WLAN as a service for IoT

Max Riegel

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
- Chair of IEEE 802.1 OmniRAN Task Group

WLAN as a service for IOT

TABLE OF CONTENT

Overview

- WLAN for IoT
- Standardization Environment
- WLAN System Architecture
- Wi-Fi Radio for 2.4 & 5 GHz
- IEEE 802.11ah SUB 1 GHz (HaLow)
- IEEE 802.11 Security
- Secure WLAN Operation
- Key Concepts of network Virtualization
- Virtualized WLAN Access for IoT

WLAN as a service for IOT

WLAN FOR IOT

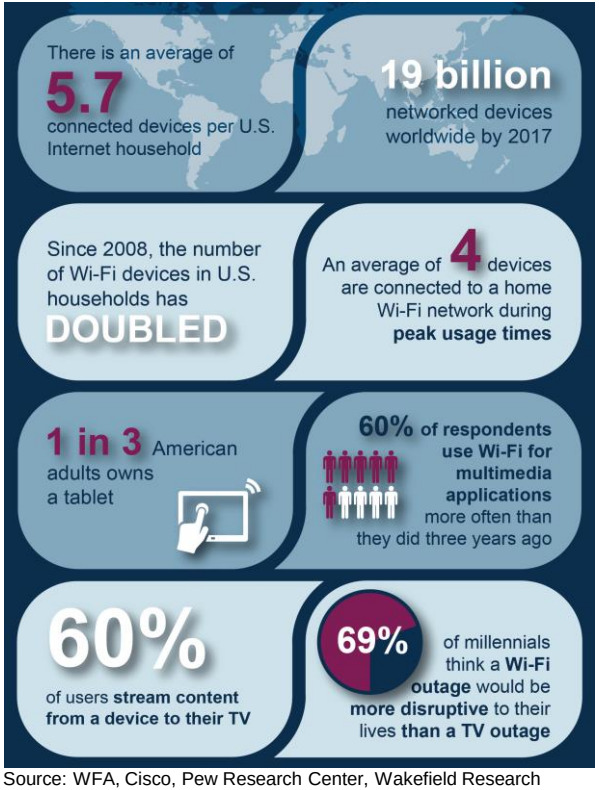
WLAN fits well to cloud-based IoT applications

- WLAN technology fulfills IoT requirements
  - Simple, robust, broadband, low-power
  - Many powerful, cost-effective SoCs
  - Global technology for all markets
  - Widely deployed in residential and enterprises
  - Access is available nearly everywhere for ‘free’

- WLAN is technology of choice for integration with cloud
  - Cloud is the most dynamic environment for service creation
  - WLAN provides transparent Internet connectivity
  - No local gateway functionality needed – just put and play

Diversity of Wi-Fi terminals and access infrastructure

Wi-Fi is predominantly deployed in homes and indoors



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

WLAN as a service for IOT

STANDARDIZATION ENVIRONMENT

IEEE 802.11 and Wi-Fi Alliance

The IEEE 802.11 provides comprehensive technical specifications

Standards Framework

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

Compatibility Conformance

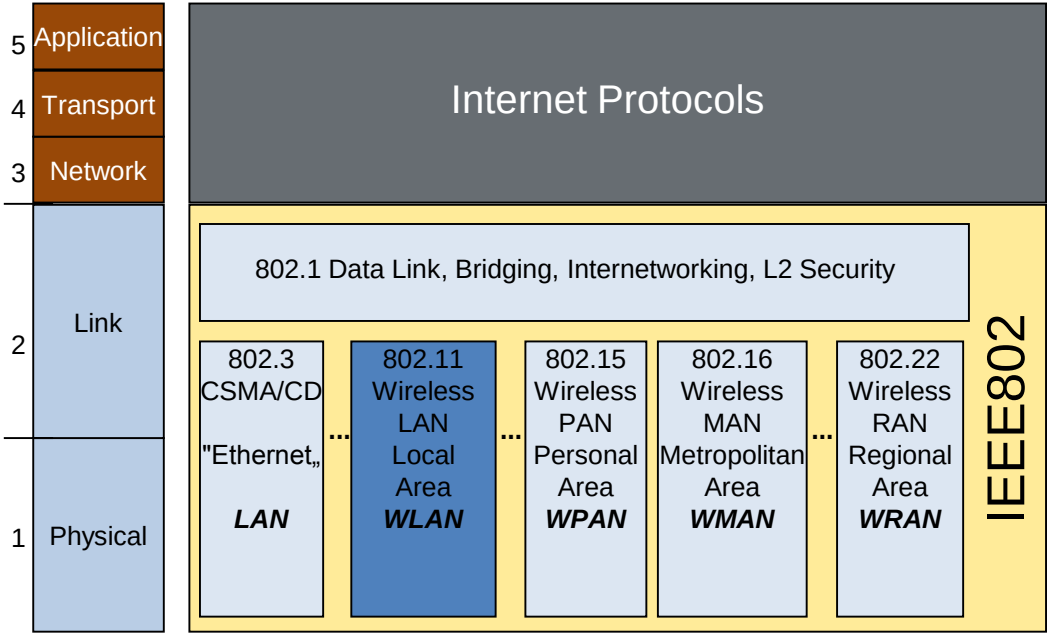
IEEE802.11 (Wi-Fi) radio standards evolution

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	2000	up to 6 700	1	SC/OFDM	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	20/40/ 80/160	tbd (~ 1.3 Gbps)	8	OFDMA	~ 80	~ 300
ay	~ 2020*	60	up to 6 GHz	> 25 Gbps	tbd	tbd	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

IEEE 802 LAN/MAN Standardization Committee

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



- Start of IEEE Computer Society Project 802 in February 1980.
  - Later renamed to “LMSC”: LAN/MAN Standardization Committee
- Initial Work was on “Ethernet” with 1 to 20 Mbps
- IEEE 802.11 started in 1990
  - Initially aimed for linking 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

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

IEEE Std 802.11™-2016 + amendment 802.11ah

- 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/802.11ah-2016.pdf
- No all the features specified in the standard are available in real Wi-Fi products
- Where appropriate presentation adopts 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

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

- Revision of IEEE Std 802.11-2012
  - Previous revisions: IEEE Std 802.11-2007 and IEEE Std 802.11-1999
  - Initial 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

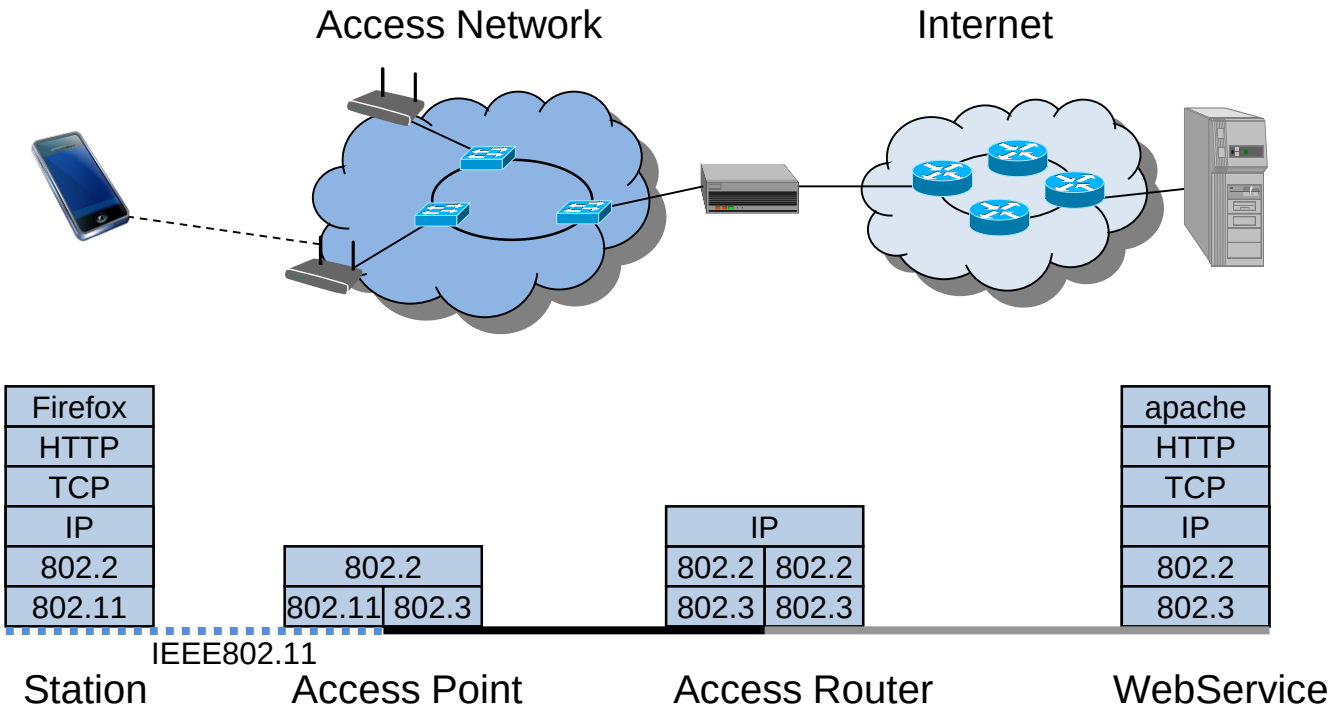
Amendment IEEE Std 802.11ah-2016

- Amendment 2: Sub 1 GHz License Exempt Operation

WLAN as a service for IOT

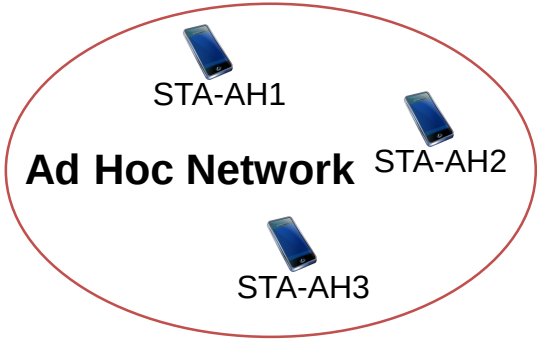
WLAN SYSTEM ARCHITECTURE

WLAN Access protocol architecture for the Internet

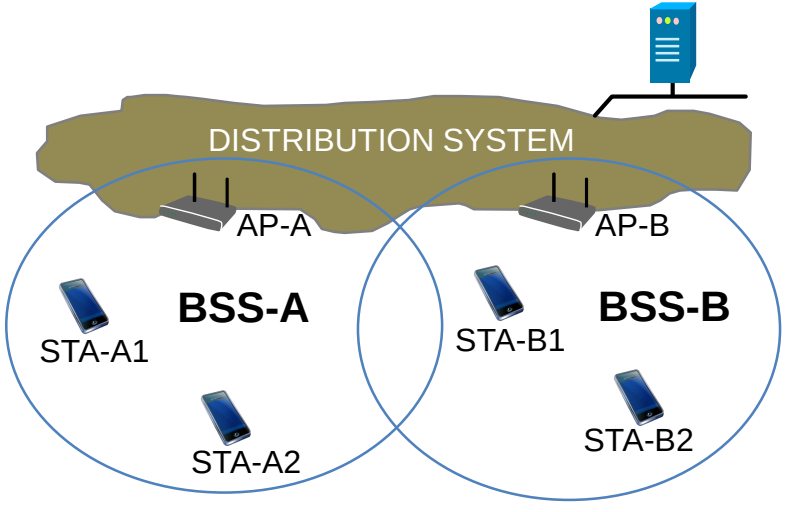


IEEE802.11 Configurations

- 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)
- Power savings (Sleep intervals)

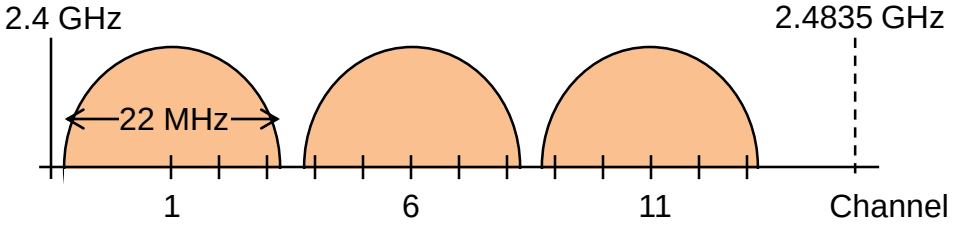
WLAN as a service for IOT

WI-FI RADIO FOR 2.4 & 5 GHZ

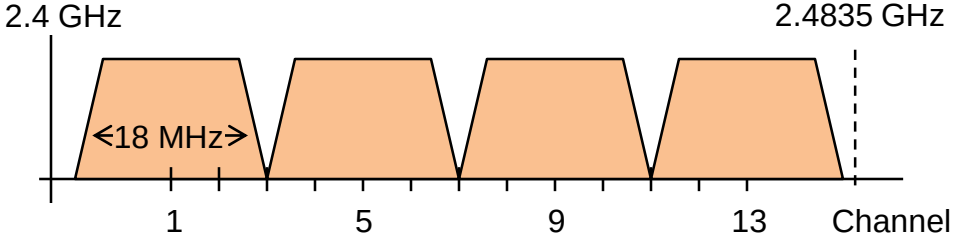
Wi-Fi in the 2.4 GHz ISM band

- Most of Wi-Fi today operate in the 2.4 GHz ISM band
  - IEEE 802.11b set the rule to deploy systems on channel 1 – 6 – 11
  - Plain IEEE 802.11 g/n (OFDM) systems would not interfere when operation on channel 1 – 5 – 9 – 13
- Avoid interference with two adjacent channels by configuration of channels in the middle.
- Regulatory requirements:
  - max TX power (EU): 100 mW EIRP
  - Use of spread spectrum coding
  - Specification: ETSI EN 300 328

DSSS/CCK (802.11b) channel bandwidth 22 MHz

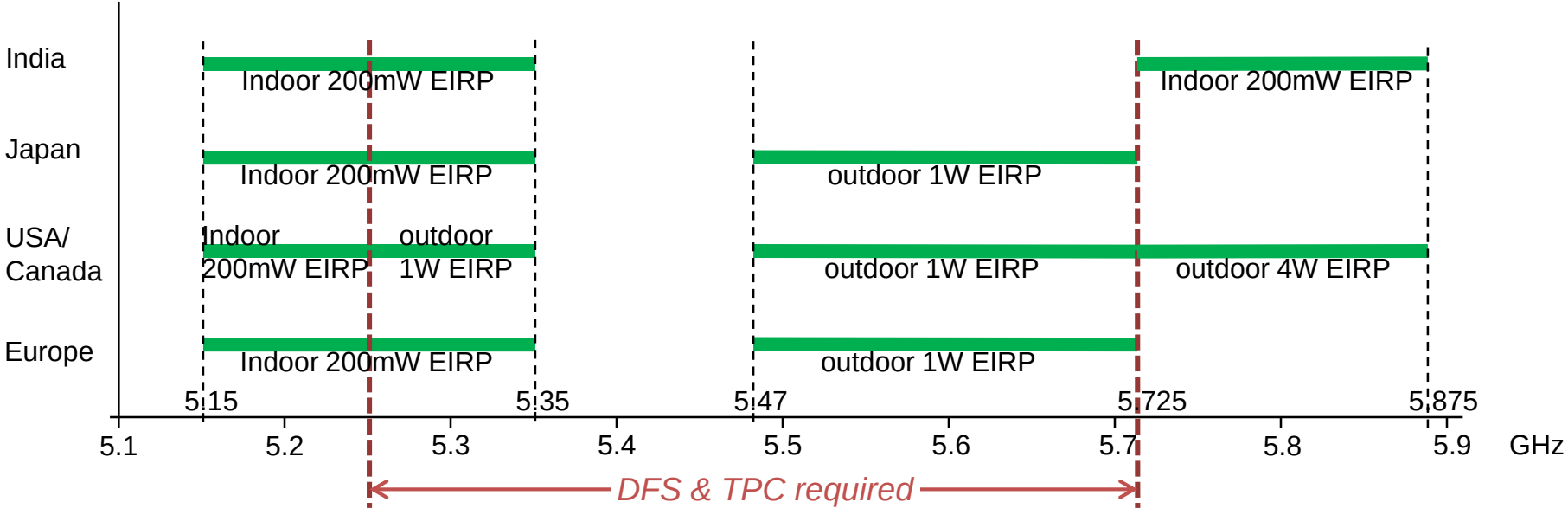


OFDM (802.11g/802.11n) 20 MHz channels



5 GHz Unlicensed Spectrum

- 455 MHz of unlicensed spectrum available mostly worldwide
  - Wi-Fi is usually secondary user of that spectrum



- Dynamic Frequency Selection (DFS) and Transmission Power Control (TPC) are required for most of the 5 GHz spectrum to protect primary users (e.g. weather radars)
  - Specification: ETSI EN 301 893

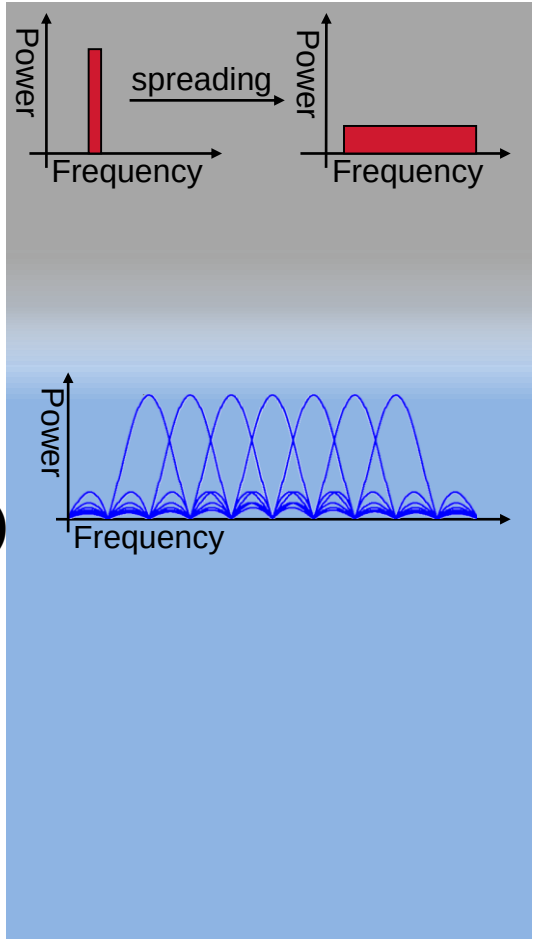
IEEE 802.11 radio standards evolution

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	2000	up to 6 700	1	SC/OFDM	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	20/40/ 80/160	tbd (~ 1.3 Gbps)	8	OFDMA	~ 80	~ 300
ay	~ 2020*	60	up to 6 GHz	> 25 Gbps	tbd	tbd	line of sight	

* Preliminary information; specifications still in early phases of development.
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power

IEEE802.11 PHY layer solutions for 2.4 GHz & 5 GHz

- 2.4 GHz Direct Sequence Spread Spectrum
  - DBPSK/DQPSK providing 1/2 Mbps
  - Channel bandwidth: 22 MHz
- 2.4 GHz High Rate DSSS **(802.11b)**
  - CCK/DQPSK providing 5.5/11 Mbps
  - Channel bandwidth: 22 MHz
- 2.4 GHz Extended Rate **(802.11g)**
  - DSSS providing 1/2/5.5/11 Mbps
  - OFDM providing 6/9/12/18/24/36/48/54 Mbps
  - Channel bandwidth: 22/20 MHz
- 5 GHz Orthogonal Frequency Division Multiplex **(802.11a)**
  - OFDM providing 6/9/12/18/24/36/48/54 Mbps
  - Channel bandwidth: 20 MHz
- 2.4 GHz & 5 GHz High Throughput **(802.11n)**
  - OFDM with up to 4x4 MIMO providing up to 600 Mbps
  - Channel bandwidth: 20 MHz & 40 MHz
- 5 GHz Very High Throughput **(802.11ac)**
  - OFDM with up to 8x8 MU-MIMO providing up to 6900 Mbps
  - Channel bandwidth: 20 MHz, 40 MHz, 80 MHz, 160 MHz



WLAN as a service for IOT

IEEE 802.11AH SUB 1 GHZ (HALOW)

Unlicensed spectrum below 1 GHz

- Frequencies below 1 GHz provide link budget benefits of at least 10dB
  - Well suited for applications requiring longer reach and low power consumption
- Band allocation for some countries:

Country	Frequency [MHz]	max. allowed channel BW [MHz]	max. transmission power EIRP [mW]
China	775 - 779	1	5
	779 - 787	not defined	10
Europe	863 – 868.6	not defined	25
Japan	915.9 – 929.7	1	2 / 40
	920.5 – 923.5		500
South Korea	917 – 923.5	not defined	3 / 10
United States	902 - 928	not defined	1000

- Availability of spectrum and allowed operational parameters for Wi-Fi below 1 GHz strongly depends on the geographic area.

IEEE802.11 (Wi-Fi) 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	2000	up to 6 700	1	SC/OFDM	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	~ 2019*	1...6	20/40/ 80/160	tbd (~ 1.3 Gbps)	8	OFDMA	~ 80	~ 300
ay	~ 2019*	60	up to 6 GHz	> 25 Gbps	tbd	tbd	line of sight	

* Preliminary information; specifications still in early phases of development.
IEEE 802.11y-2008 is only licensed in the United States by the FCC; licensed spectrum allows for higher TX power

Wi-Fi HaLow (IEEE 802.11ah)

Wi-Fi operating in frequency bands below 1 GHz for IoT and extended range

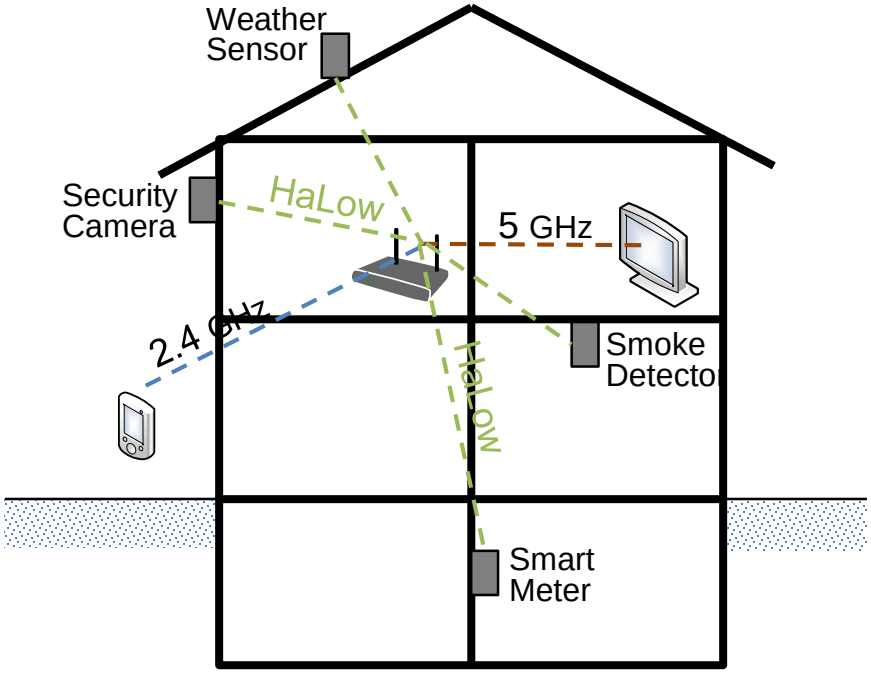
- Increased range compared to traditional Wi-Fi
  - For frequency bands below 1GHz with at least 10 dB link budget advantage
  - Reluctant to larger delay spread and Doppler spread supporting outdoor operation
  - An extra robust 1 MHz mode (MCS10) for up to 1 km range
- No need for interoperability with legacy IEEE 802.11
- Two types of device configurations:
  - IEEE 802.11ah-only for IoT-type connectivity
  - Multi-band devices
- Low Power Consumption
  - Multi-year battery life operation for sensors
- Rich Data Sets
  - 150Kbps ~ 87 Mbps per spatial stream
- Scalable bandwidth and MIMO support
  - 1, 2, 4, 8, 16 MHz channel; up to 4 parallel streams
- Scalable
  - Supports up to 8191 devices per AP
- IP Connectivity
  - Same as Wi-Fi

	Edge Rate (Range)	TxR
11ac/n 5 GHz 20 MHz BW 40 MHz BW	6.5 Mbps (27m)	3x2
11n/g 2.4 GHz 20 MHz BW	6.5 Mbps (54m)	3x2
11ah 900 MHz 8 MHz BW (US Only)	5.8 Mbps (88m)	2x2

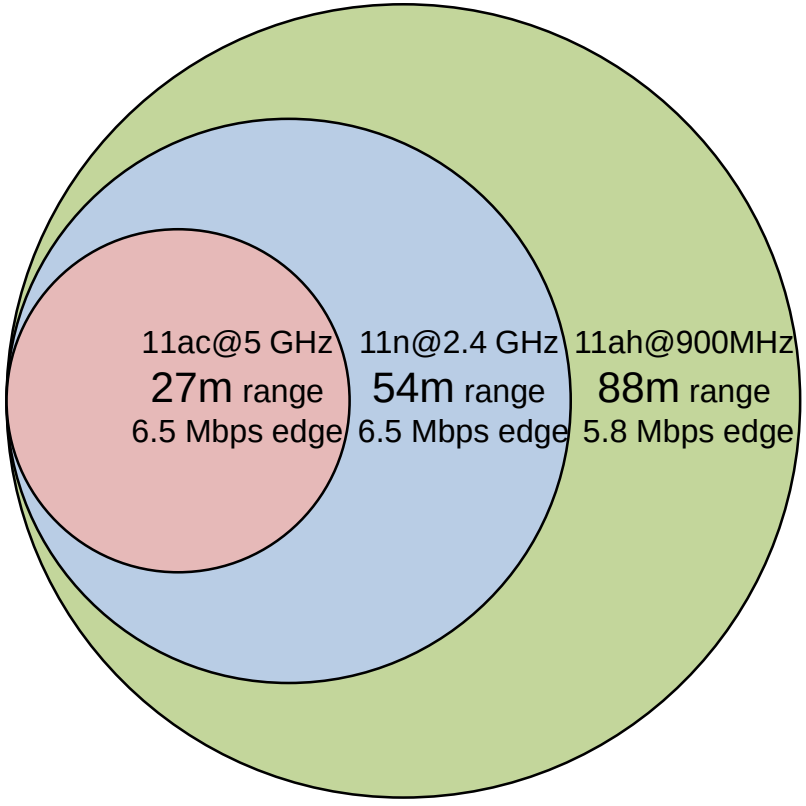
Simulation Assumptions: Minimum QoS 5Mbps, Retail AP, 21 dBm/Tx chain Tx power, Indoor to outdoor (d^4) channel model

HaLow (802.11ah) use cases

Sensors and meters



Extended range



HaLow (802.11ah) basic PHY features

- 150 kbps – 346 Mbps data rates

Channel Bandwidth	Data rates for 1SS	Data rates for 2SS
1 MHz	150 kbps – 4.44 Mbps	600 kbps – 8.88 Mbps
2 MHz	650 kbps – 8.67 Mbps	1.3 Mbps – 17.3 Mbps
4 MHz	1.35 Mbps – 20 Mbps	2.7 Mbps – 40 Mbps
8 MHz	2.9 Mbps – 43.3 Mbps	5.8 Mbps – 87 Mbps
16 MHz	5.8 Mbps – 87 Mbps	11.7 Mbps – 173 Mbps

- 2, 4, 8, or 16 MHz channel bandwidth
  - 802.11ac OFDM design on a tenth clocking rate, i.e. 31.25 kHz spacing
  - Symbol length ten times of that in 802.11ac.
  - Up to 4x4 MIMO
- 1 MHz channel bandwidth:
  - 24 data subcarriers per OFDM symbol maintaining 31.25 KHz spacing
  - MCS 10 added for single stream long range transmission w/ 150 kbps
    - For sensing-type applications requiring extended range

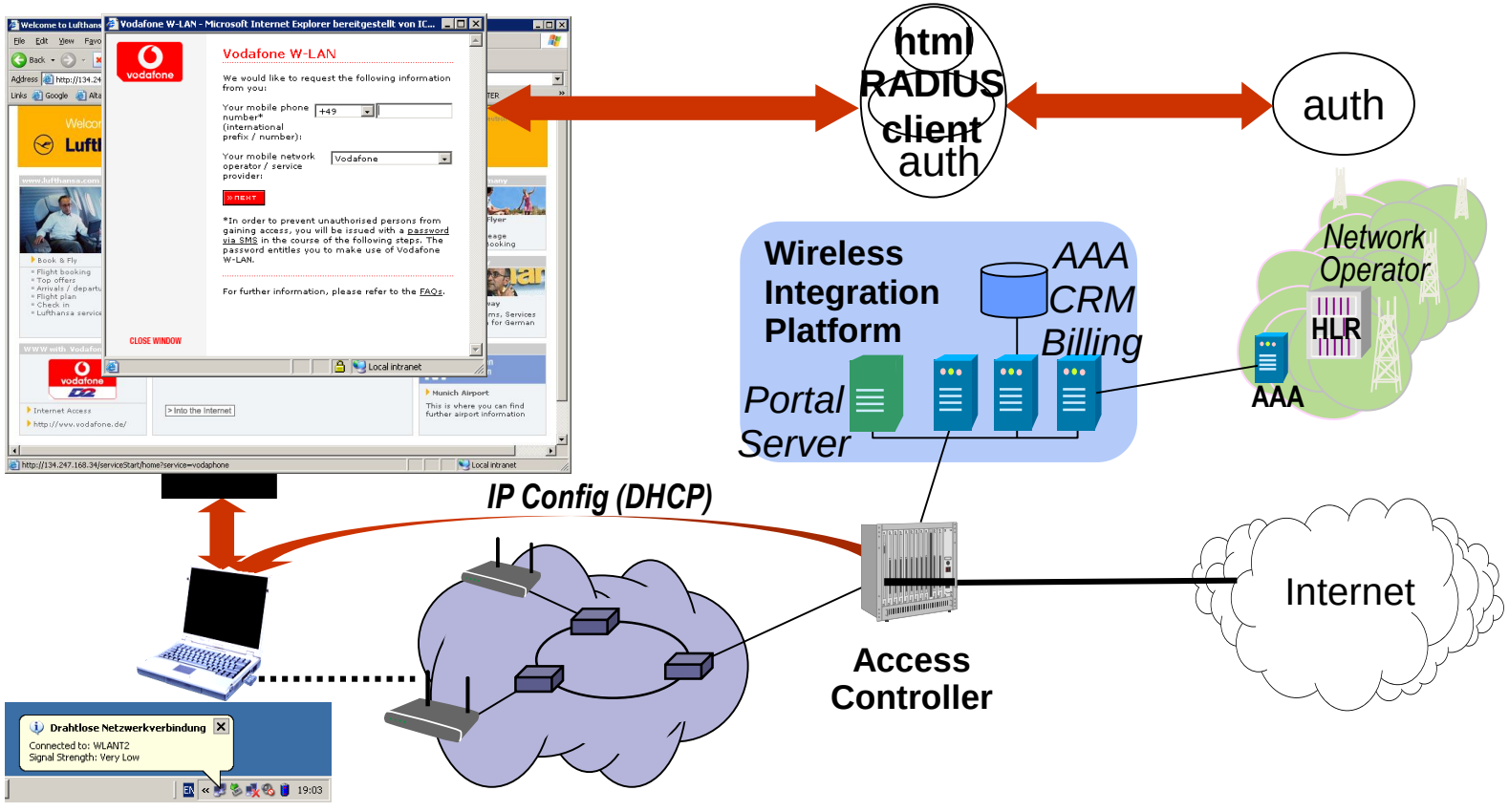
HaLow (IEEE 802.11ah) MAC Features

- Short frames to reduce active Tx/Rx time
  - 11ah Short Control frames: use an NDP (Non-Data-Packet) with MAC info in S1G field
  - Short MAC header
  - Short beacon frame (and compressed TIM) to reduce beacon decode times
  - Short probe request/response
- Support for larger number of associations
  - New TIM structure and encoding
  - Multiple TIM segments. First segment aligns with DTIM.
- Pseudo-scheduling and grouping sensor traffic
  - To support large number of devices in network and reduce contention time
  - Target wakeup times (TWT) for STAs agreed with AP
  - Periods of time where contention is restricted to group of STAs
  - Speed frame exchange, for quick UL/DL transaction
  - Improved PS-poll operation to allow sensors to sleep while AP fetches data
- Increase standby time
  - Operation without beacon; use of PS-Poll to check for data and/or re-synch
  - Expand listen and MAX BSS idle periods to allow STAs sleep for hours/days
- Coexistence and prioritization of sensor traffic
  - Ad hoc EDCA parameters to favor battery operated STAs
  - Reservation of periods of time for sensors

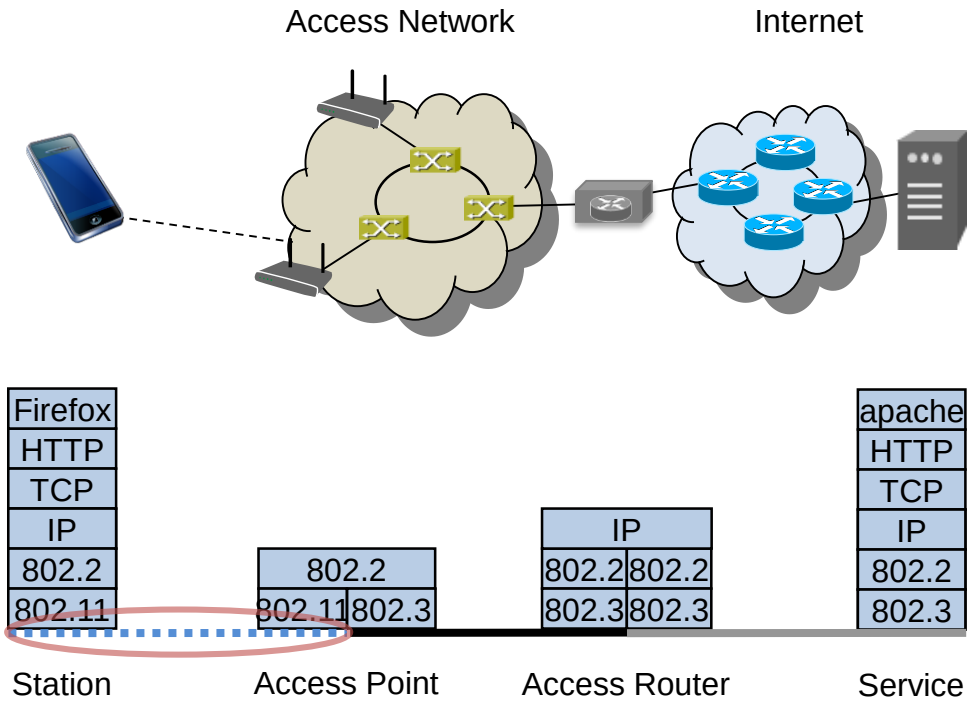
WLAN as a service for IOT

IEEE 802.11 SECURITY

Captive portals do not provide security



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

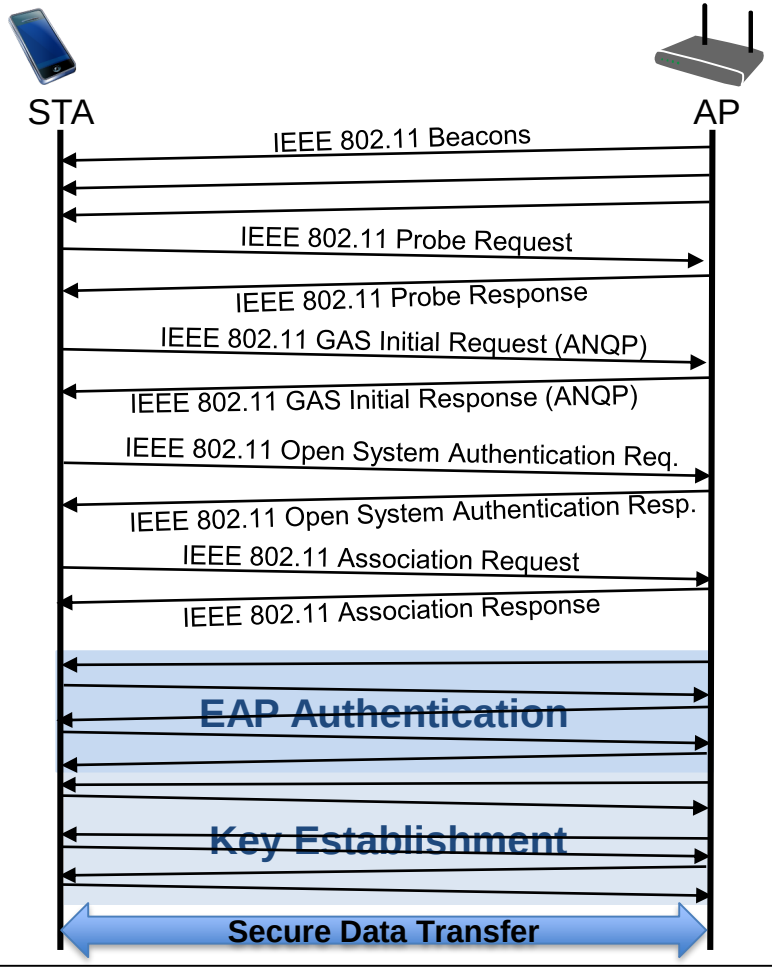
History of IEEE 802.11 Security

- 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 Security Establishment



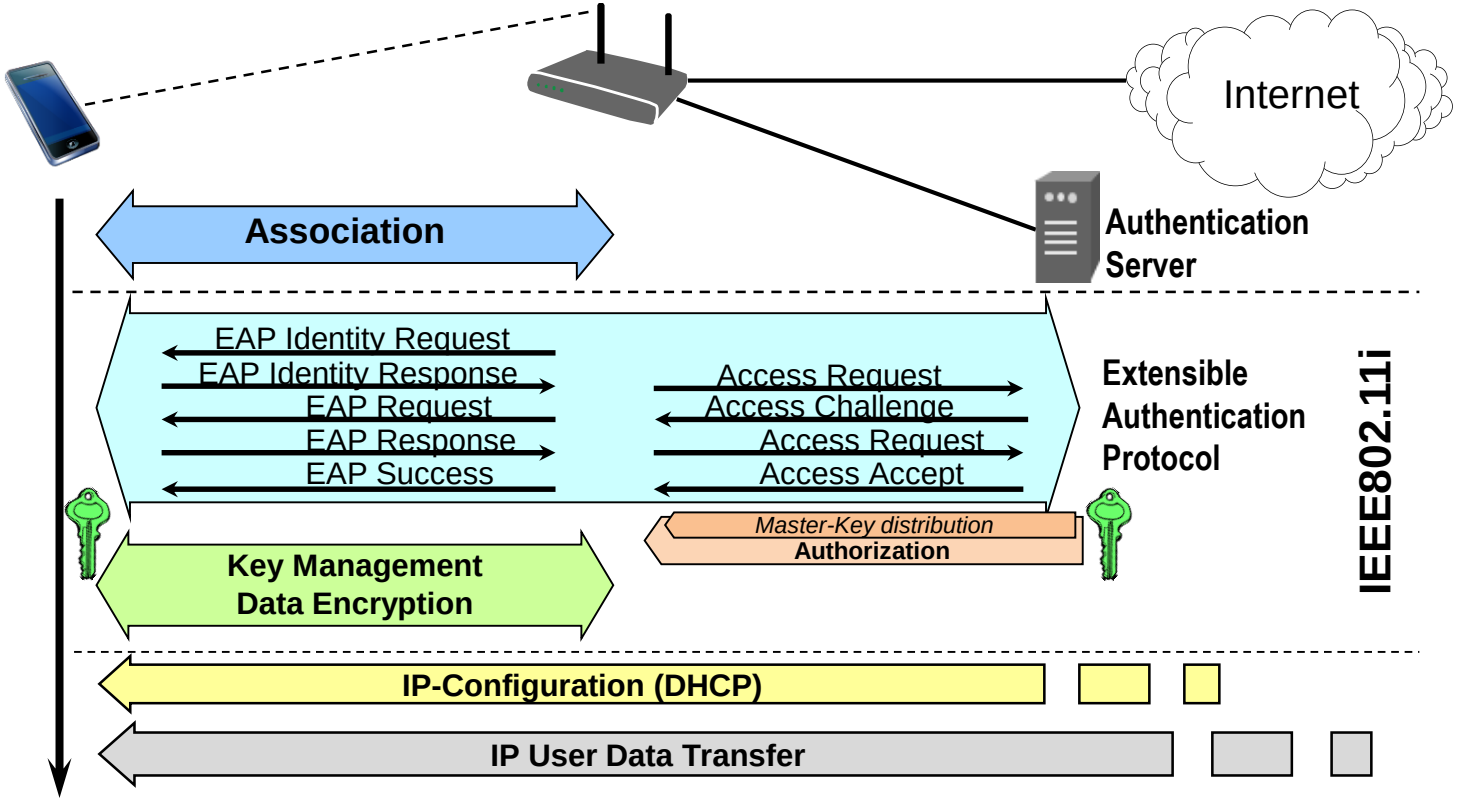
- Scanning
  - Beacon
  - Probe Request/Response
- Network Selection
  - GAS (ANQP Request/Response)
- Authentication
  - Open System Authentication
- Association
  - Association Request/Response
- Authentication/Authorization
  - IEEE 802.1X EAPoL follows association message exchange
    - Starts with 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

RSNA establishment

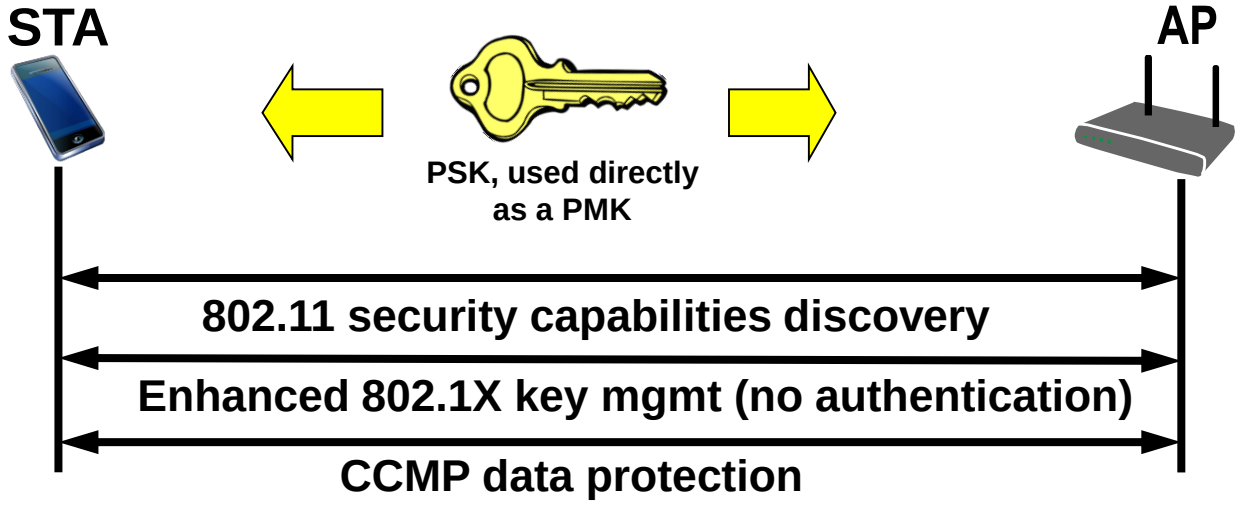
WPA2-Enterprise	WPA2-PSK
• RSN Capability identification from Beacon or Probe Response frames	
• Open System authentication.	
• Cipher suite negotiation during the association process	
• *Case of STA and AP supporting*	
802.1X Authentication	PSK
IEEE Std 802.1X-2004 Authentication Derive Pairwise Master Key	Use PSK as 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	

WPA2-Enterprise

Individual security for each station through EAP



WPA2-PSK for ‘simple’ use cases



- 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
- Reason to provide PSK-Mode:
  - Home users might configure passwords, but will never configure keys

WLAN as a service for IOT

SECURE WLAN OPERATION

The maintenance dilemma of IoT devices

- IoT devices are installed once, and might be kept forever
  - IoT devices are expected to operate 10+ years
    - Smartphones may be used for about 3 years, tablets and notebooks for 5 years
  - Btw, WLAN is keen on its long backward compatibility (20+ years)

- How to maintain secure operation over long periods
  - Most likely, security bugs in the firmware will be discovered
  - Maintenance will suffer due to rare availability of updates
    - In particular, when the devices are getting older

- If you can’t correct it, you might have to protect it!

Protecting sensitive things in a hostile environment

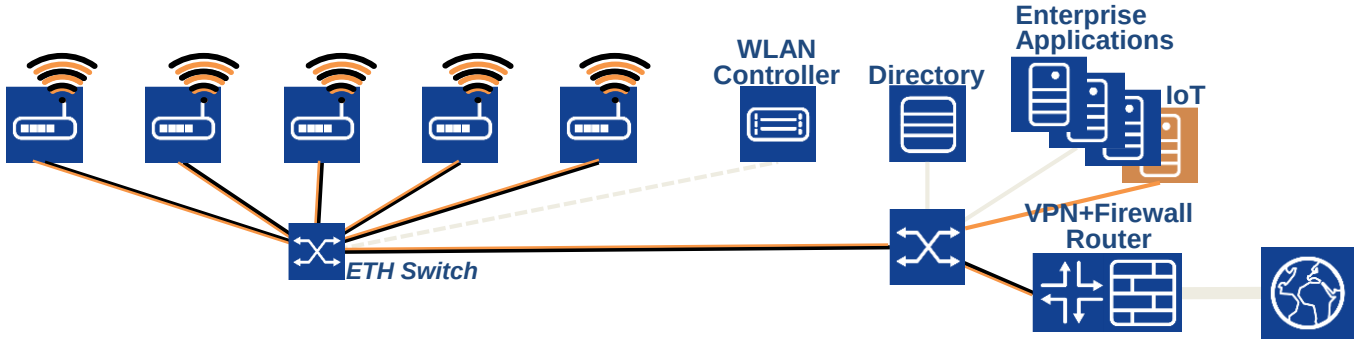
- Isolate, separate, build walls around, and gate access
  - Well proven principles of protection for centuries

By © MFSG / Wikimedia Commons, CC BY-SA 3.0

- Protection of IoT devices can follow the same principles.
  - Strictly control the communication of WLAN IoT devices.
  - Operating IoT devices in a dedicated WLAN access network might even allow for secure operation of vulnerable firmware.

Virtualized WLAN access networks

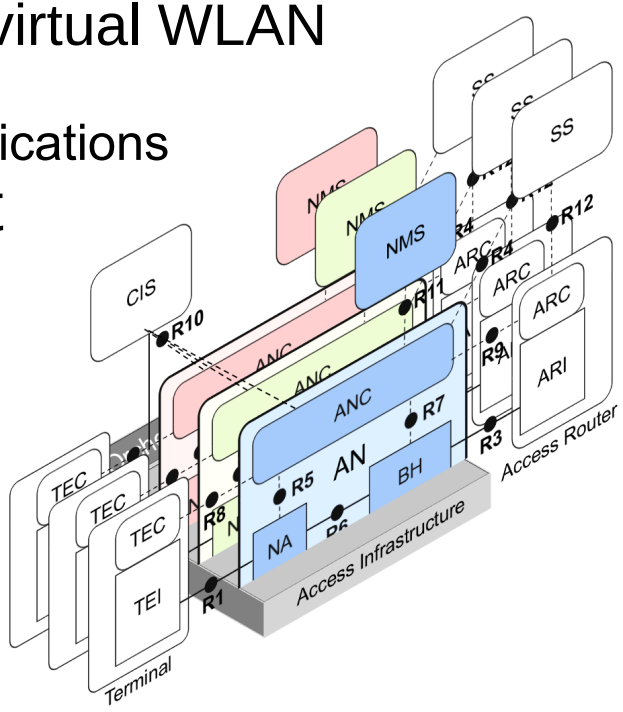
- Multiple WLAN accesses through ‘multi SSID’ configuration
  - WLAN has build-in virtualization capabilities.



- Network virtualization allows for multiple separate access infrastructures on a common infrastructure.
  - Network virtualization is promising technology to create ‘cloud economy’ also for network infrastructures.
- Virtualized WLAN creates remarkable business potential for operators and service providers.

WLAN virtualization – an evolving topic

- Enterprise WLAN solutions and Community WLAN are early examples of virtual WLAN access networks.
  - Not yet really virtualized, only secondary user planes
  - BBF TR-181 allows for configuration of virtual WLAN access in CPE devices.
    - Like ‘assembler programming’ for web applications
- IEEE 802.1 group works on abstract model of virtualized WLAN access infrastructure.
  - P802.1CF defines architecture and functional model of virtualized IEEE 802 access network.
    - Covering complete network lifecycle: Operation, Administration, Maintenance, and Provisioning



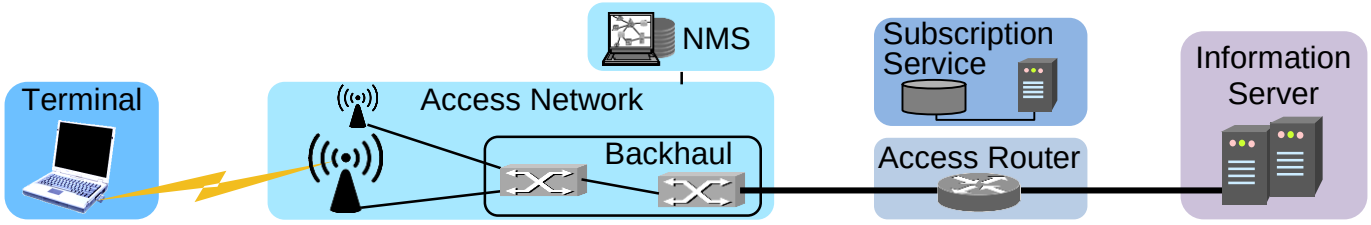
WLAN as a service for IOT

KEY CONCEPTS OF NETWORK VIRTUALIZATION

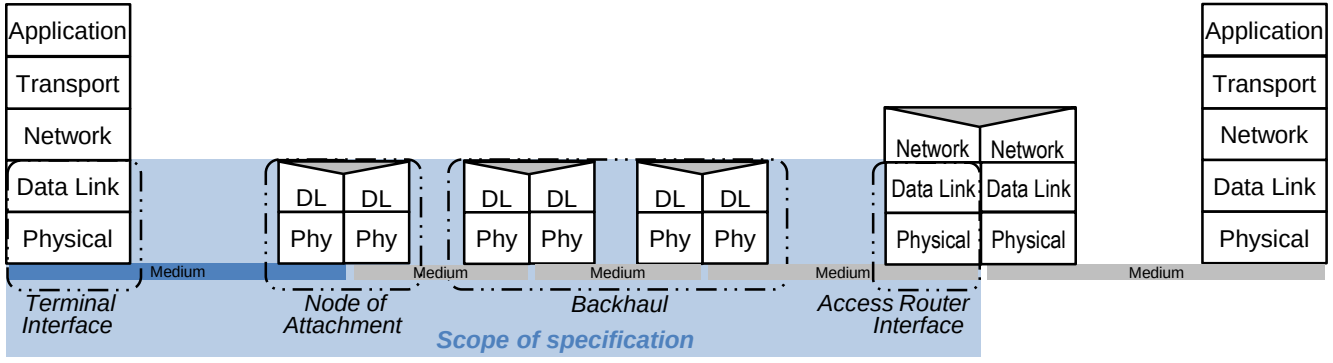
Network Reference Model

Network virtualization requires an Network Reference Model

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



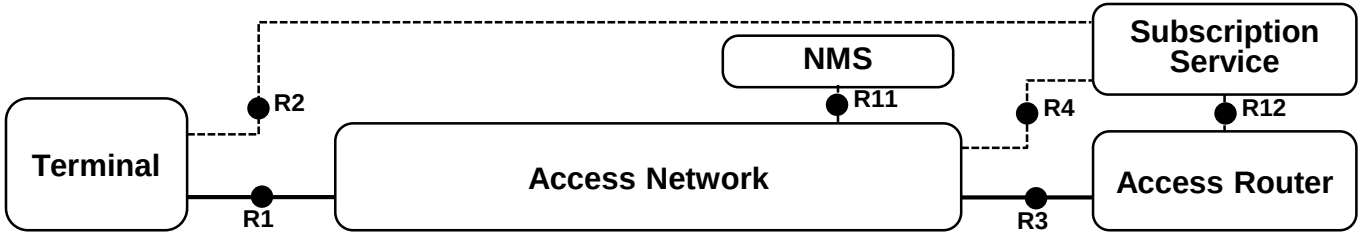
- The portion of the access infrastructure in scope of IEEE 802 was defined according to the protocol layer architecture of the data path



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

Network Reference Model basics

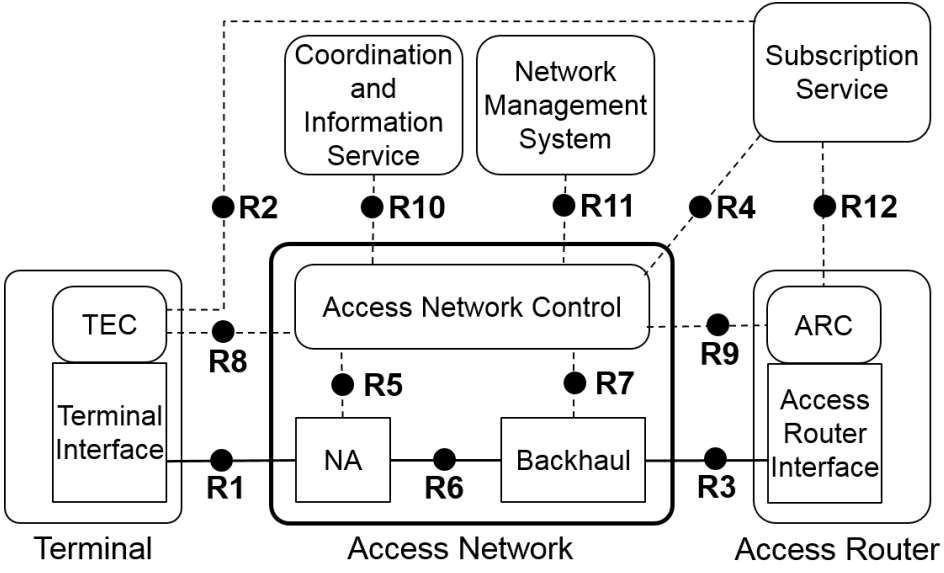
- The NRM denotes the functional entities and their relation to each others



- 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

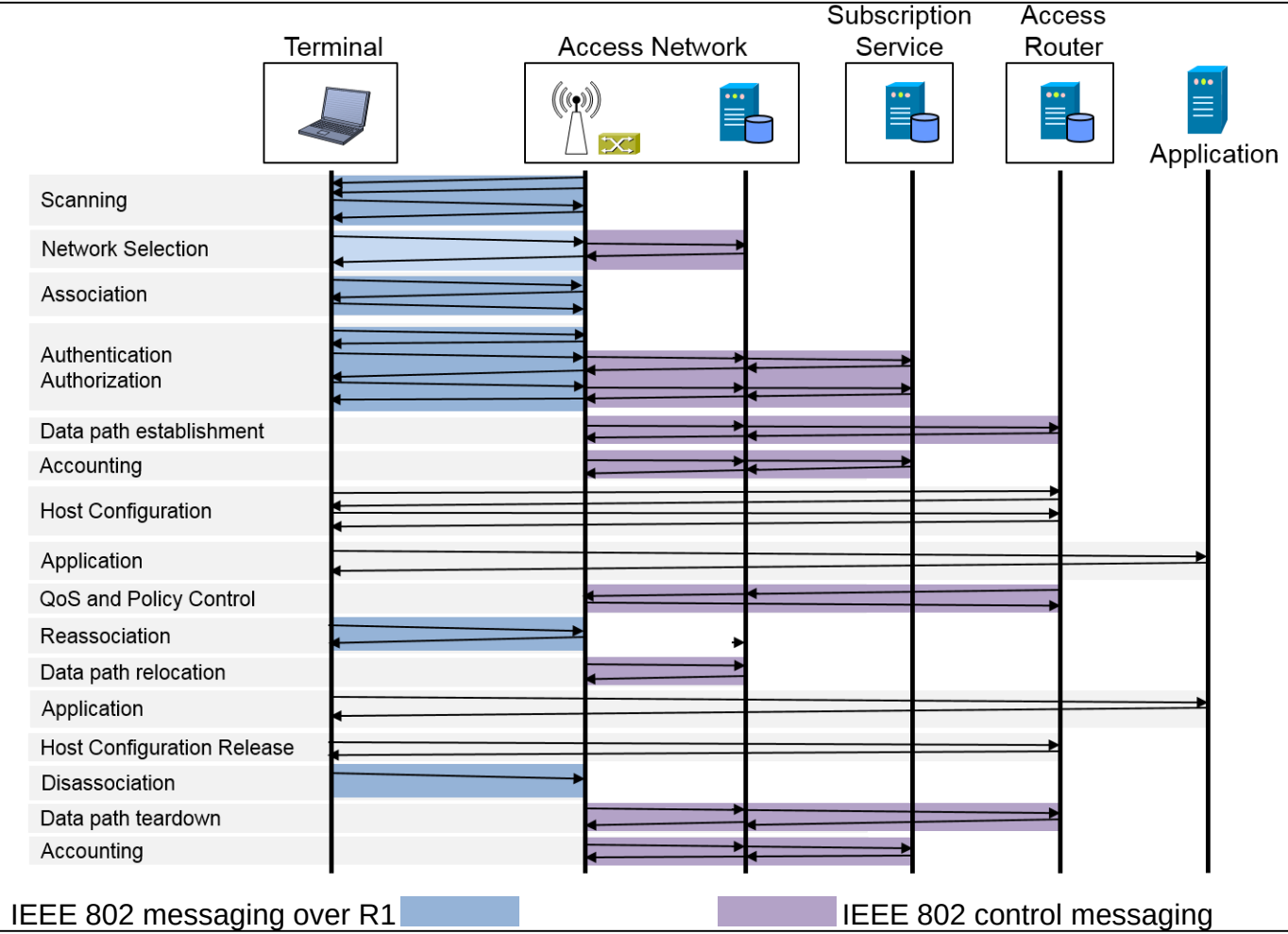
IEEE 802 Access Network Reference Model

- 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

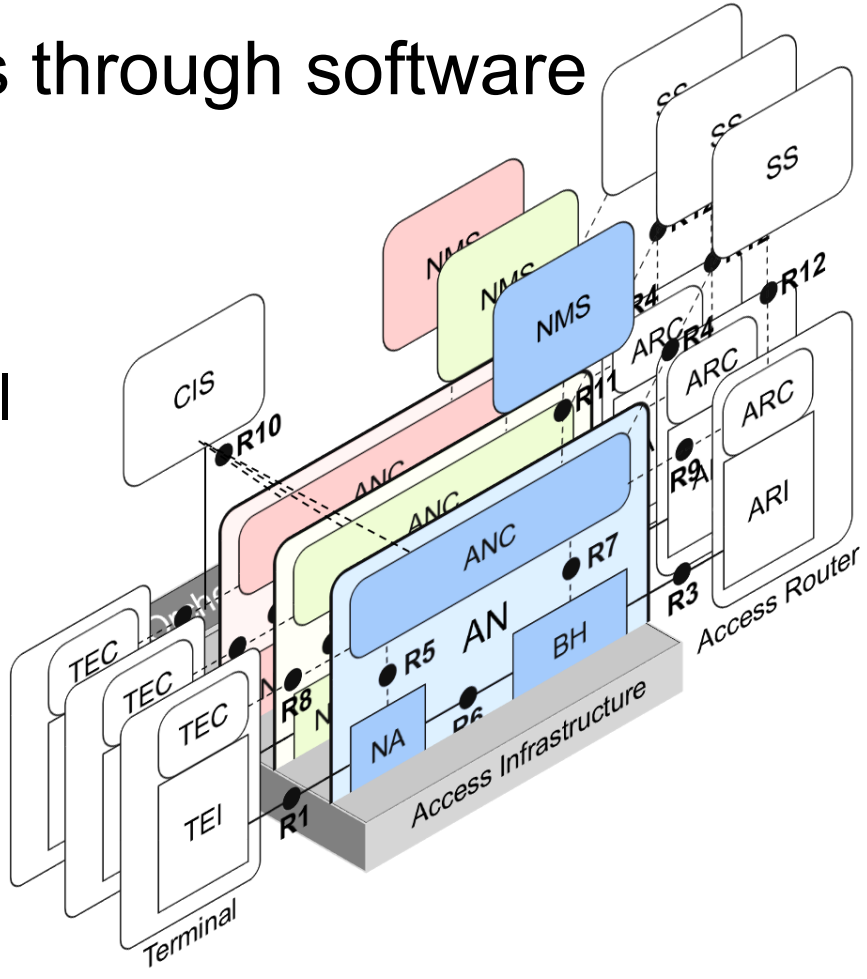
The life-cycle of an IEEE 802 session



Network softwarization

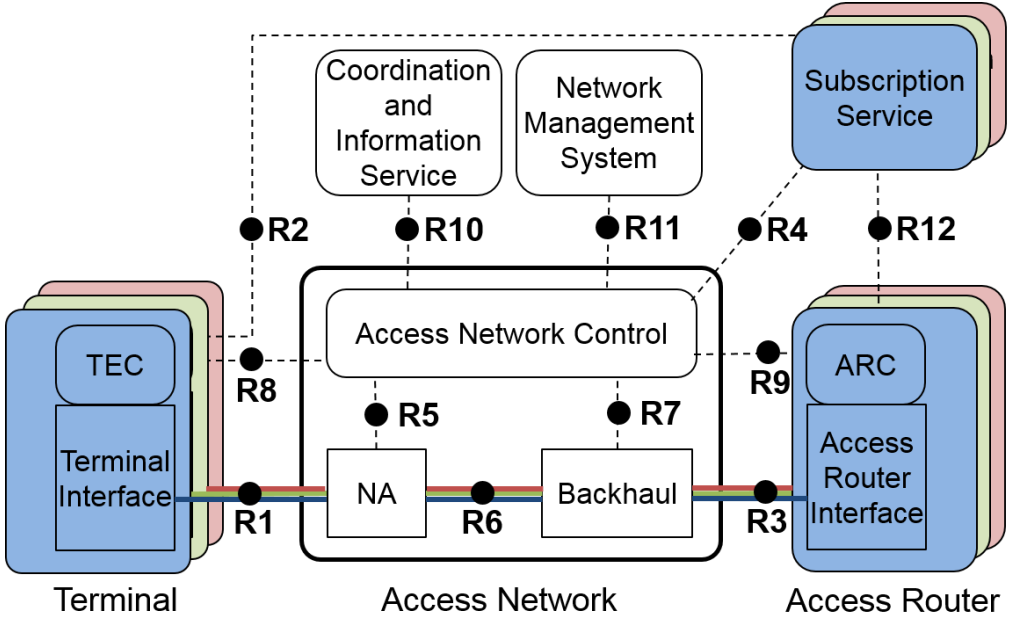
Building ‘complete’ networks through software

- P802.1CF provides model for network virtualization of IEEE 802 access networks
- Allows for realization of several separate networks on a common infrastructure
- Virtualization establishes separate control instances for each of the networks
  - Multiple operational domains



The lesser virtualization: Virtual Networks

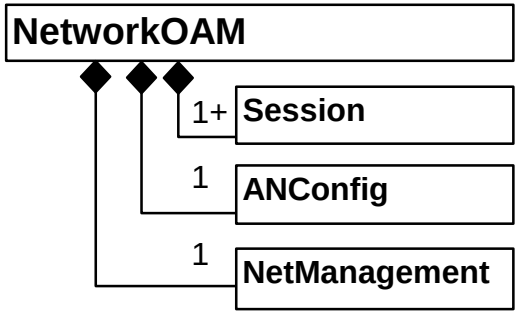
- VLANs provide separate datapaths under a common control
  - Single operational domain

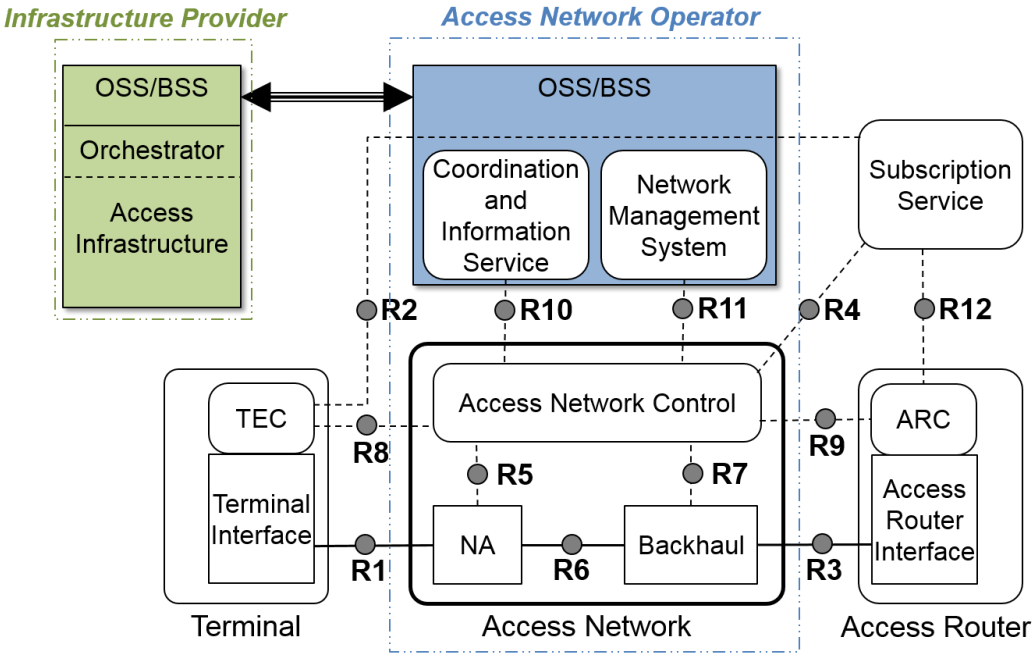


  - BTW: '5G network slicing' is more like virtual networks
    - Service differentiations through separate datapaths

Realization of virtualized access network

- Network softwarization requires an information model of access network
- Has to cover full network life-cycle
  - Operation
  - Administration
  - Maintenance
  - Provisioning



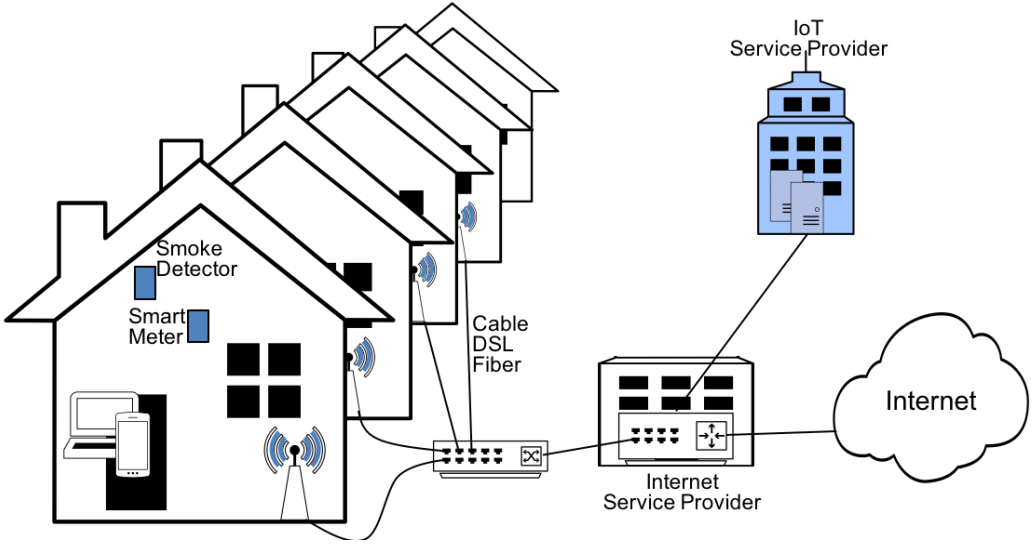


WLAN as a service for IOT

VIRTUALIZED WLAN ACCESS FOR IOT

Virtualized Wi-Fi access networks

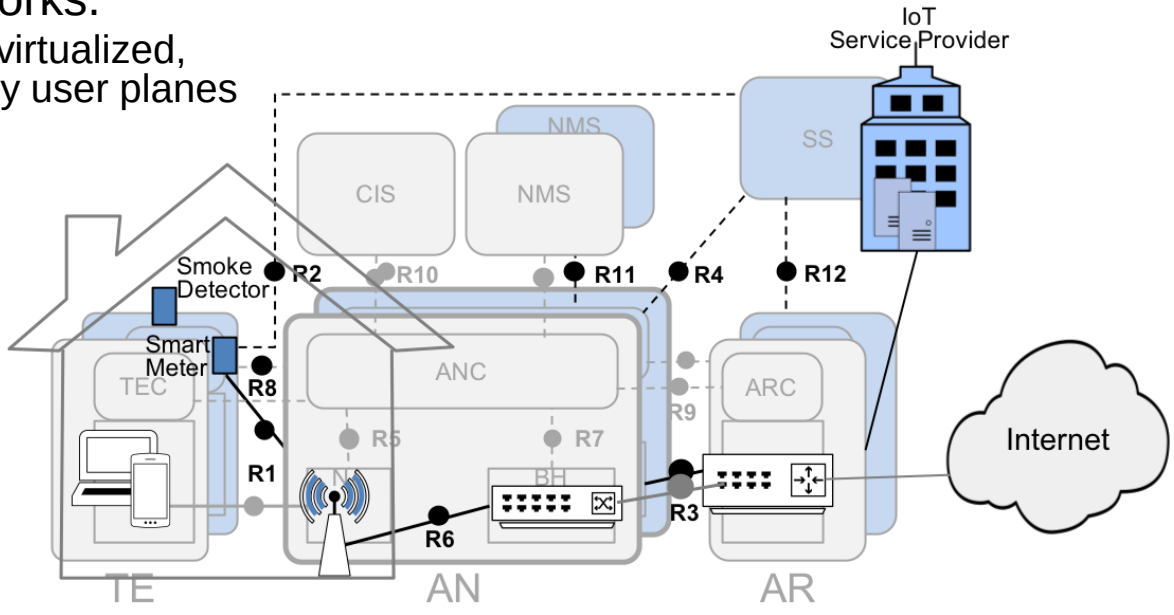
- Multiple Wi-Fi accesses through ‘multi SSID’ configuration
  - Wi-Fi has build-in virtualization capabilities.



- Network virtualization allows for multiple separate access infrastructures on a common infrastructure.
  - Network virtualization is promising technology to create ‘cloud economy’ also for network infrastructures.

Wi-Fi access network virtualization

- Enterprise Wi-Fi solutions and Community Wi-Fi are early examples of virtual Wi-Fi access networks.
  - Not yet really virtualized, only secondary user planes



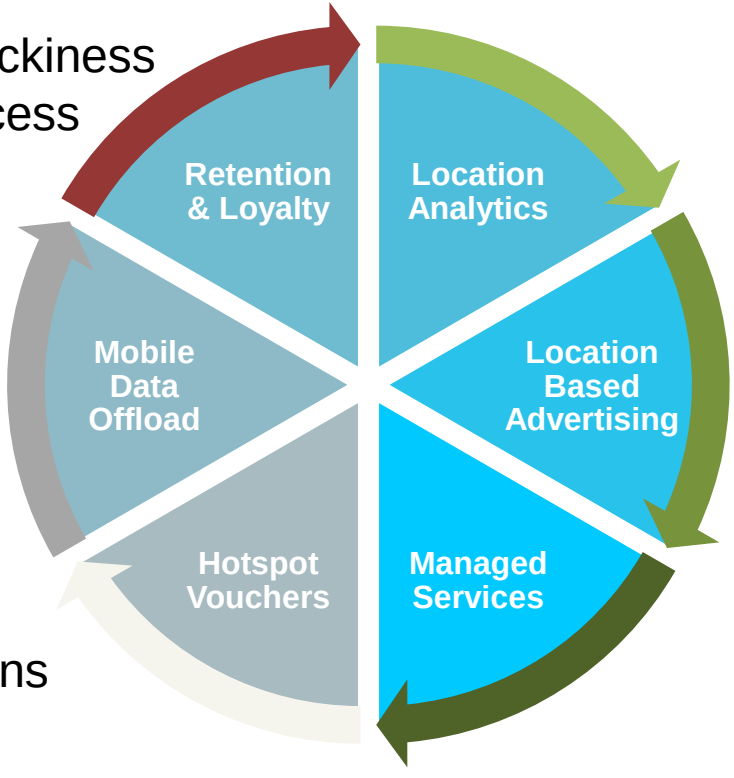
- Virtualization of Wi-Fi access requires model of desired network.
  - Covering complete network lifecycle: Operation, Administration, Maintenance, Provisioning
- P802.1CF provides architecture and functional model of virtualized IEEE 802 access network, which can be applied to Wi-Fi.

Operator WLAN use cases and value generation

Increase customer stickiness by offering mobile access through public Wi-Fi

Optimize mobile data network or deploy offload services

Create revenue by short term subscriptions to consumers



Create new revenues through location data analytics

Create new revenue streams via mobile advertising

Increase B2B revenues with managed wireless services

Conclusion and outlook

- WLAN will play a big role in IoT applications.
- Long-term system security of IoT devices is the real challenge.
- Virtualized WLAN access infrastructures can mitigate the issue.
- Broad demand for virtualized WLAN access creates business potentials for operators.
- Still a mile to go to develop and mature the technology
  - BBF TR181 and IEEE 802.1CF pave the path.

- IMHO, WLAN as a service for IoT is an emerging topic with very bright future.

Questions? Comments?

Thank you for your attendance!