Trends der drahtlosen Kommunikation
Kapitel 2: WLAN

Prof. Dr. Wolfgang Mühlbauer

wolfgang.muehlbauer@th-rosenheim.de

Fakultät für Informatik

Sommersemester 2019

Some slides are based on [1] and [3]

Motivation

- WLANs are everywhere
  - Home, cafes, airports, universities, …
- Challenges compared to Ethernet
  - wireless nature of communication
  - mobility of end users
- Standard: IEEE 802.11
  - WiFi = WLAN certified by WiFi alliance

"Wi-Fi"

Source: [2]

Outline

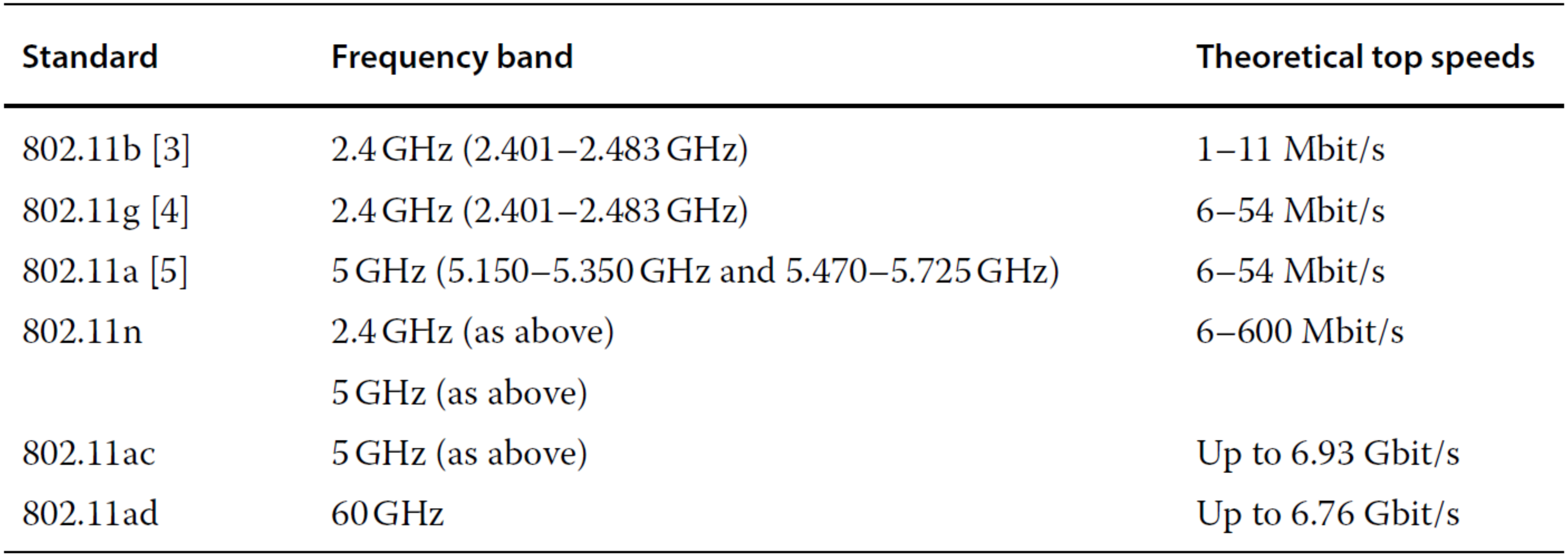
- **WLAN standards**
- WLAN architecture, frame format
- Multiple access control
- WLAN security
- WLAN mobility

Standards

- Each standard offers several bit rates
  - Choice depends on signal strength, etc.

- New WLAN adapters support multiple standards
  - Backward compatibility

- All use the unlicensed spectrum (ISM band)



Standard	Frequency band	Theoretical top speeds
802.11b [3]	2.4 GHz (2.401–2.483 GHz)	1–11 Mbit/s
802.11g [4]	2.4 GHz (2.401–2.483 GHz)	6–54 Mbit/s
802.11a [5]	5 GHz (5.150–5.350 GHz and 5.470–5.725 GHz)	6–54 Mbit/s
802.11n	2.4 GHz (as above) 5 GHz (as above)	6–600 Mbit/s
802.11ac	5 GHz (as above)	Up to 6.93 Gbit/s
802.11ad	60 GHz	Up to 6.76 Gbit/s

ax

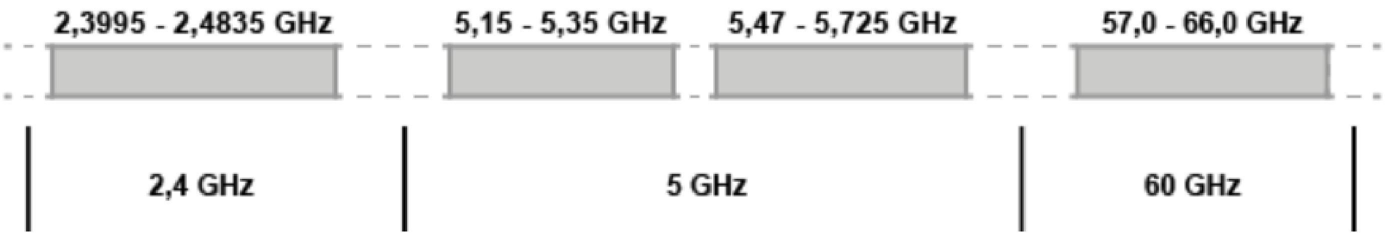
Source: [4]:

802.11 Physical Layers (1)

- **All 802.11 standards share**
  - Same link-layer format.
  - Use CSMA/CA for multiple access.
  - Have base station and ad-hoc network versions.

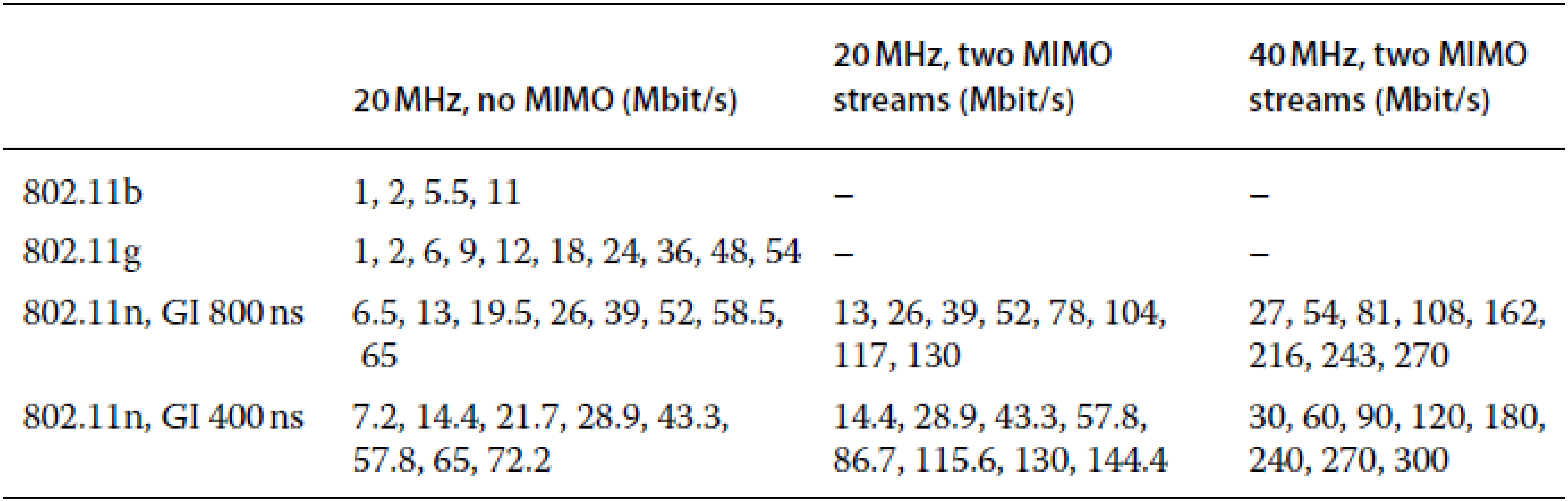
- **Example: 802.11b**
  - 2.4 GHz ISM band, 11 channels, 22 MHz per channel
  - Maximum transmission power 100 mW
  - Data rates from 1 to 11 Mbps
  - ***Modulation***: e.g.: Differential Binary/Quadrature Phase Shift Keying
    - Transmission of bit 1 changes phase of 180°C/ 90°C

WLAN-Frequenzen und -Kanäle



Source: [5]:

802.11 Feature Combinations



	20 MHz, no MIMO (Mbit/s)	20 MHz, two MIMO streams (Mbit/s)	40 MHz, two MIMO streams (Mbit/s)
802.11b	1, 2, 5.5, 11	–	–
802.11g	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	–	–
802.11n, GI 800 ns	6.5, 13, 19.5, 26, 39, 52, 58.5, 65	13, 26, 39, 52, 78, 104, 117, 130	27, 54, 81, 108, 162, 216, 243, 270
802.11n, GI 400 ns	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	14.4, 28.9, 43.3, 57.8, 86.7, 115.6, 130, 144.4	30, 60, 90, 120, 180, 240, 270, 300

Outline

- WLAN standards
- **WLAN architecture, frame format**
- Multiple access control
- WLAN security
- WLAN mobility

Wireless Modes

- A WLAN device can work in one of the following modes.
  - Station **(STA)** infrastructure mode
    - Regular WLAN client
  - Access Point **(AP)** infrastructure mode
    - Regular WLAN access point.
  - Ad-Hoc **(IBSS)** mode
    - „Peer-to-peer“ infrastructure
  - Monitor **(MON)** mode
    - For packet sniffing and packet injection.
  - Wireless Distribution System **(WDS)** mode
  - Mesh mode

- For some WLAN devices, it is possible to run in multiple modes at the same time.

Infrastructure Mode (STA and AP)

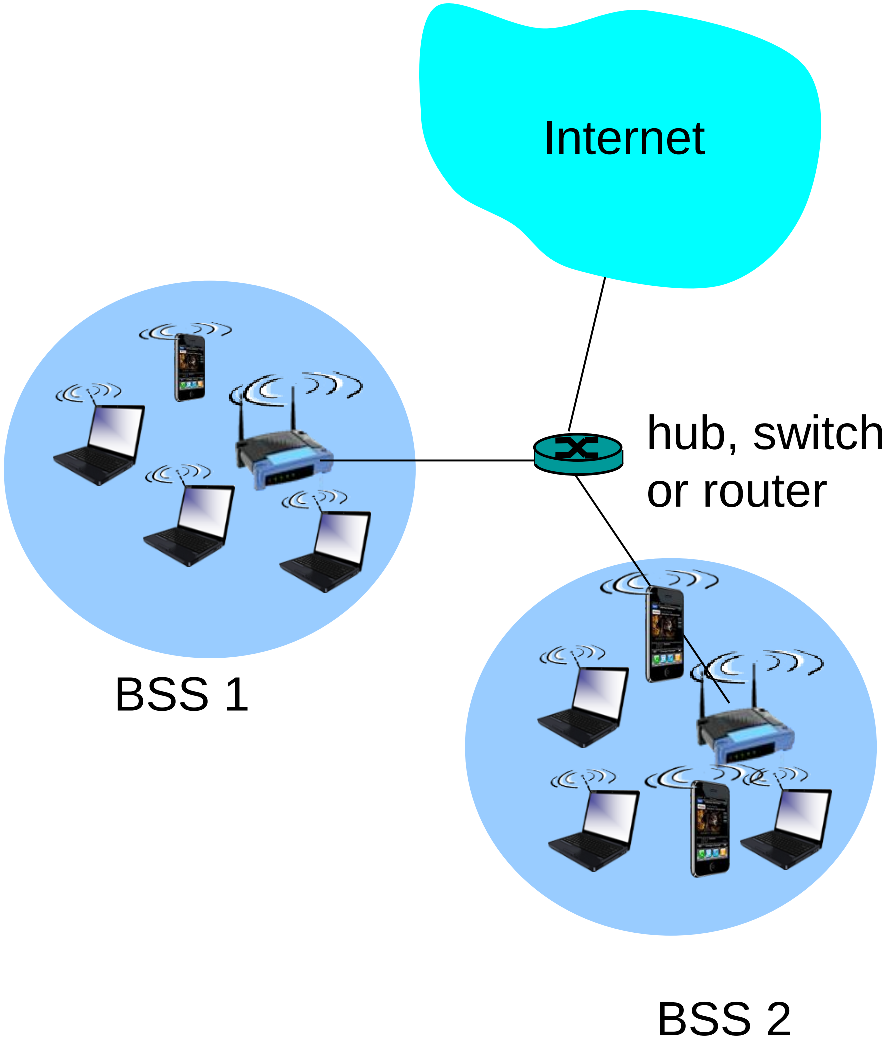
- **Access Point (AP)**
  - WiFi devices are clients and they only talk to each other via the AP.
  - Frame from A first goes to AP, then to B.
  - AP generally acts as relay to the Internet.

- ***Basic Service Set* (BSS)**
  - All devices that are associated with same AP form the BSS.
  - The MAC address of the AP is called the **BSSID** and identifies the WLAN network.
  - **SSID**: Human-readable name to identify the WLAN network, set by the AP.

- ***Advantages***
  - AP is central → coverage area of BSS increased.
  - AP generally offers DHCP, connection to Ethernet, DHCP, routing functionality

- Most common setup

infrastructure mode



Ad-Hoc Mode (IBSS)

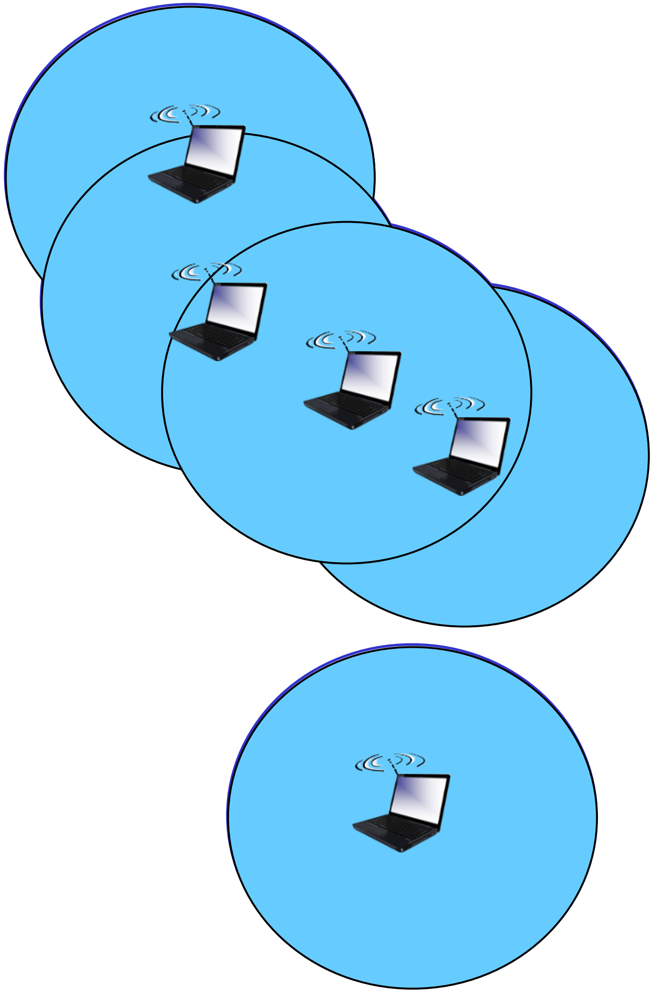
- ***"Peer-to-Peer"***
  - No access point.
  - Hosts communicate with each other directly.
  - Host discards received frames with wrong SSIDs.

- ***Independent Basic Service Set (IBSS)***
  - Hosts with same ***Service Set Identity (SSID)*** and same frequency form an IBSS.
  - Any hosts that can reach each other. The connectivity among hosts may change.

- Hosts need to manually configure an IP address

- Generally no access to the global Internet

- Not very popular except for very limited environments.



Ad-Hoc Network

Monitor Mode (MON)

- All packets in the air are passed to the host computer.

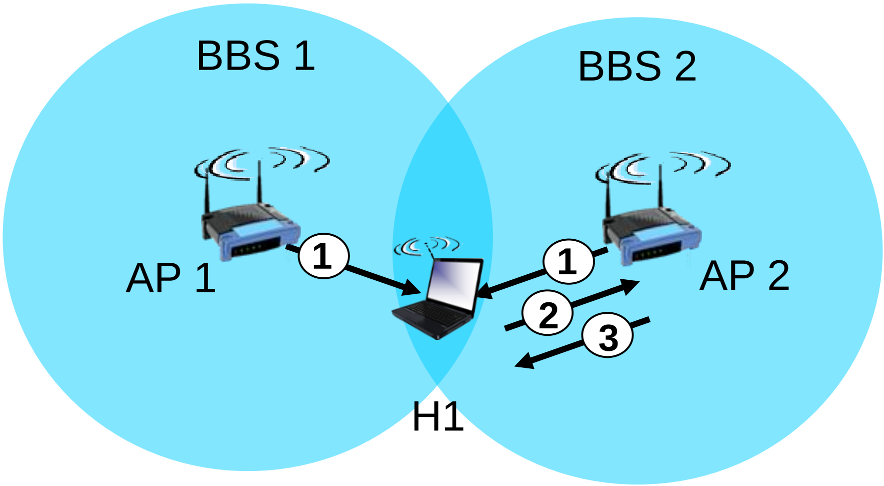
- Allows to capture packets ***without*** associating with an AP or ad-hoc network
  - More than *promiscuous mode*.
  - Promiscuous requires association. It only sees packets of the same WLAN.
  - Yet, also packets destined to another layer-2 network interface.

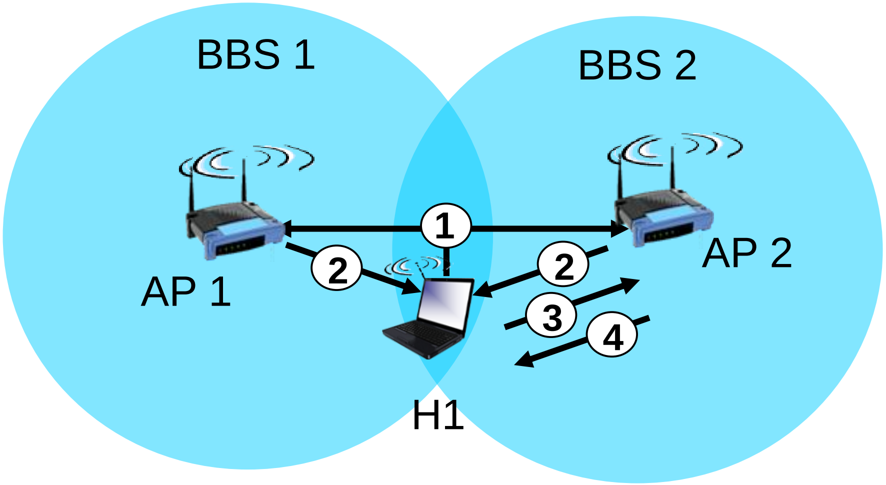
- A WLAN card can be in monitor mode in addition to a regular device mode
  - If HW supports it.

- ***Applications***
  - WLAN sniffing
  - Transmission of packets (packet injection)

- Badly support by off-the-shelf WLAN drivers.

Detection of Access Point





Passive scanning:

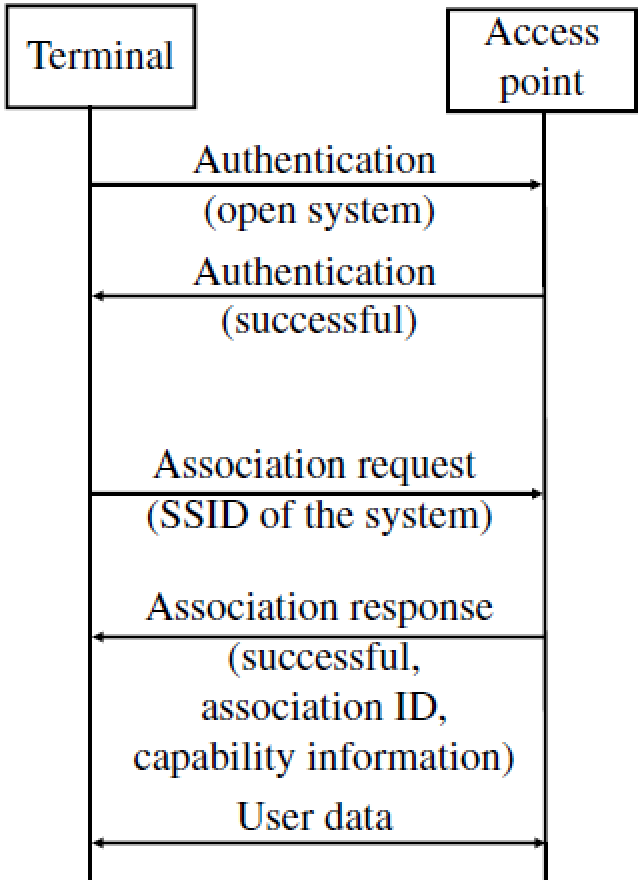
(1) Beacon frames sent from APs
(2) Association Request frame sent: H1 to selected AP
(3) Association Response frame sent from selected AP to H1

***Active scanning*:**

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

802.11: Authentication, Association

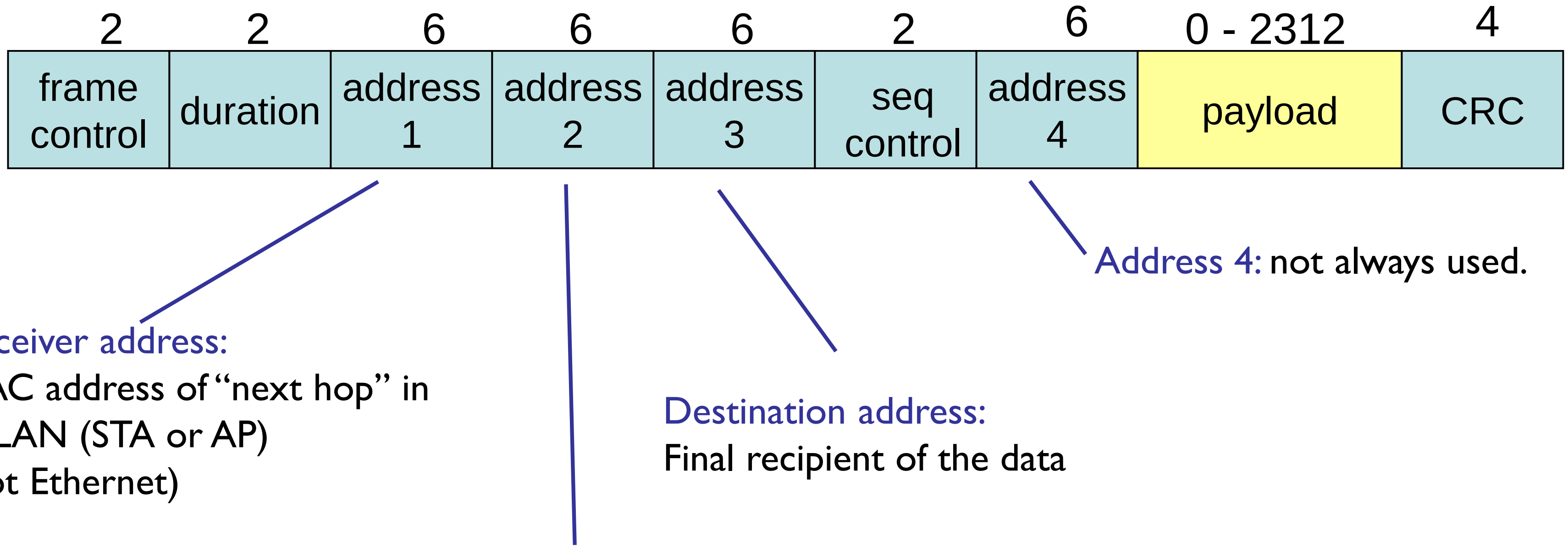
- ***Authentication***
  - Client needs to authenticate to AP
  - 2 options
    - Shared Key: WEP, not used any more
    - Open System: No authentication now!
  - WPA(2) etc. only comes later
- ***Association***
  - Final decision of client to connect with AP
  - Association request and response
  - Response includes
    - capabilities of WLAN AP (e.g., available data rates)
    - association ID (needed for power-saving mode)
- DHCP generally follows
- Only then: WPA and WPA2



Source: [5]

802.11 Frame Format

- ***Management frames***: association, authentication
- ***Control frames***: e.g., ACK, see "Multiple Access Control")
- ***Data frames:*** payload, have 3 addresses to pass via APs



2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Address 4: not always used.

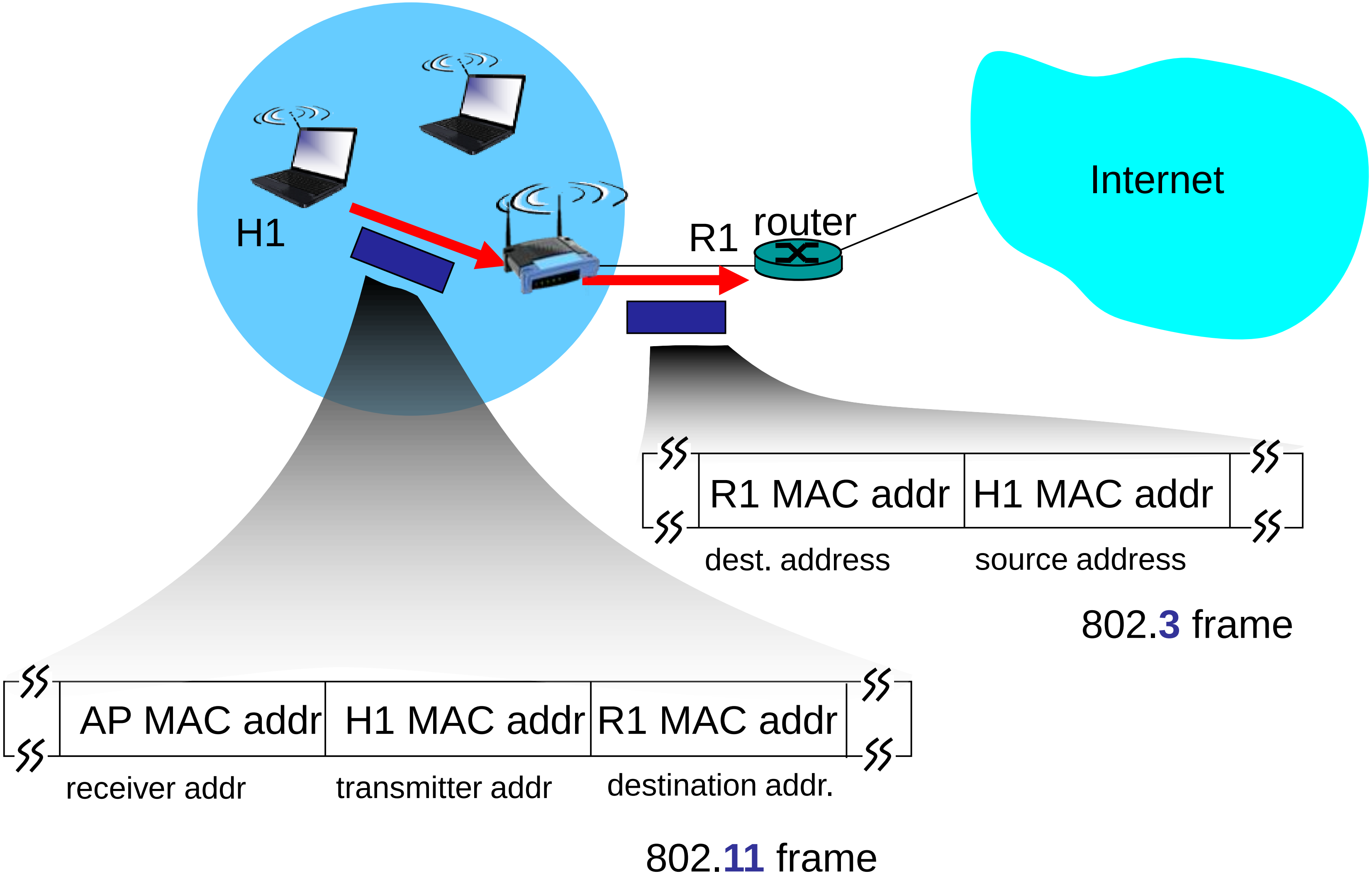
Receiver address:
MAC address of "next hop" in WLAN (STA or AP) (not Ethernet)

Destination address:
Final recipient of the data

Transmitter address:
MAC address "last WLAN hop" (STA or AP)

Number of used addresses and meanings depends on mode, see Übung 2

IEEE 802.11: Addressing



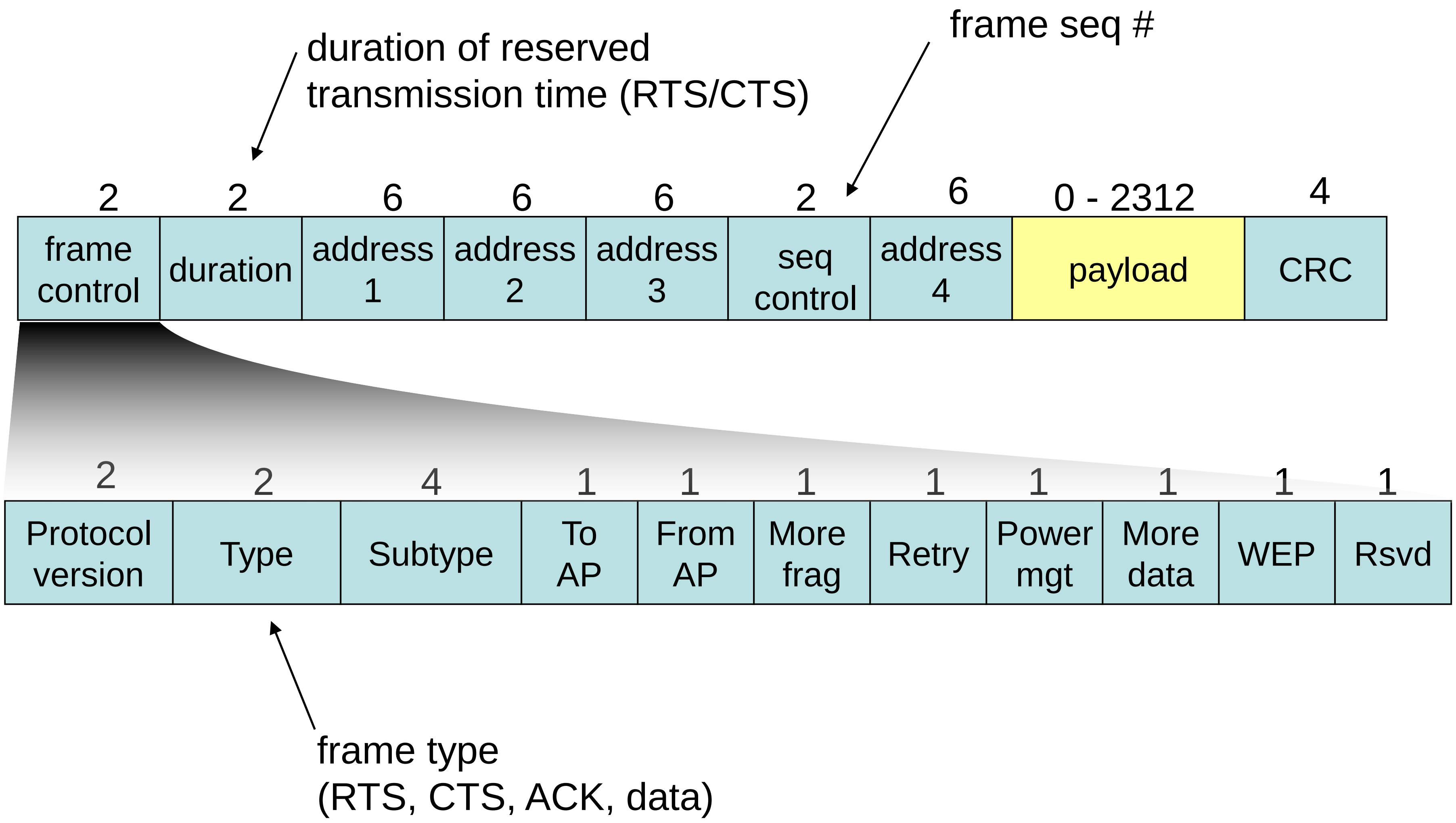
R1 MAC addr	H1 MAC addr
dest. address	source address

802.3 frame

AP MAC addr	H1 MAC addr	R1 MAC addr
receiver addr	transmitter addr	destination addr.

802.11 frame

802.11 Frame Format: Details



duration of reserved transmission time (RTS/CTS)

frame seq #

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

frame type
(RTS, CTS, ACK, data)

Linux: WLAN Commandline Tools

- **`wpa_supplicant`**
  - User for WLAN cards running in station mode (STA)
  - Performs authentication, association, security key management

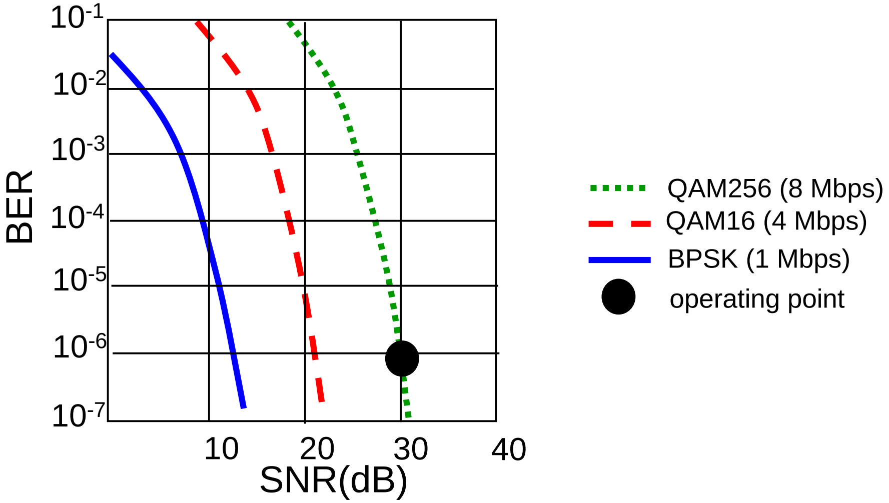
- **`hostapd`**
  - User application that implements the access point functionality
  - Can be used to run an AP on Linux.

- **`iw`**
  - Used to communicate with the WLAN kernel components.
  - Used to configure drivers, perform WLAN scan, read statistics, etc.
  - Previous tool: iwconfig

802.11: Rate Adaptation

- S/N ratio changes when wireless host moves
  - Host moves away from AP: S/N decreases, bit error rate (BER) increases

- AP and wireless host dynamically change transmission rate (i.e. modulation technique)
  - When acknowledgments are dropped, switch to lower transmission rate (more robust modulation)



802.11: Power management

- Wireless nodes can change between wake and sleep state
  - The latter saves energy!

- Node informs AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - AP buffers incoming frames for this node
  - Node wakes up before next beacon frame

- Beacon frame
  - Contains list of nodes with buffered frames waiting to be sent
  - Node will stay awake if AP has buffered frames for it; otherwise it will sleep again until next beacon frame

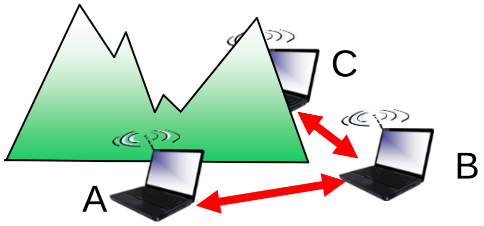
- Node can be asleep 99% of the time

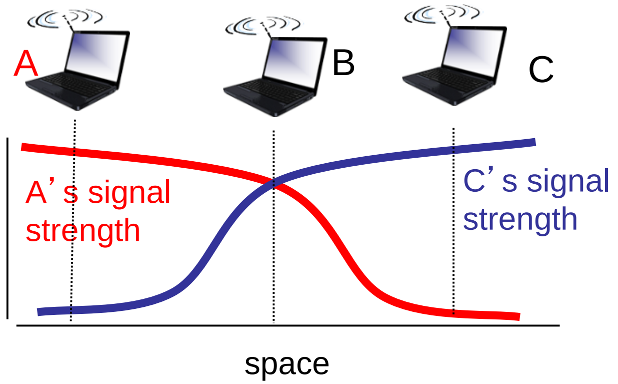
Outline

- WLAN standards
- WLAN architecture, frame format
- **Multiple access control**
- WLAN security
- WLAN mobility

IEEE 802.11: Multiple Access

- Avoid collisions: >2 nodes want to transmit simultaneously
- 802.11: CSMA → ***sense*** before transmitting
  - Don't collide with ongoing transmission by other node
- ***Differences*** to wired Ethernet 802.3
  - *No* collision detection but ***collision avoidance*** (CSMA/CA)
    - Half-duplex: Can't listen while transmitting
    - Can't sense all collisions in any case: hidden terminal, see later.
  - Link-layer acknowledgment / retransmission scheme





CSMA/CA: Algorithm

802.11 sender

1. if sense channel idle for **DIFS time** then

   transmit entire frame

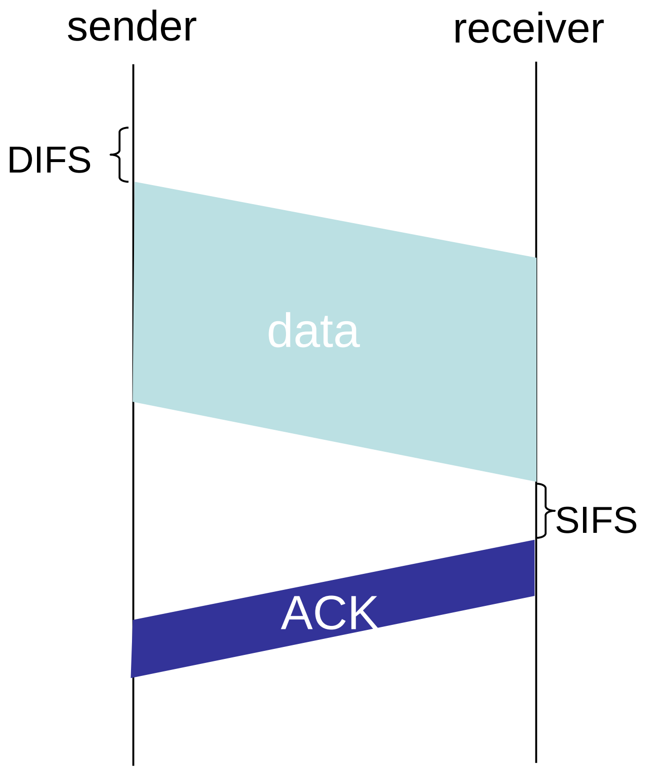
2. if sense channel busy then

   start random “backoff” timer

   timer counts down **while channel idle**

   transmit when timer expires

   if no ACK, increase random backoff interval, repeat 2



802.11 receiver

if frame received OK

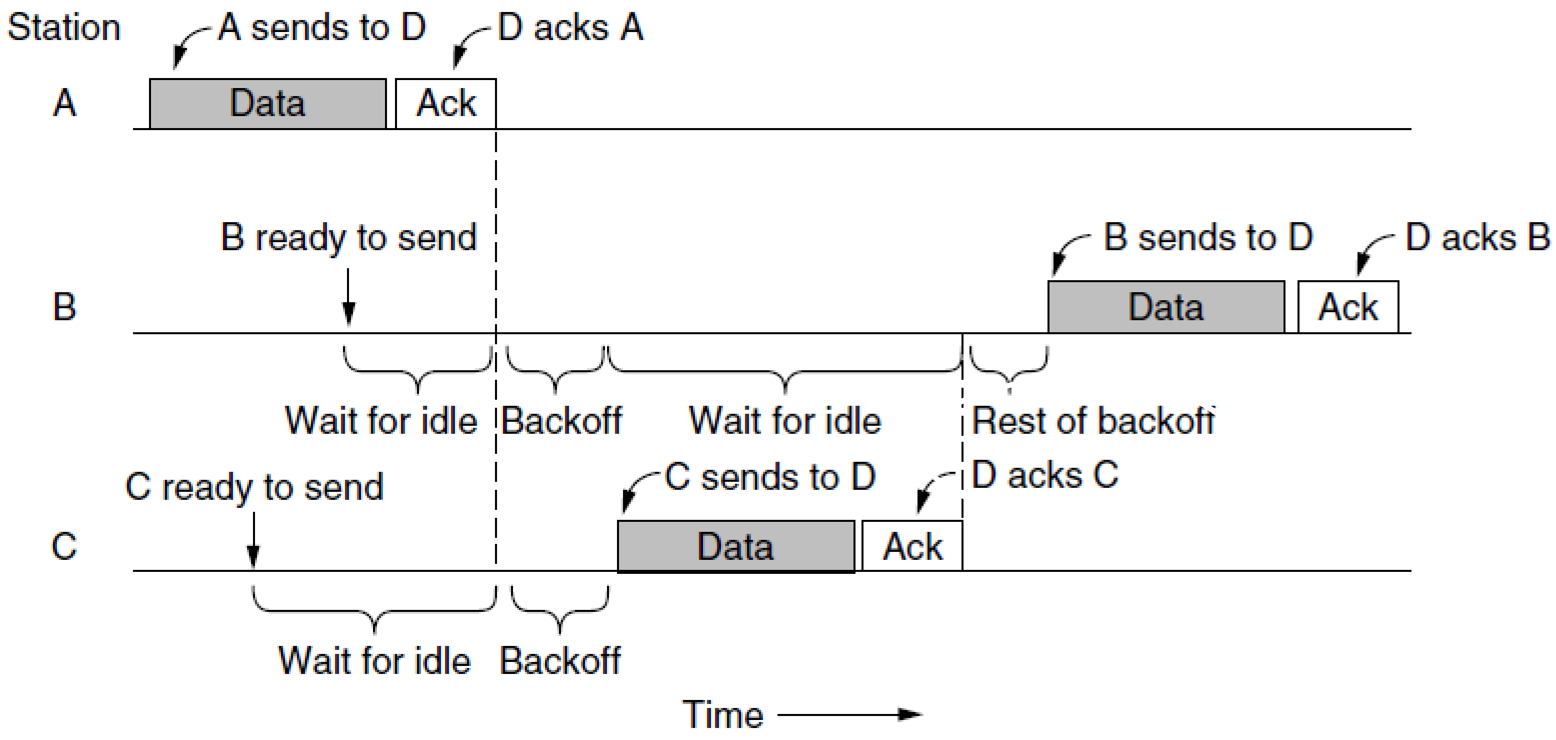
return ACK after **SIFS time**

(ACK needed due to hidden terminal problem)

SIFS time period shorter than DIFS. Why?

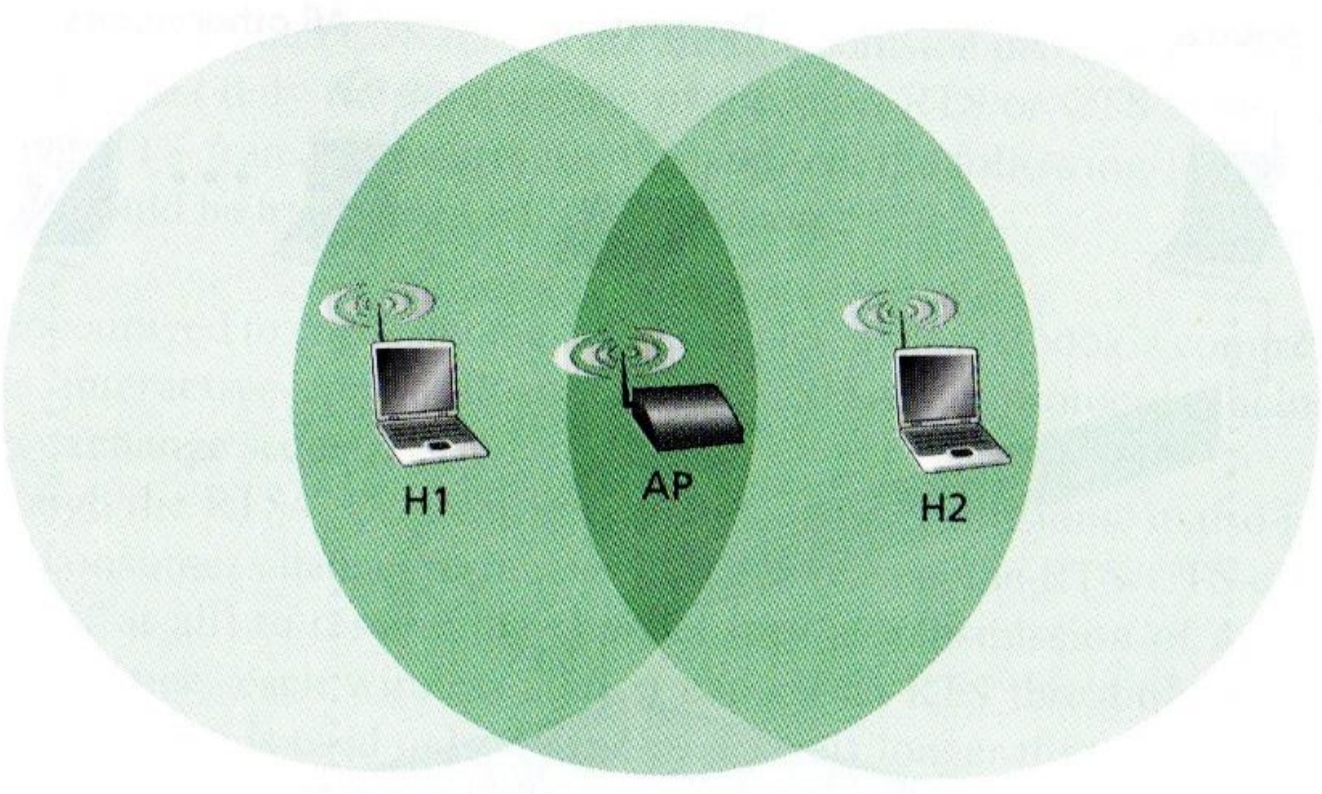
CSMA/CA: Example

- CSMA/CA inserts backoff slots to avoid collisions
- MAC uses ACKs/retransmissions for wireless errors
- Picture without DIFS and SIFS waiting times



Hidden Terminal Problem

- Does the proposed CSMA/CA algorithm work in this scenario?
    - H1 and H2 want to transmit simultaneously



aus Kurose&Ross

CSMA/CA + RTS/CTS

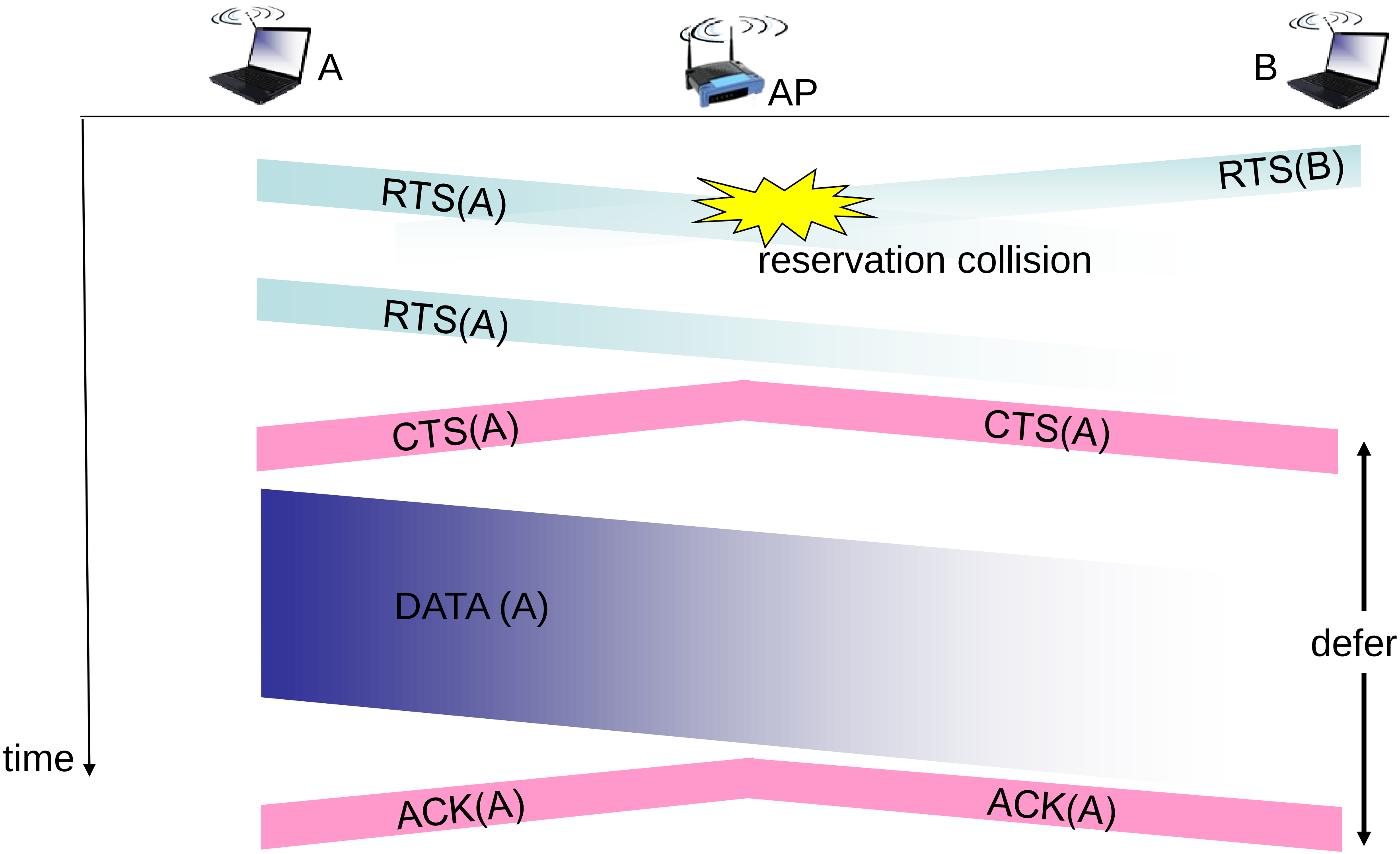
- Optional extension: only used for long data frames

- Sender first transmits *small* ***request-to-send (RTS)*** packets to AP using CSMA
  - Reserves channel for total time required to transmit data + ACK

- AP broadcasts ***clear-to-send (CTS)*** in response to RTS

- CTS heard by all nodes since all nodes are associated with AP
  - Sender transmits data frame
  - Other stations postpone their transmissions

Collision Avoidance: RTS-CTS Exchange



Outline

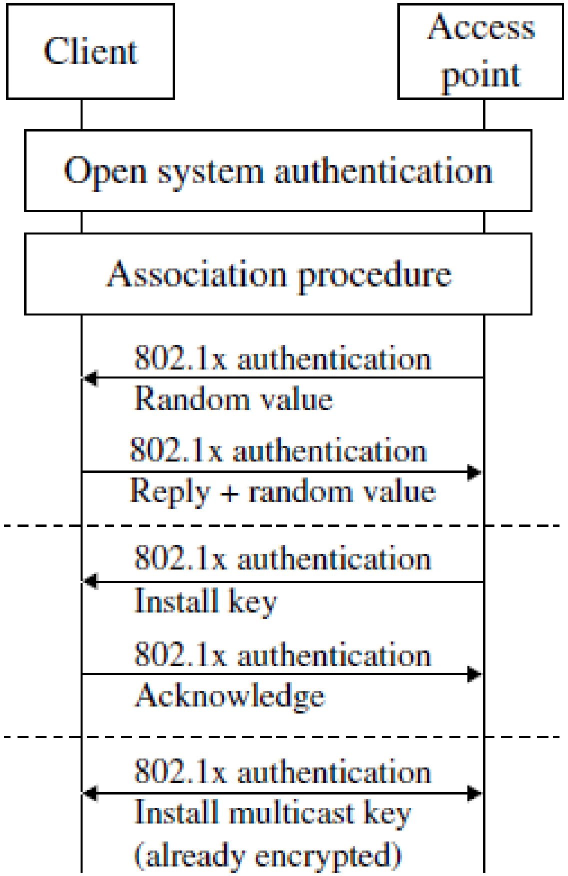
- WLAN standards
- WLAN architecture, frame format
- Multiple access control
- **WLAN security**
- WLAN mobility

WLAN Security

- Original standard WEP insecure.

- ***Encryption***
  - WPA: Temporal Key Integrity Protocol (TKIP)
    - Security issues!
  - WPA2: AES-based

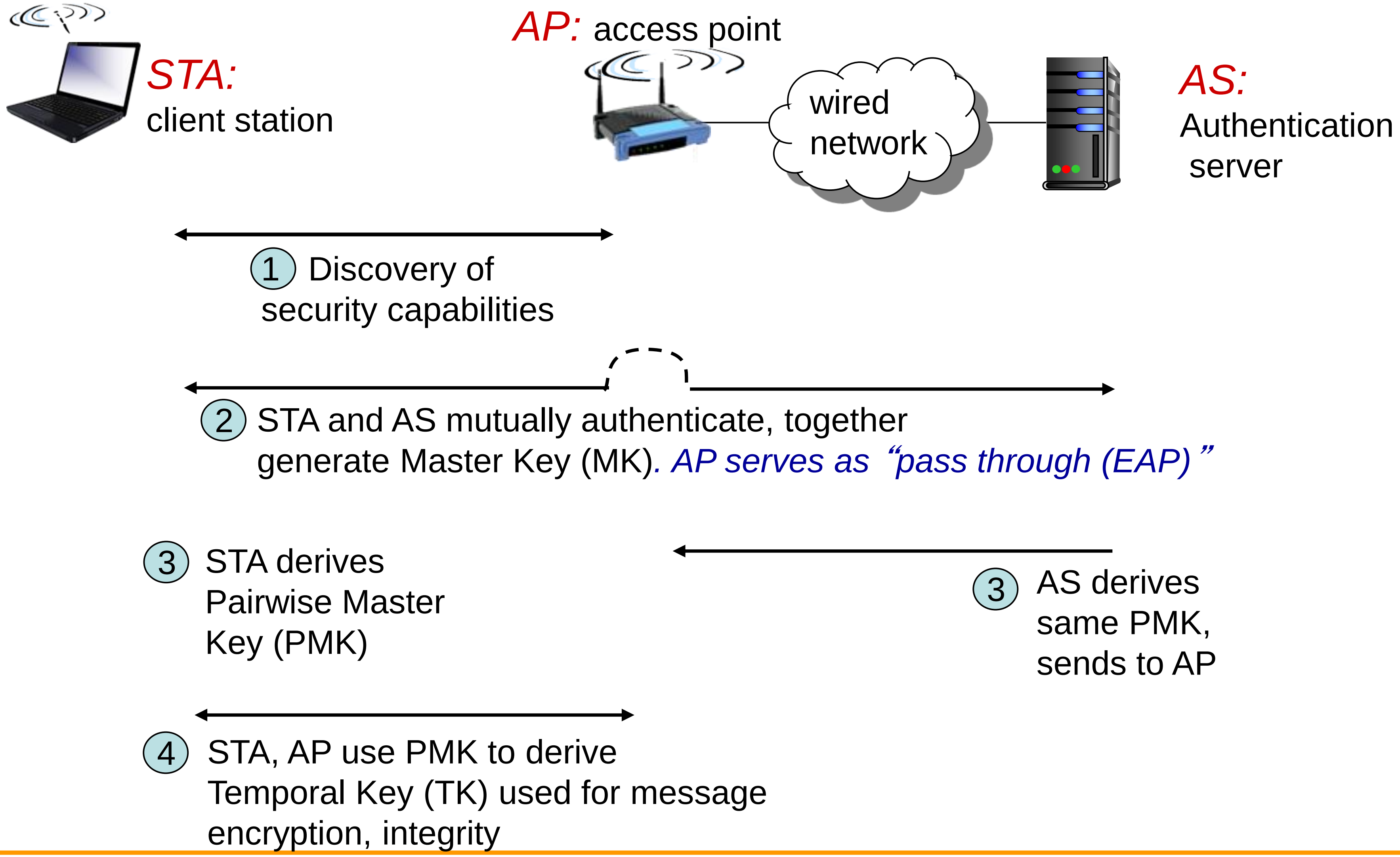
- ***2 modes***
  - WPA and WPA2 *Personal Mode*
    - *Pre-shared key* authentication: Same key stored in AP and client devices.
    - Client device and AP derive a common key session key for encryption.
  - WPA and WPA2 *Enterprise Mode* / 802.11i
    - Different key for each device.
    - See next slide.



WPA-PSK authentication and ciphering key exchange

WPA (2) Enterprise Mode / 802.11 i

Authentication Server ≠ Access Point



STA: client station

AP: access point

wired network

AS: Authentication server

1 Discovery of security capabilities

2 STA and AS mutually authenticate, together generate Master Key (MK). *AP serves as "pass through (EAP)"*

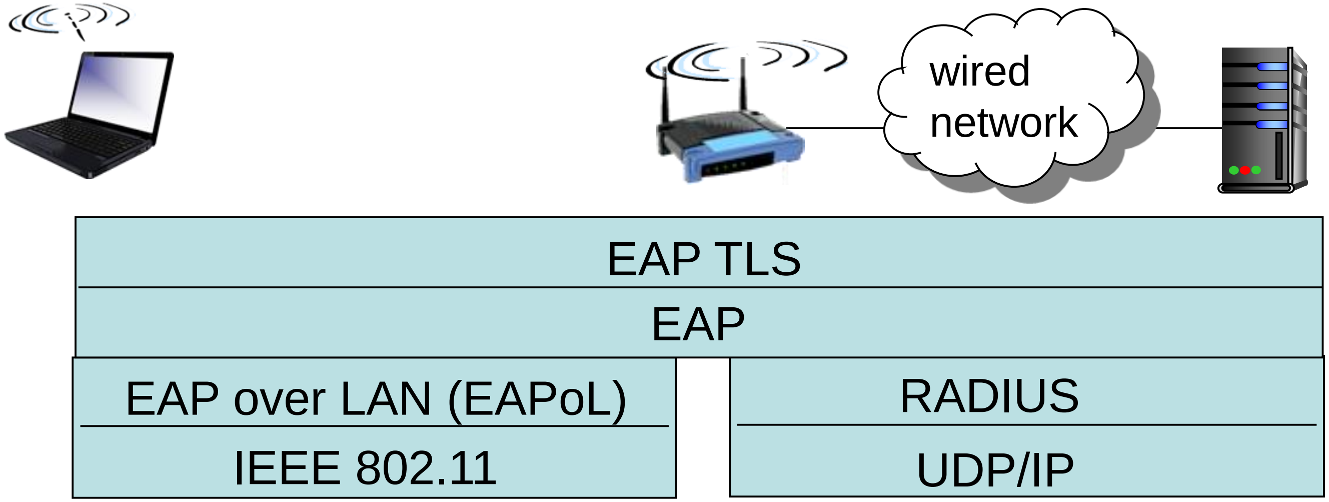
3 STA derives Pairwise Master Key (PMK)

3 AS derives same PMK, sends to AP

4 STA, AP use PMK to derive Temporal Key (TK) used for message encryption, integrity

EAP: Extensible Authentication Protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate "links"
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)



EAP TLS

EAP

EAP over LAN (EAPoL) | RADIUS

IEEE 802.11 | UDP/IP

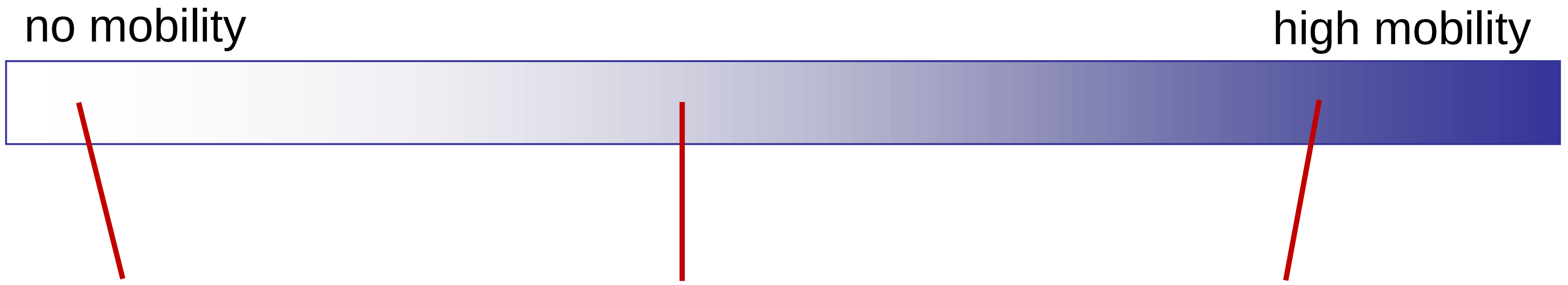
Outline

- WLAN standards
- WLAN architecture, frame format
- Multiple access control
- WLAN security
- **WLAN mobility**

Mobility

- Two types of mobility:
  - Mobile node remains in the **same IP subnet** but changes AP
  - Mobile node changes to a **different IP subnet** (change of IP address?)

- Spectrum of mobility, from the ***network*** perspective:



mobile wireless user, using same AP, walking around

mobile user, connecting/ disconnecting from network using DHCP.

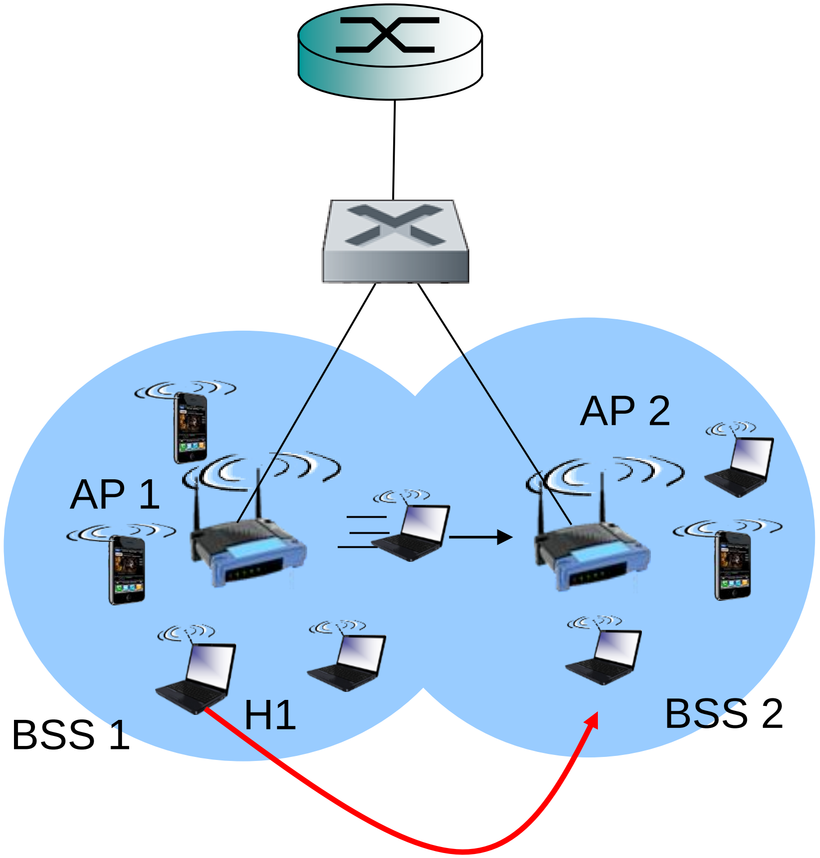
mobile user, passing through multiple access points while maintaining ongoing connections (like cell phone)

Mobility: AP are connected via Ethernet

- BSS1 and BSS2 have the same SSID and share an IP subnet

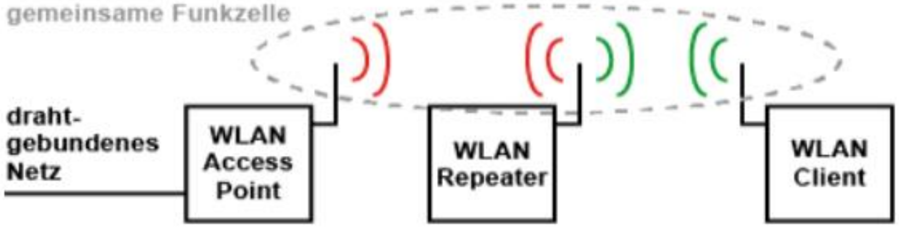
- H1 remains in same IP subnet
  - H1 can keep its IP address.
  - H1 can keep its ongoing TCP sessions.

- H1 moves from BSS1 to BSS2
  - Signal to AP1 gets weaker.
  - H1 associates with AP2.
  - It may ***take some time*** until switch learns that H1 is now reachable via a different port.

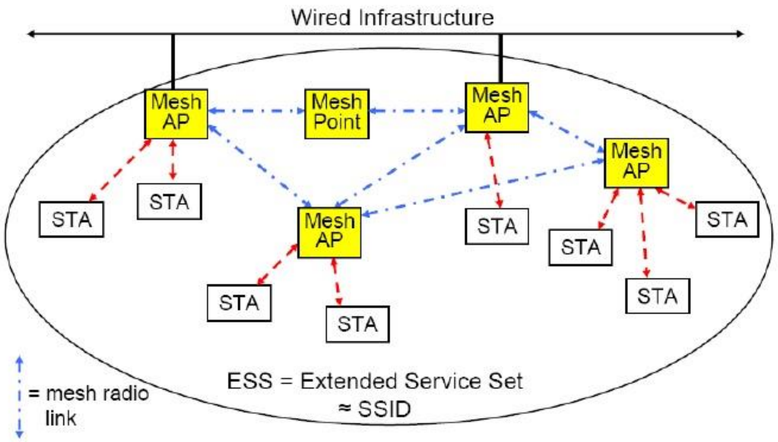


Outlook: WDS and Mesh

- Normally, APs are connected to each other through the wired network to form a Distributed System (***DS***). Yet, this can also happen using the ***wireless link***.
- General assumption: All AP have the same SSID.
- Wireless Mesh is layer-3 while WDS is layer-2
- General issue: Frequently works only for WLAN routers from different vendors.



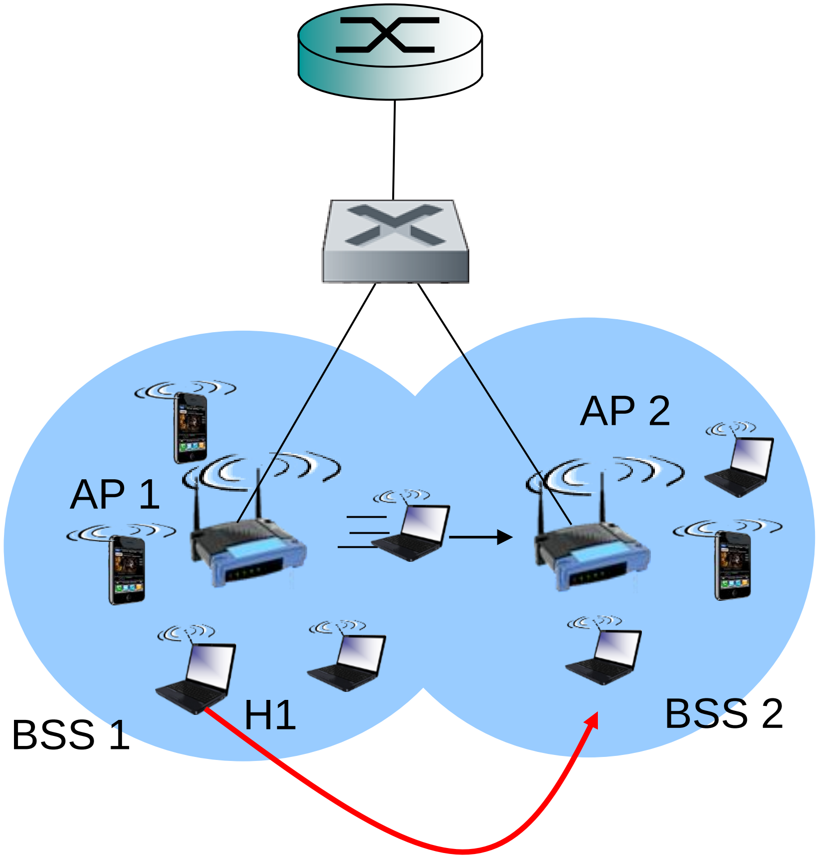
WLAN with mesh



Seamless Mobility

- ***Problem***
  - Switch only updates its forwarding table after H1 sends a packet via the switch / router to the Internet.
  - This can take a while!

- ***Solutions***
  - After H1 associates with AP: AP sends a broadcast Ethernet frame with H1's source address. (ugly)
  - General idea
    - Old AP buffers packets
    - New AP informs old AP point
    - Optional in 802.11 standard
    - Generally, no support across APs of different vendors!

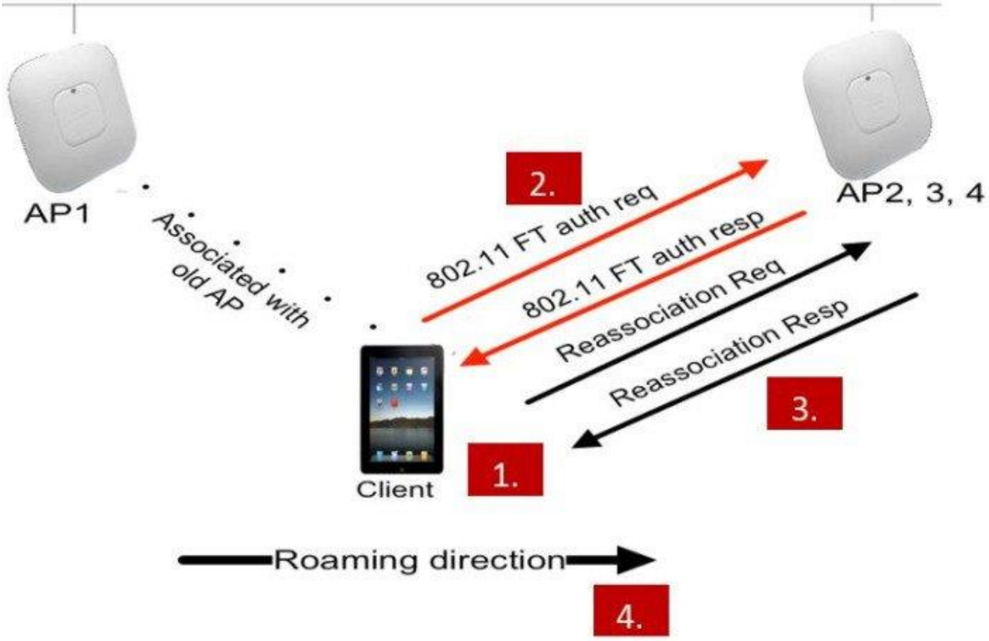


Standards for WLAN Roaming

- ***802.11r: Fast Transition Roaming***
  - Handshake with new AP occurs while client still associated with old AP.
  - Pairwise Master Key (PMK) calculated on advance.

- ***802.11k: Assisted Roaming***
  - Client can ask for „neighbor reports“.
  - Allows client to decide to which AP to roam.

- 802.11v, 80211w, etc.



Summary

- Wireless LANs
  - Different versions of IEEE 802.11
  - Beacon frames, association
- Multiple access: CSMA/CA
  - How to avoid interference from simultaneous transmission
- IEEE 802.11 standard
  - Frame format
  - Interworking with Ethernet 802.3
- Mobility
  - Within the same IP subnet
  - Between different subnets
  - Mobile IP: Short intro
- WLAN Security

Quellenverzeichnis

[1] A. Tanenbaum, D. Wetherall. *Computer Networks*, Fifth Edition, Pearson, 2014
dt. Ausgabe: "*Computernetzwerke*"

[2] http://www.webdonuts.com/comics/2014-04-28-wi-fi.jpg (abgerufen am 08.10.16)

[3] J. Kurose, K. Ross. *Computer Networking, A Top-Down Approach*, Sixth Edition, Pearson, 2013
dt. Ausgabe: "*Computernetzwerke – Der Top-Down Ansatz*"

[4] M. Sauter*, From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband*, Third Edition, John Wiley & Sons Ltd., 2017

[5] https://www.elektronik-kompendium.de/sites/net/0610051.htm (abgerufen am 23.03.2018)

Quellenverzeichnis

[1] A. Tanenbaum, D. Wetherall. *Computer Networks*, Fifth Edition, Pearson, 2014
dt. Ausgabe: "*Computernetzwerke"*

[2] http://www.webdonuts.com/comics/2014-04-28-wi-fi.jpg (abgerufen am 08.10.16)

[3] J. Kurose, K. Ross. *Computer Networking, A Top-Down Approach*, Sixth Edition, Pearson, 2013
dt. Ausgabe: "*Computernetzwerke – Der Top-Down Ansatz*"

[4] M. Sauter*, From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband*, Third Edition, John Wiley & Sons Ltd., 2017

[5] https://www.elektronik-kompendium.de/sites/net/0610051.htm (abgerufen am 23.03.2018)