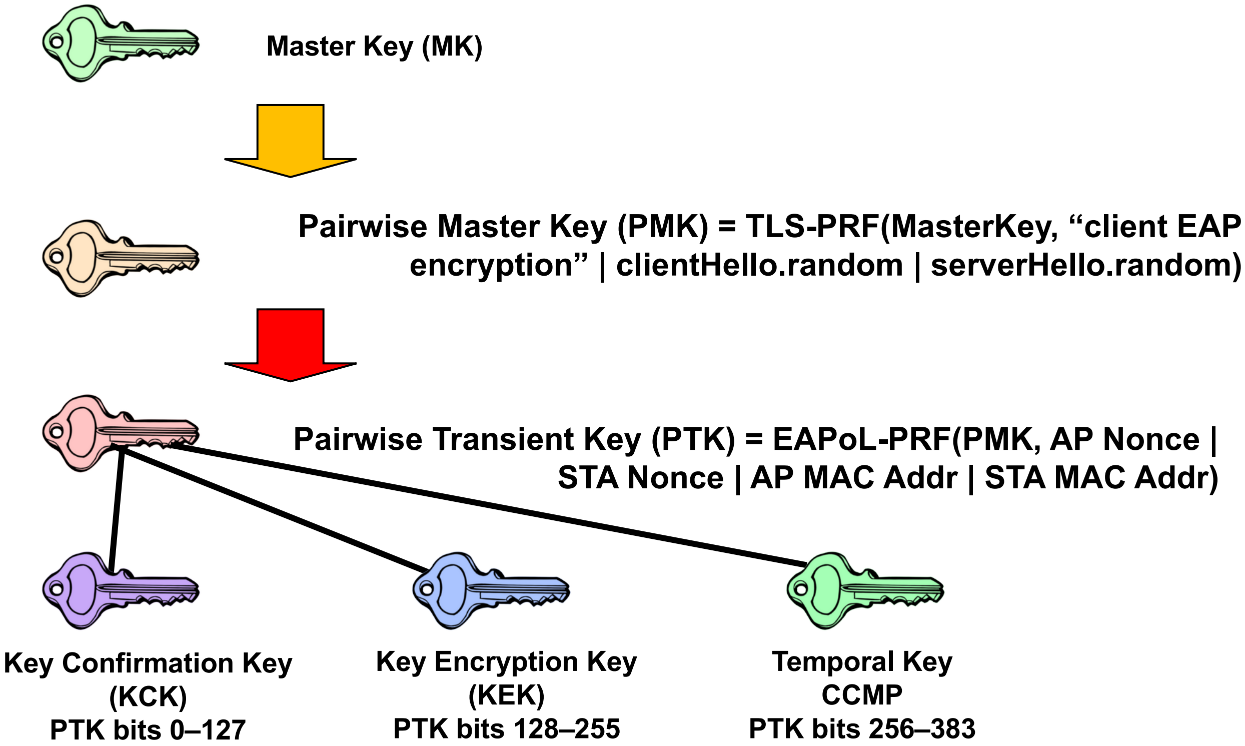
Robust Security Network

KEY MANAGEMENT

Key Management

- Redesigned by P802.11i to fix original 802.1X key management
  - Derive a Pairwise Master Key (PMK)
  - AP and STA use PMK to derive Pairwise Transient Key (PTK)
  - Use PTK to protect the link
- Limitations:
  - No explicit binding to earlier association, authentication
  - Keys are only as good as back-end allows
- 4-Way Handshake
  - Establishes a fresh pairwise key bound to STA and AP for this session
  - Proves liveness of peers
  - Demonstrates there is no man-in-the-middle between PTK holders if there was no man-in-the-middle holding the PMK
  - Synchronizes pairwise key use
- Group Key Handshake provisions group key to all STAs

Pairwise Key Hierarchy



Master Key (MK)

Pairwise Master Key (PMK) = TLS-PRF(MasterKey, “client EAP encryption” | clientHello.random | serverHello.random)

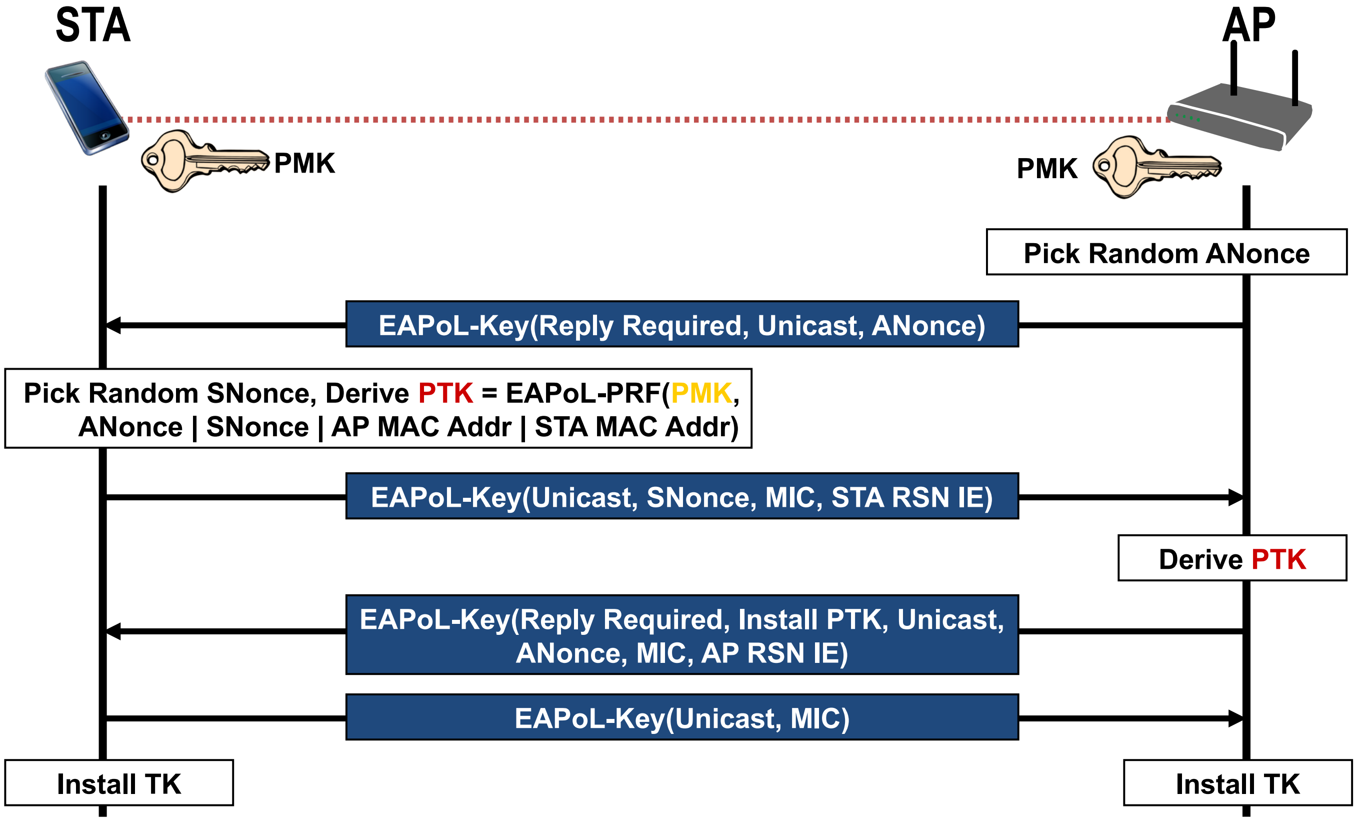
Pairwise Transient Key (PTK) = EAPoL-PRF(PMK, AP Nonce | STA Nonce | AP MAC Addr | STA MAC Addr)

Key Confirmation Key
(KCK)
PTK bits 0–127

Key Encryption Key
(KEK)
PTK bits 128–255

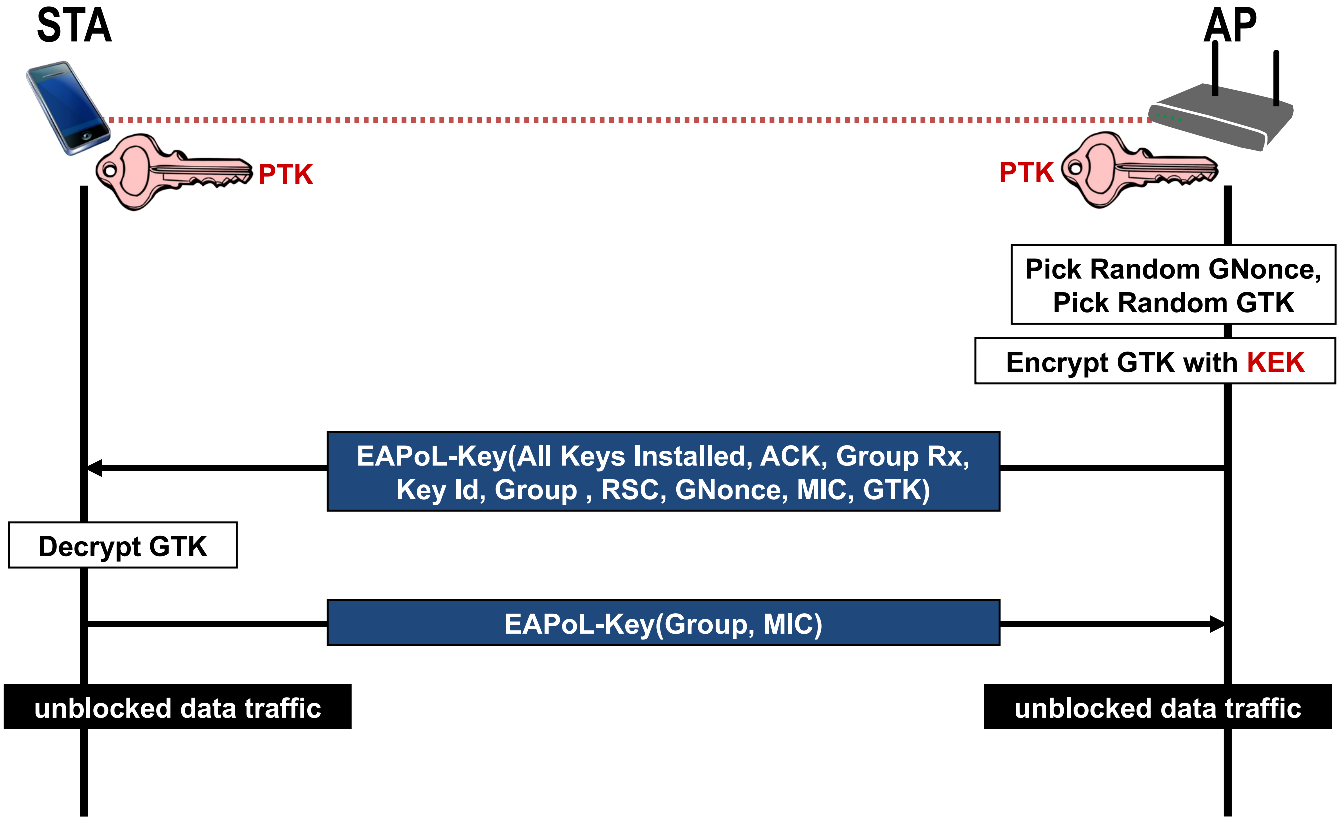
Temporal Key
CCMP
PTK bits 256–383

4-Way Handshake to create Temporal Key



STA
AP
PMK
PMK
Pick Random ANonce
EAPoL-Key(Reply Required, Unicast, ANonce)
Pick Random SNonce, Derive PTK = EAPoL-PRF(PMK, ANonce | SNonce | AP MAC Addr | STA MAC Addr)
EAPoL-Key(Unicast, SNonce, MIC, STA RSN IE)
Derive PTK
EAPoL-Key(Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE)
EAPoL-Key(Unicast, MIC)
Install TK
Install TK

Group Key Handshake



Robust Security Network

DATA PROTECTION

Data Protection Requirements

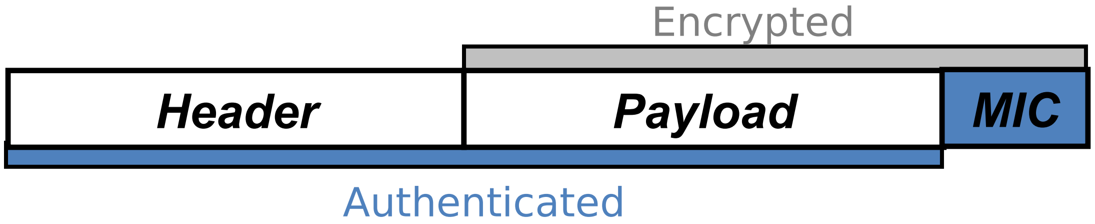
- Never send or receive unprotected packets
- Authenticate message origin
  - Forgeries prevention
- Sequence packets
  - Replay detection
- Avoid rekeying
  - 48 bit packet sequence number
- Protect source and destination addresses
- Use strong cryptography
  - For both, confidentiality and integrity

CCM

- Counter mode with Cipher-block chaining Message authentication code (CCM)
  - A symmetric key block cipher mode providing confidentiality using counter mode (CTR) and data origin authenticity using cipher-block chaining message authentication code (CBC-MAC).
  - See IETF RFC 3610
  - Assumes 128 bit block cipher – IEEE 802.11i uses AES
  - AES realized in hardware
- CCM Properties
  - CCM provides authenticity and privacy
  - CCM is packet oriented
  - CCM can leave any number of initial blocks of the plaintext unencrypted

CCMP (CTR with CBC-MAC Protocol)

- CCMP makes use of CCM to
  - Encrypt packet data payload
  - Protect packet selected header fields from modification



- CBC-MAC used to compute a MIC on the plaintext header, length of the plaintext header, and the payload
- CTR mode used to encrypt the payload and the MIC
- Same 128-bit Temporal Key at both AP and STA
  - Fresh key configured by 802.1X
- Mandatory to implement in all Wi-Fi equipment
- Especially designed for IEEE 802.11i

WPA3-Enterprise

- Introduces an enhanced 192-bit security mode
- Replaces 128-bit CCMP through 256-bit GCMP (Galois/Counter Mode Protocol)
  - GCMP was introduced to IEEE 802.11 through IEEE 802.11ad (WigGig)
  - 256-bit GCMP was used instead of 192-bit GCMP due to broader adoption
- In addition:
  - More secure key derivation and key confirmation through 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
  - More secure key establishment and authentication through Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
  - Used security algorithms are known as ‘Suite B’
- Mandatory support of Protected Management Frames required
- No need for transition mode, but considerations given for interoperability between WPA2-Enterprise and WPA3-Enterprise

Robust Security Network

SUMMARY

Purpose of each phase

- Security negotiation
  - Determine promising parties with whom to communicate
  - AP advertises network security capabilities to STAs
- Authentication based on 802.1X
  - Centralize network admission policy decisions at the AS
  - STA determines whether it does indeed want to communicate
  - Mutually authenticate STA and AS
  - Generate Master Key as a side effect of authentication
  - Use master key to generate session keys = authorization token
- RADIUS-based key distribution
  - AS moves (not copies) session key (PMK) to STA's AP
- Key management by 802.1X
  - Bind PMK to STA and AP
  - Confirm both AP and STA possess PMK
  - Generate fresh operational key (PTK)
  - Prove each peer is live and synchronize PTK use
- Data Protection
  - Encrypt data by CTR (AES)
  - Authenticate data by CBC-MAC (AES)

IEEE 802.11 Security

PROTECTED MANAGEMENT FRAMES

Protected Management Frames (PMF)

- Management frames are used to initiate and tear down sessions
  - E.g.: authentication, de-authentication, association, dissociation, beacon, probe
- Management frames must be transmitted as open
  - To be heard and understood by all clients
- Protection necessary to avoid attacks through forgery
- IEEE 802.11w-2009 provides Protected Management Frames (PMF) service to
  - Disassociation,
  - De-authentication, and
  - Robust Action Frames (IEEE 802.11-2016 Table 9-47).
    - I.e: Spectrum management, QoS, DLS, Block Ack, Radio measurement, Fast BSS Transition, SA Query, WNM, Mesh, Multihop, Vendor specific protected

PMF components and operation

- Broadcast/Multicast Integrity Protocol
  - Adds a MIC calculated based on the shared IGTK key
- Integrity Group Temporal Key (IGTK)
  - Random value, assigned by the broadcast/multicast source STA/AP
    - Protection of its group addressed MAC management protocol data units (MMPDUs)
- Key Distribution:
  - With PMF the AP includes the encrypted GTK and IGTK values in the EAPOL-Key frame
    - Message 3 of 4-way handshake.
  - For later changes of the GTK, AP sends the new GTK and IGTK to the client using the Group Key Handshake.
- Operation
  - Client protection is added by the AP adding cryptographic protection to de-authentication and dissociation frames
  - Infrastructure protection is added by adding a Security Association (SA) tear down protection mechanism.

IEEE 802.11 Security

FAST TRANSITION

Fast BSS Transition

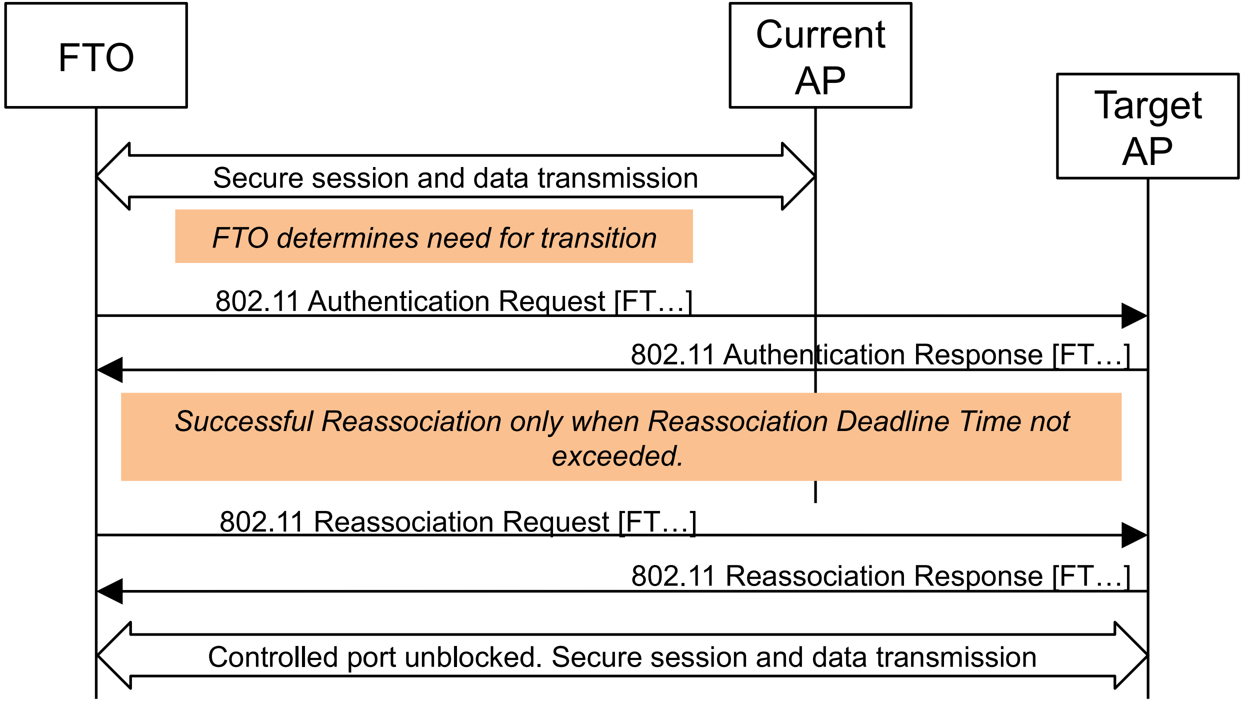
- Fast BSS transition reduces the interruption period between a STA and the DS during BSS transition.
- IEEE 802.11r-2008 supports fast BSS transitions between Aps
  - Key negotiation in IEEE 802.11i requires key renegotiation on every handoff
    - Time consuming process, as shown before for EAP-TLS authentication
  - Redefined the security key negotiation protocol by allowing both the negotiation and user data transmissions to occur in parallel.
- Solution: caching in the wireless network part of the key derived from the server
  - Reasonable number of future connections based on the cached key.
- FT protocols are part of the re-association service
  - Only apply to STA transitions between APs within the same mobility domain within the same ESS.

FT protocol overview

- Protocol initiated during the initial association of FT Originator (FTO) and AP.
  - Initial exchange: FT initial mobility domain association
  - Subsequent re-associations to APs within the same mobility domain may make use of the FT protocols.
- Two FT protocols are defined:
  - FT Protocol when no resource request prior to its transition.
  - FT Resource Request Protocol when a FTO has to request a resource prior to transition.
- Two FT methods:
  - Over-the-Air
  - Over-the-DS
    Between current AP and target AP communication is encapsulated as described in IEEE 802.11-2016: 13.10.3.
- APs advertise both, capabilities and policies for the support of the FT protocols and methods.

Over-the-air Fast Transition

- The FTO communicates directly with the target AP
  - Use of IEEE 802.11 authentication frame with the FT authentication algorithm.



FTO

Current AP

Target AP

Secure session and data transmission

FTO determines need for transition

802.11 Authentication Request [FT…]

802.11 Authentication Response [FT…]

Successful Reassociation only when Reassociation Deadline Time not exceeded.

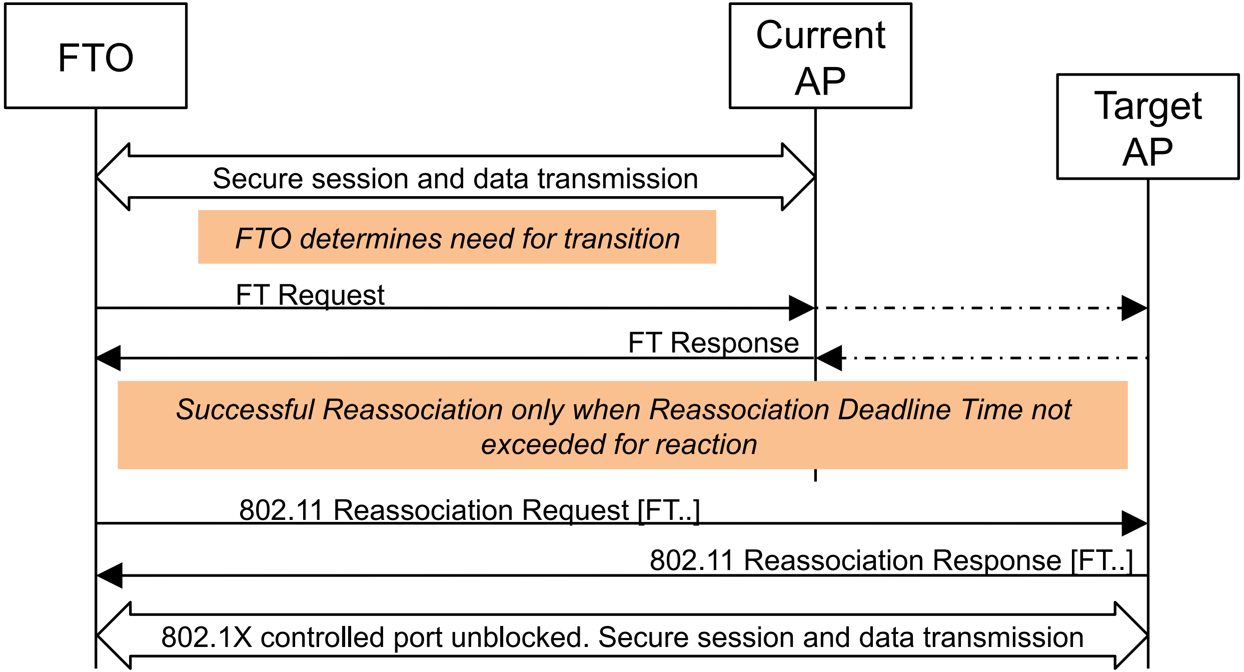
802.11 Reassociation Request [FT…]

802.11 Reassociation Response [FT…]

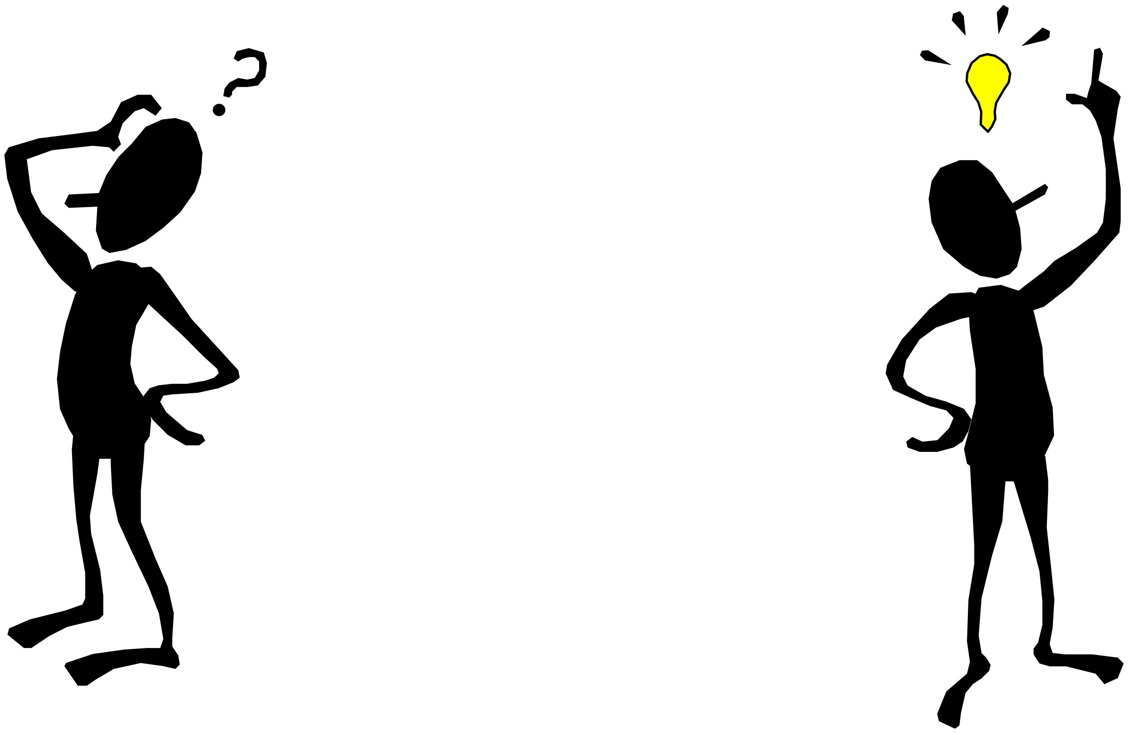
Controlled port unblocked. Secure session and data transmission

Over-the-DS Fast Transition

- The FTO communicates with the target AP via the current AP.
  - The communication between the FTO and the target AP is carried in FT Action frames between the FTO and the current AP.


FTO
Current AP
Target AP
Secure session and data transmission
FTO determines need for transition
FT Request
FT Response
Successful Reassociation only when Reassociation Deadline Time not exceeded for reaction
802.11 Reassociation Request [FT..]
802.11 Reassociation Response [FT..]
802.1X controlled port unblocked. Secure session and data transmission

Questions and answers



Questions…

Security

1) What are the initial MAC management message exchanges before the EAP authentication exchange?
2) What does RSN mean?
3) What is the purpose of IEEE 802.1X?
4) What were the deficiencies of WEP aside of missing user authentication and mutual authentication?
5) Which IEEE 802.11 amendment fixed the bugs of WEP?
6) Which cryptographic methods are used by RSN of IEEE 802.11i?
7) What kind of authentication is supported by IEEE 802.11i?
8) Which name is used by Wi-Fi Alliance to denote the certification of IEEE 802.11i security based on AES encryption?
9) What is the difference between WPA2-Enterprise and WPA2-Personal?
10) Which authentication protocol is used in the Robust Security Network?
11) What is the outcome of the configuration phase in the Robust Security Network?
12) What are the peer entities of the EAP protocol in IEEE 802.11i?
13) How is the master key transferred from the AAA server to the AP?

More questions…

Security, cont.

14) Which peer entities create the PMK used for the user data encryption in WPA2-Enterprise?
15) Where is the supplicant located used in WPA2-Enterprise?
16) What is the function of the PAE in IEEE 802.1X?
17) What kind of credentials are used in EAP-TLS to identify the peers?
18) Why was the PSK method introduced in WPA?
19) Which key is used for input to the 4-way handshake in RSN?
20) What is the purpose of the group key in IEEE 802.11?
21) Which default key length is used in RSN for AES?
22) Why is it important that CCMP protects but does not encrypt the header part of a WLAN frame?
23) What is the purpose of Protected Management Frames?
24) What is the purpose of Fast BSS Transition?
25) How can the Fast Transition Originator communicate with the Target AP?

Anything left for today?

See you again next week:-).