521150A
Introduction to Internet

Lecture 6 – Data link layer, part IV: Wireless networks

Erkki Harjula 2023

Schedule of the course

PART I: Basics of networking and Internet, data link layer

Mon 13.3. 10-12 L6/Zoom	Lecture 1: Introduction & motivation
Tue 14.3. 10-12 L6/Zoom	Lecture 2: Architecture & design principles
Wed 15.3. 10-12 L5/Zoom	Lecture 3: Data link layer – basics part I
Thu 16.3. 10-12 L4/Zoom	Exercise session 1A
Mon 20.3. 10-12 L6/Zoom	Lecture 4: Data link layer – basics part II
Tue 21.3. 10-12 L6/Zoom	Exercise session 1B
Tue 21.3. 14-18 AT122/Zoom	Lab exercise 1 – group 3
Wed 22.3. 10-12 L5/Zoom	Lecture 5: Data link layer – Wired networks
Wed 22.3. 14-18 AT122/Zoom	Lab exercise 1 – group 4
Thu 23.3. 14-18 AT122/Zoom	Lab exercise 1 – group 2
Fri 24.3. 12-16 AT122/Zoom	Lab exercise 1 – group 1
Mon 27.3. 14-16 L5/Zoom	Exercise session 1C
Tue 28.3. 10-12 L6/Zoom	Lecture 6: Data link layer – Wireless networks
Wed 29.3. 10-12 Moodle	Theory exam 1

PART II: Network and transport layers

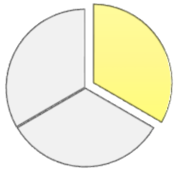
Thu 30.3. 8-10 L5/Zoom	Lecture 7: Network layer part I
Mon 3.4. 14-16 L5/Zoom	Exercise session 2A
Tue 4.4. 10-12 L6/Zoom	Lecture 8: Network layer part II
Wed 5.4. 10-12 L5/Zoom	Lecture 9: Transport layer part I; Course work intro
Tue 11.4. 10-12 L6/Zoom	Lecture 10: Transport layer part II
Tue 11.4. 14-18 AT122/Zoom	Lab exercise 2 – group 3
Wed 12.4. 10-12 Moodle	Theory exam 2
Wed 12.4. 14-18 AT122/Zoom	Lab exercise 2 – group 4
Thu 13.4. 8-10 L5/Zoom	Exercise session 2B
Thu 13.4. 14-18 AT122/Zoom	Lab exercise 2 – group 2
Fri 14.4. 12-16 AT122/Zoom	Lab exercise 2 – group 1

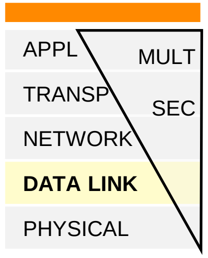
PART III: Application layer, network security and multimedia

Fri 14.4. 10-12 L5/Zoom	Lecture 11: Networking applications
Mon 17.4. 14-16 L5/Zoom	Lecture 12: Network security
Tue 18.4. 10-12 L6/Zoom	Exercise session 3A
Wed 19.4. 10-12 L5/Zoom	Lecture 13: Multimedia and QoS
Mon 24.4. 14-16 L5/Zoom	Exercise session 3B
Tue 25.4. 14-18 AT122/Zoom	Lab exercise 3 – group 3
Wed 26.4. 10-12 L5/Zoom	Lecture 14: Challenges&Future Internet trends
Wed 26.4. 14-18 AT122/Zoom	Lab exercise 3 – group 4
Thu 27.4. 14-18 AT122 /Zoom	Lab exercise 3 – group 2
Fri 28.4. 12-16 AT122 /Zoom	Lab exercise 3 – group 1
Wed 3.5. 10-12 Moodle	Theory exam 3
Thu 25.5. 16-19 L1	Final exam

Course work (independent work)

Main learning objectives of this lecture

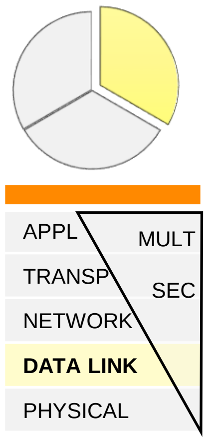




1. Know the basics of wireless networks
2. Be aware of the basic concepts and functions of IEEE 802.11 WLAN
   - Architecture
   - Medium access control (DCF, CSMA/CA, RTS/CTS)
   - Technology evolution

Basics of Wireless Communication: Elements, topologies, types, link characteristics

Starting premise & promise

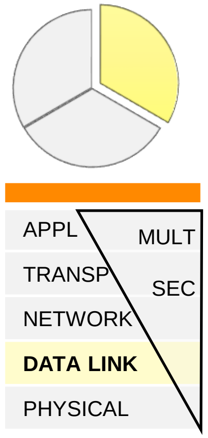


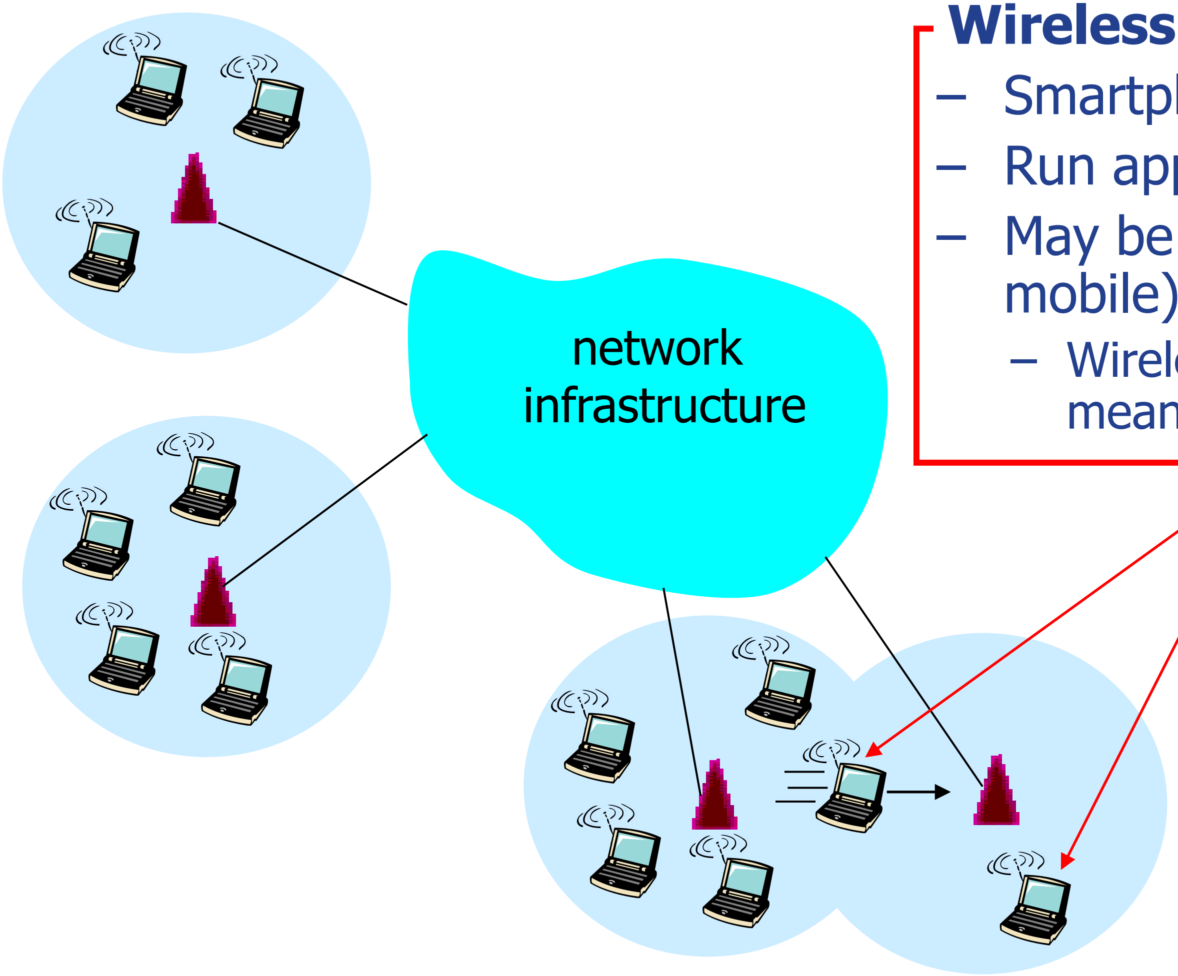
- Wireless (mobile) phone subscribers has a long time ago exceeded wired phone subscribers

- Computer networks: laptops, tablets, Internet-enabled phones provide anytime untethered Internet access

- Two important related but different challenges
  - **Wireless**: communication over wireless link
  - **Mobility**: handling mobile user who changes point of attachment to network

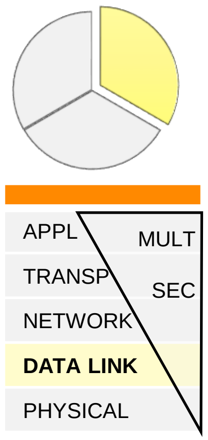
Elements of a wireless network (1)

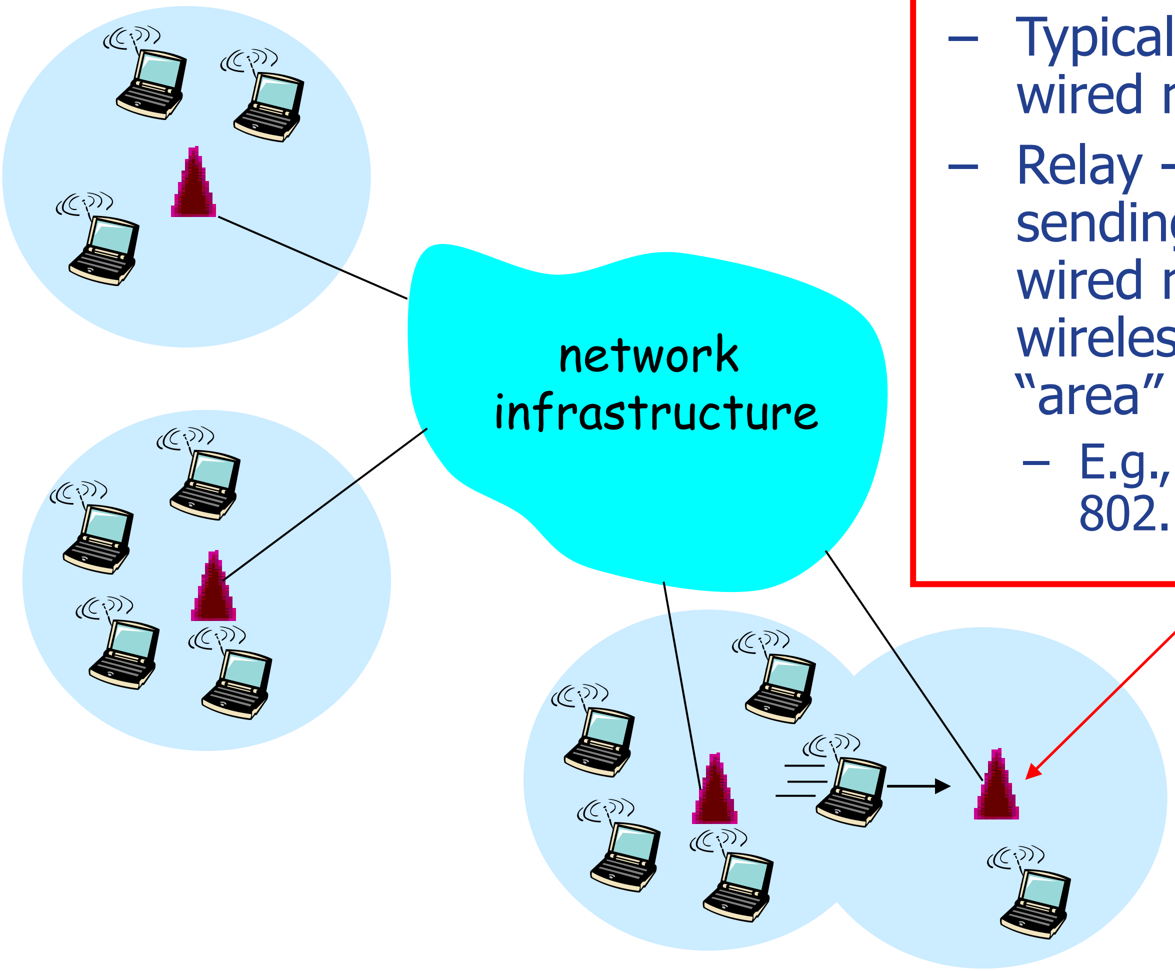




Wireless hosts
- Smartphone, tablet, laptop
- Run applications
- May be stationary (non-mobile) or mobile
  - Wireless does *not* always mean mobility

Elements of a wireless network (2)

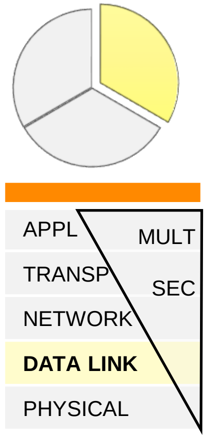


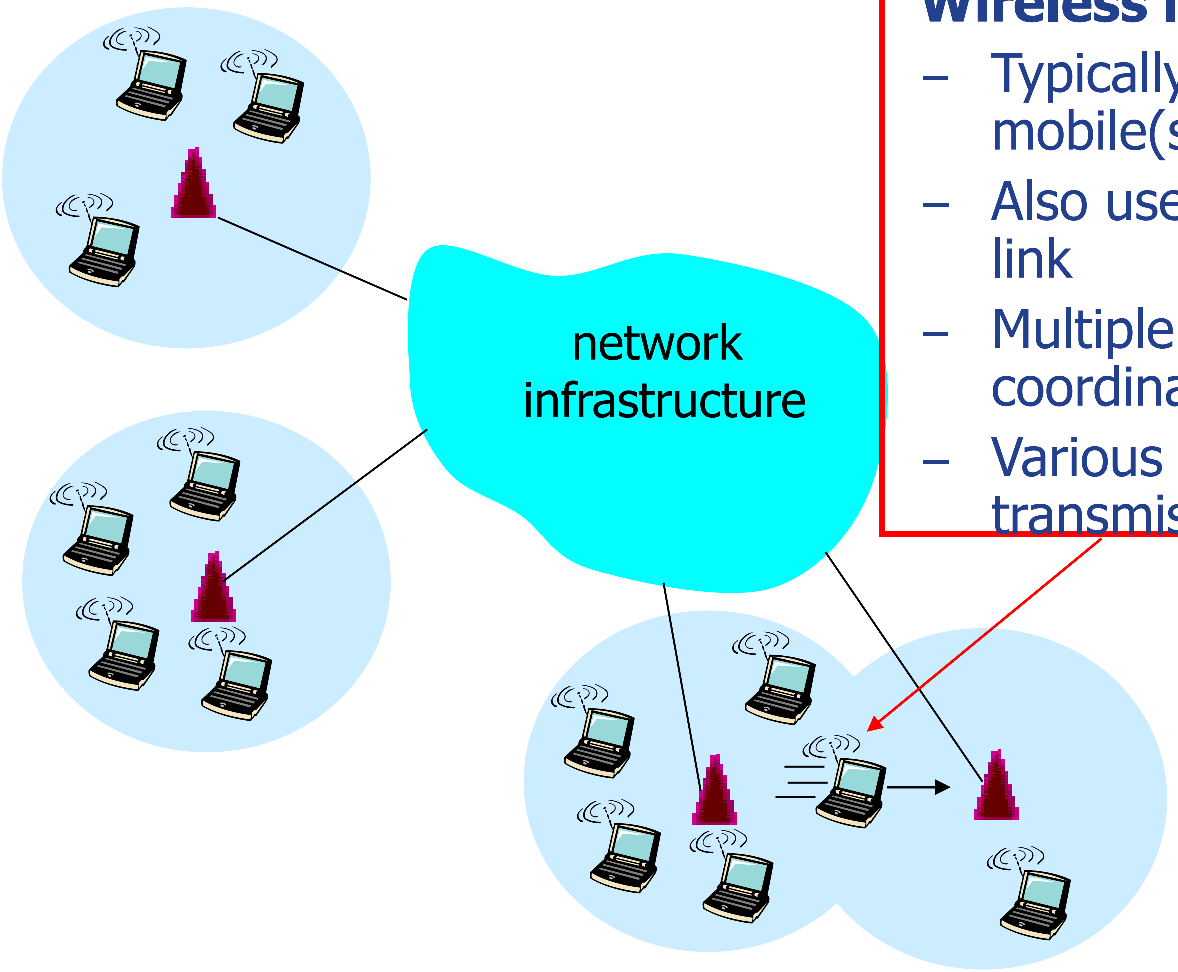


Base station

- Typically connected to wired network
- Relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - E.g., GSM/3G/4G tower, 802.11 AP (access point)

Elements of a wireless network (3)

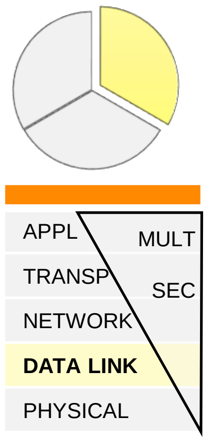


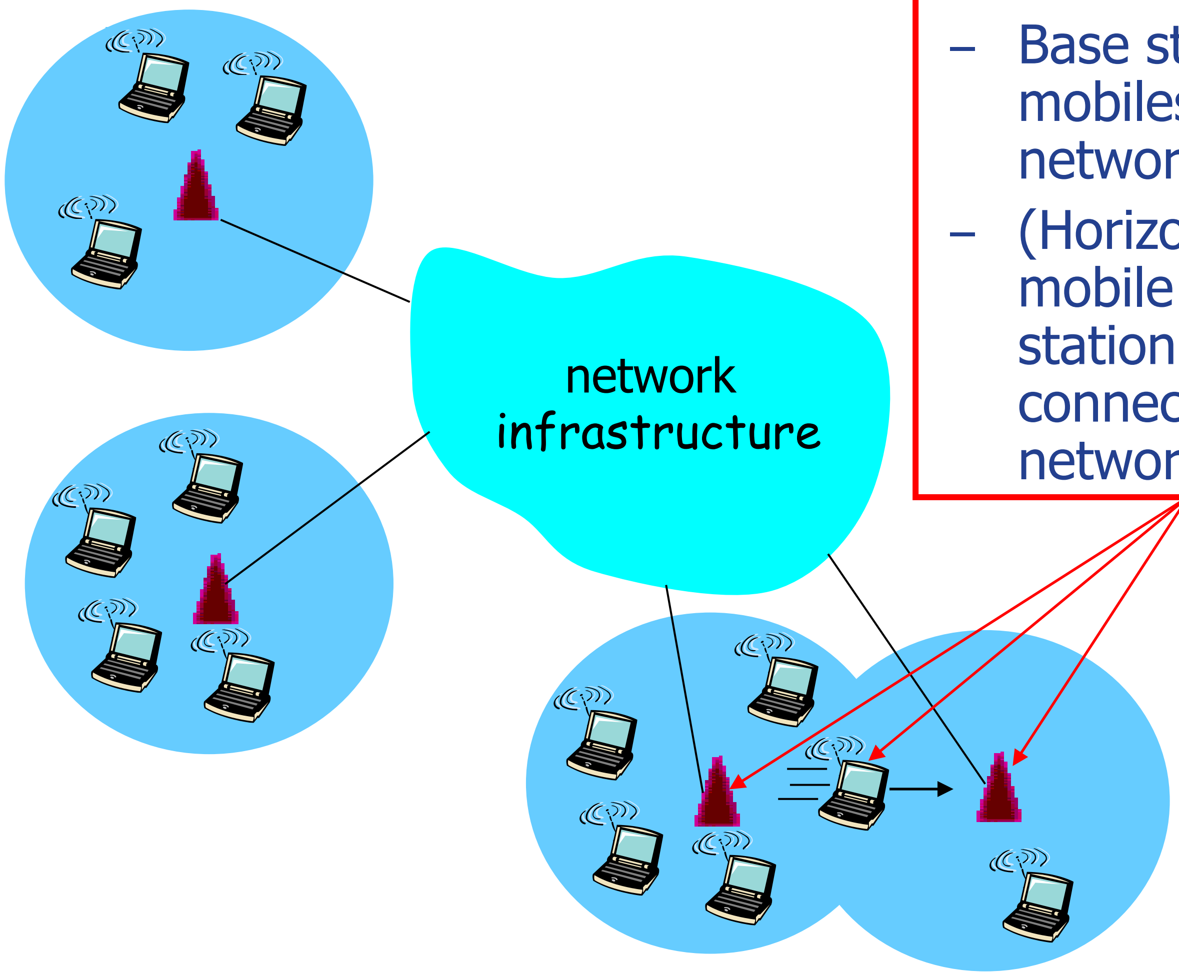


Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access
- Various data rates, transmission distance

Elements of a wireless network (4)

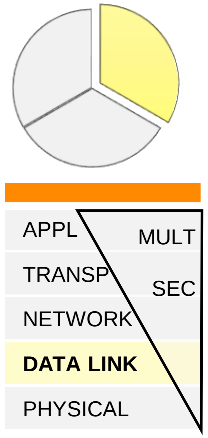


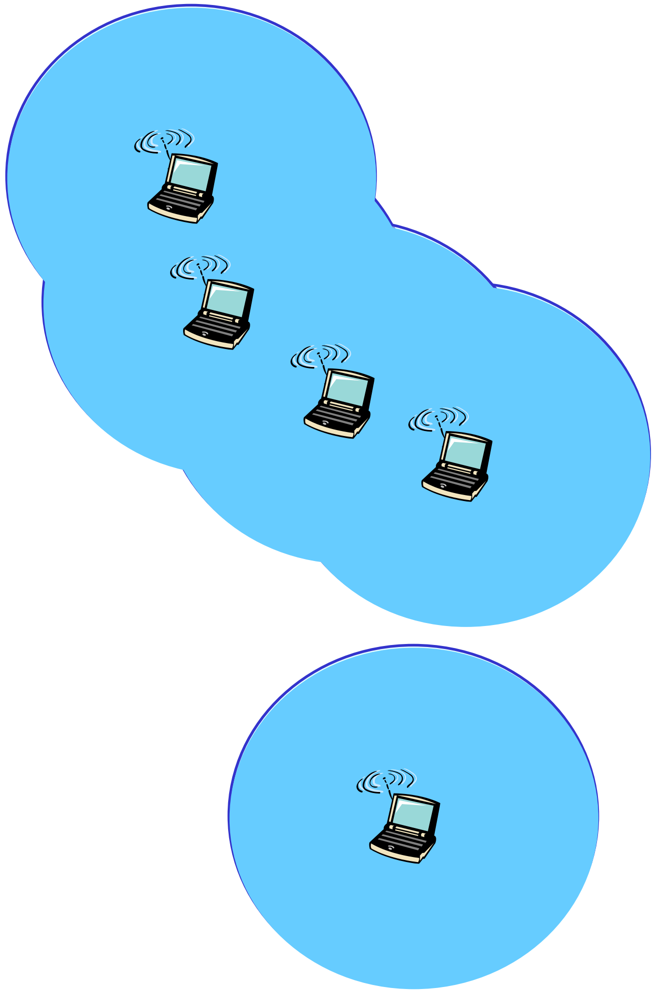


Infrastructure mode

– Base station connects mobiles into wired network
– (Horizontal) Handoff: mobile changes base station providing connection into wired network

Elements of a wireless network (5)

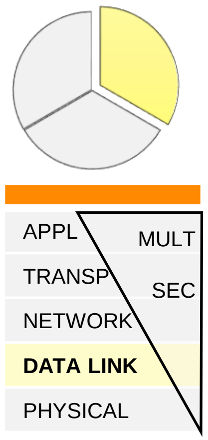




Ad hoc mode

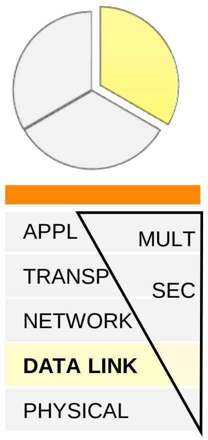
- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes organize themselves into a network: route among themselves

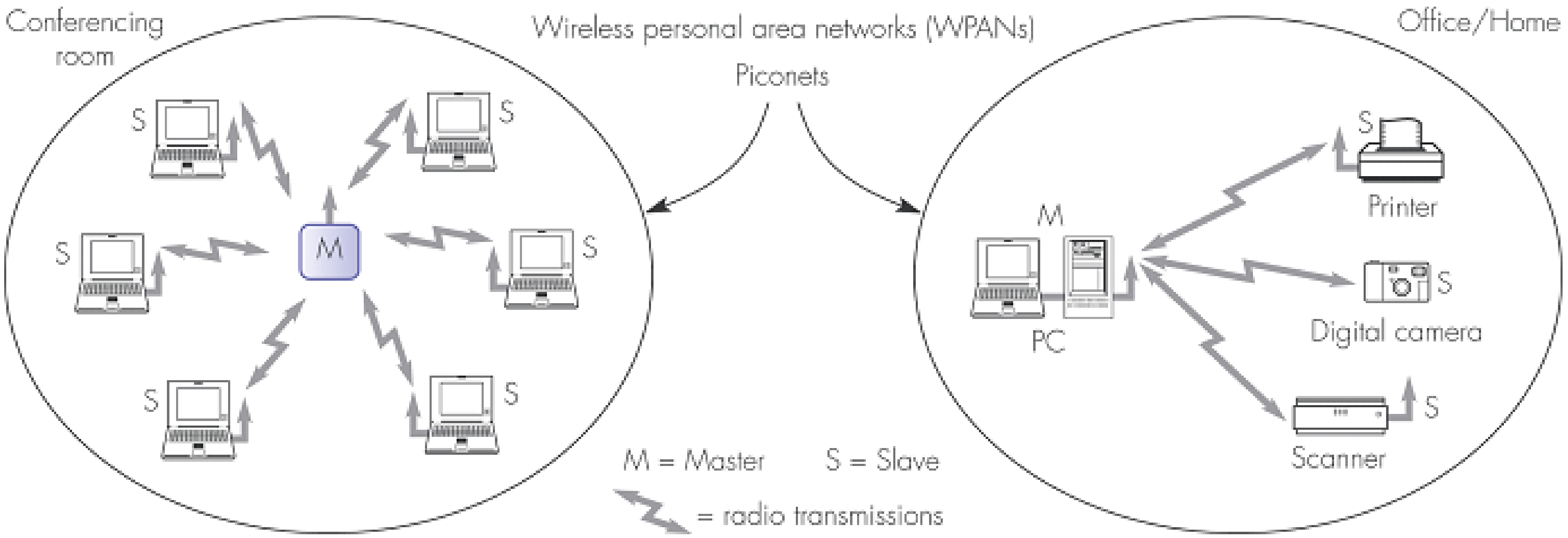
Elements of a wireless network (6)



	Single hop	Multi hop
Infrastructure	Host connects to base station (WiFi, WiMAX, cellular) which connects to Internet	Host may have to relay through several wireless nodes to connect to Internet (mesh network)
Ad hoc	No base station, no connection to Internet (Bluetooth, ad hoc nets)	No base station, no connection to Internet, may have to relay over wireless nodes to reach given wireless node (MANET, VANET)

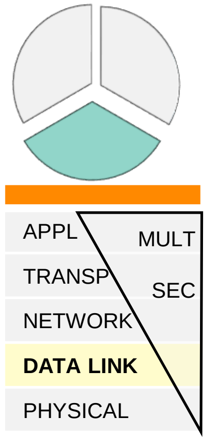
Wireless networks: WPAN (Wireless Personal Area Network) (also Wireless Body Area Network)





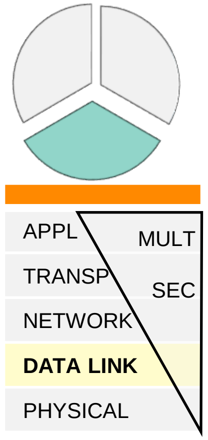
Many different technologies for implementing WPAN:
Bluetooth, IEEE 802.15.X, Zigbee, Wibree, ...

Example WPAN: home automation



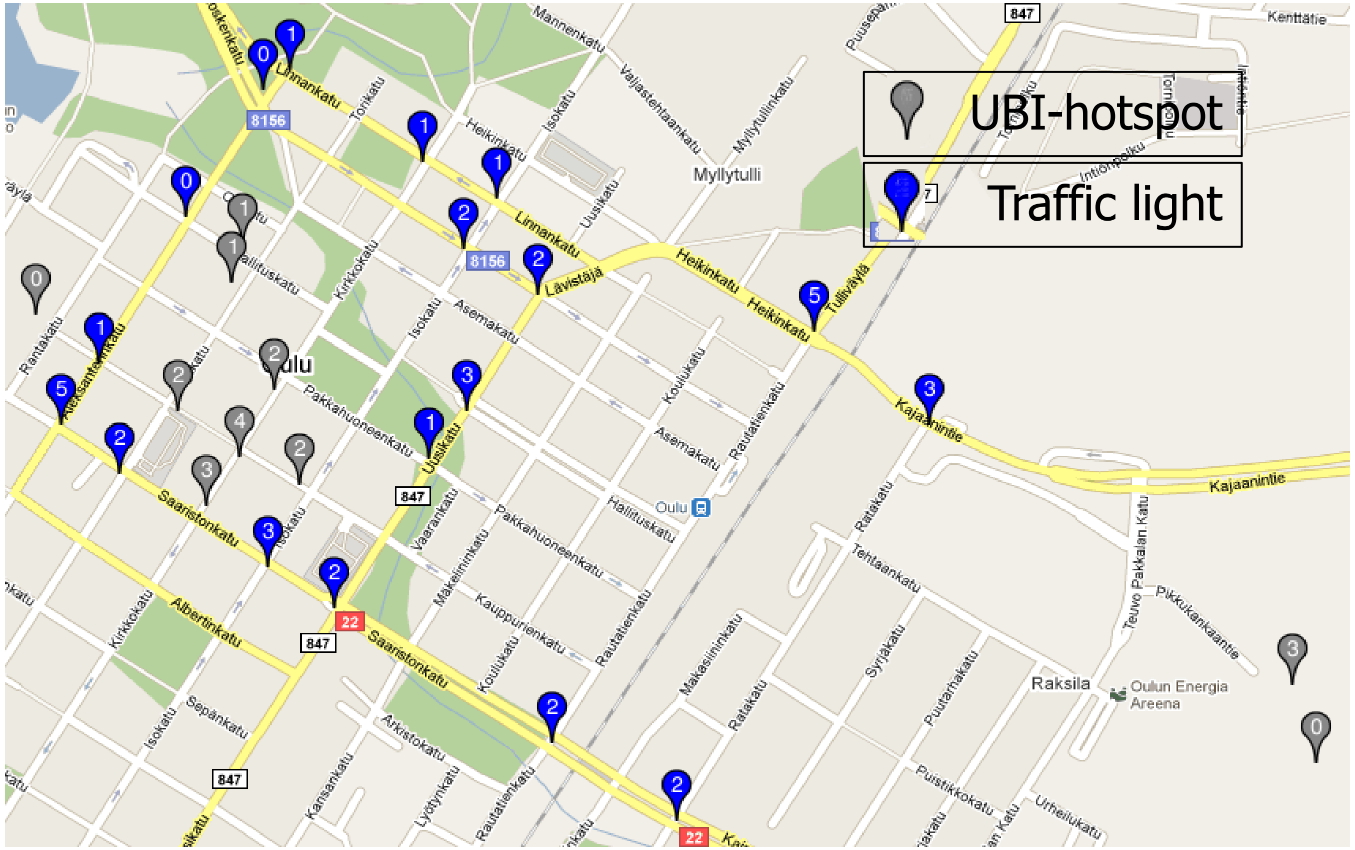
- **Sensor nodes**
  - Distributed around home to collect data about temperature, humidity, moisture, motion, smoke etc.
- **Actuator nodes**
  - Control different home appliances, locking, doors, alarms, air ventilation, heating, etc.
- **Central unit**
  - Operational logic, applications, data processing
    - Local or cloud-based
  - Communicates with sensors and actuators
    - Typically BLE, ZigBee, or other low-power radios
    - Also e.g. WLAN for e.g. surveillance cameras
  - Connects home automation to
  - Internet for remote control&access

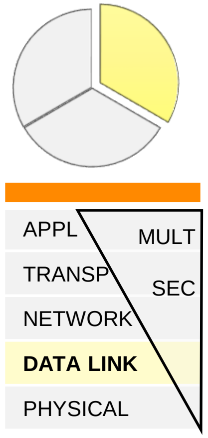
Example WPAN: panOULU BT



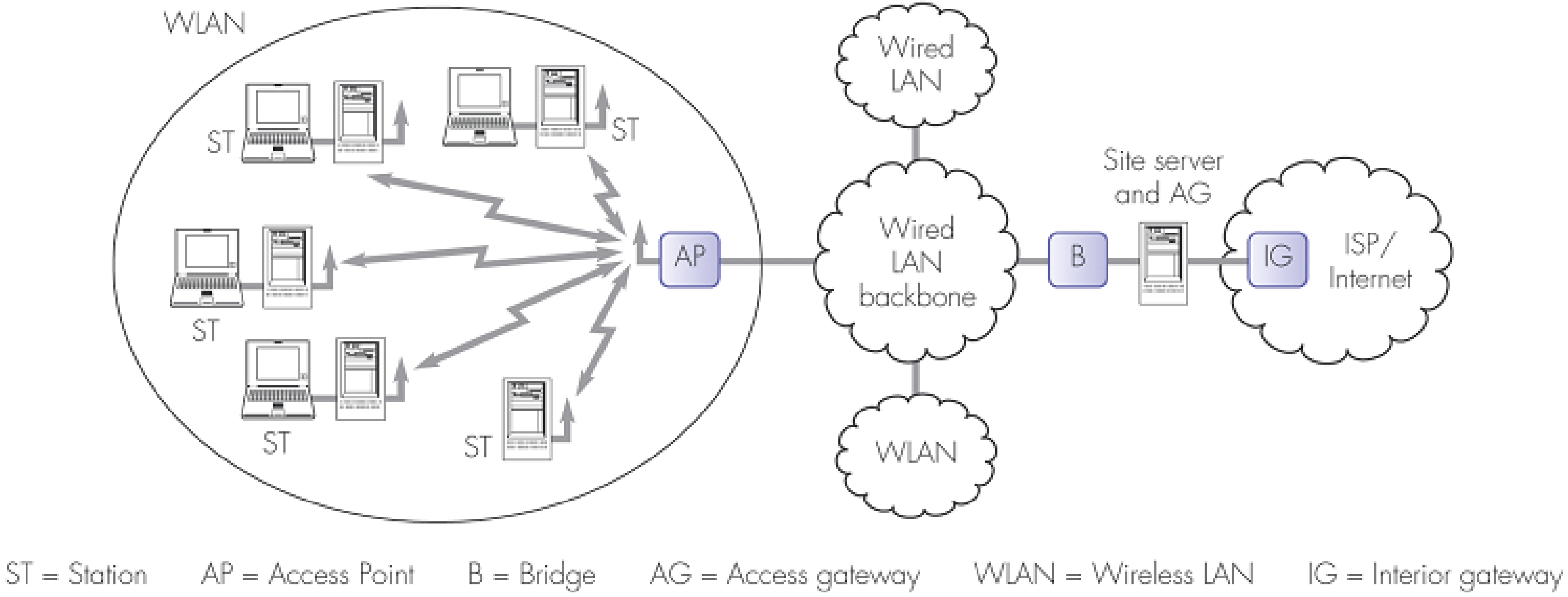
- ~60 BT access points around Oulu (each has 3 BT radios)
- Traffic light poles
- UBI-hotspots
- Portable enclosures with touch screens

panOULU
http://www.panoulu.net/
AVOIN VERKKO
Bluetooth™
OPEN NETWORK



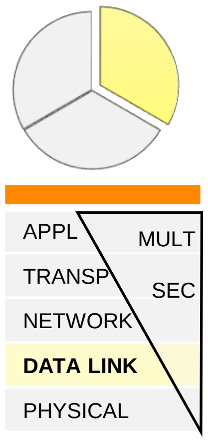


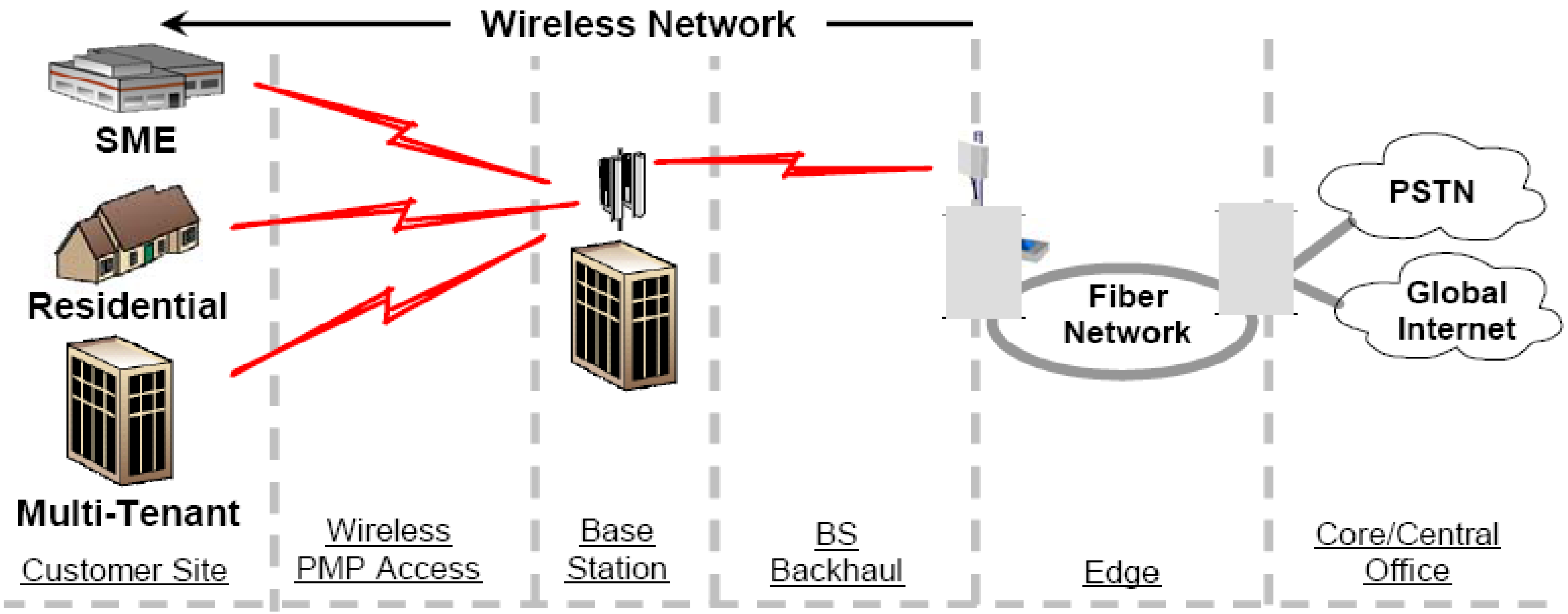
Wireless networks:
WLAN (Wireless Local Area Network)



WLAN often implemented with IEEE 802.11 (”WiFi”)

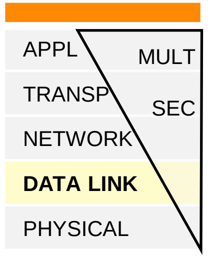
Wireless networks: WMAN (Wireless Metropolitan Area Network)





WMAN often implemented with IEEE 802.16 (”WiMAX”)

Wireless networks: Cellular/mobile radio networks



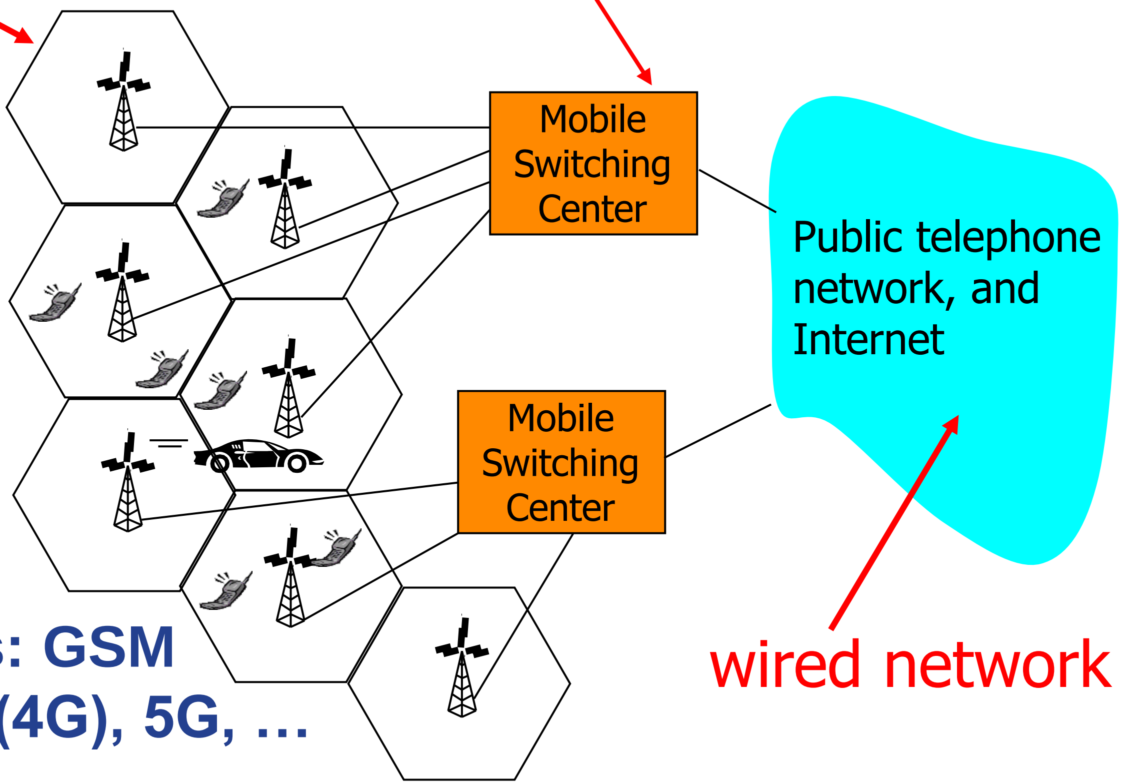
Considered as WMAN or WWAN networks

MSC

- Connects cells to wide area net
- Manages call setup
- Handles mobility

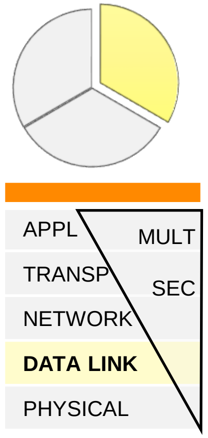
Cell

- Covers geographical region
- *Base station* (BS)
- *Mobile users* attach to network through BS
- *Air-interface:* physical (L1) and link layer (L2) protocol between mobile and BS

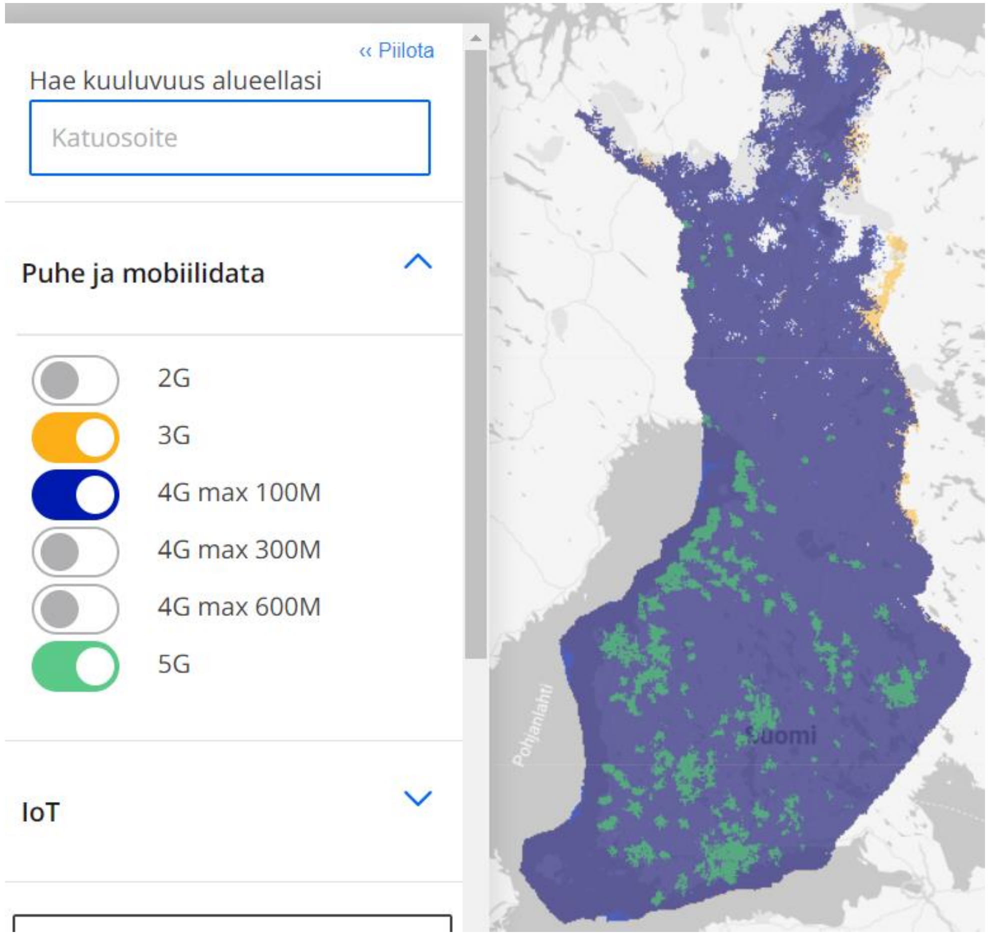


Different technologies: GSM (2G), UMTS (3G), LTE (4G), 5G, …

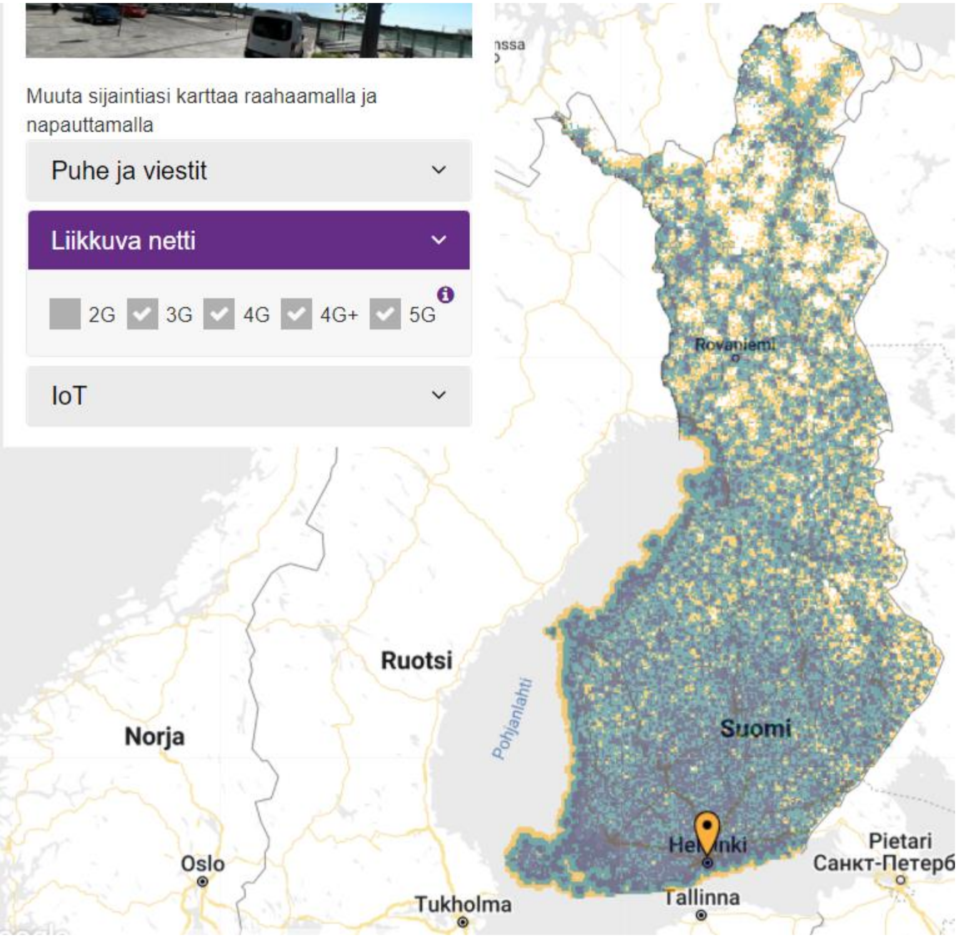
Example Cellular



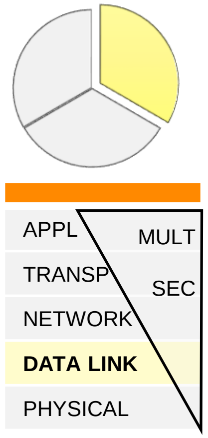
– Elisa



-Telia



Wireless link characteristics (1)

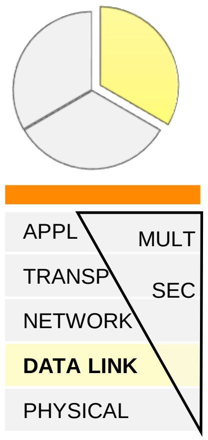


– Differences from a wired link ….

- **Decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **Interference from other sources:** license exempt ("free") wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., microwave ovens); motors interfere as well
- **Multipath propagation:** radio signal reflects off objects ground, arriving at destination at slightly different times

… make communication across wireless link (even point-to-point) much more "difficult"

Wireless link characteristics (2)



– Issues relevant to link performance

- Transmission power

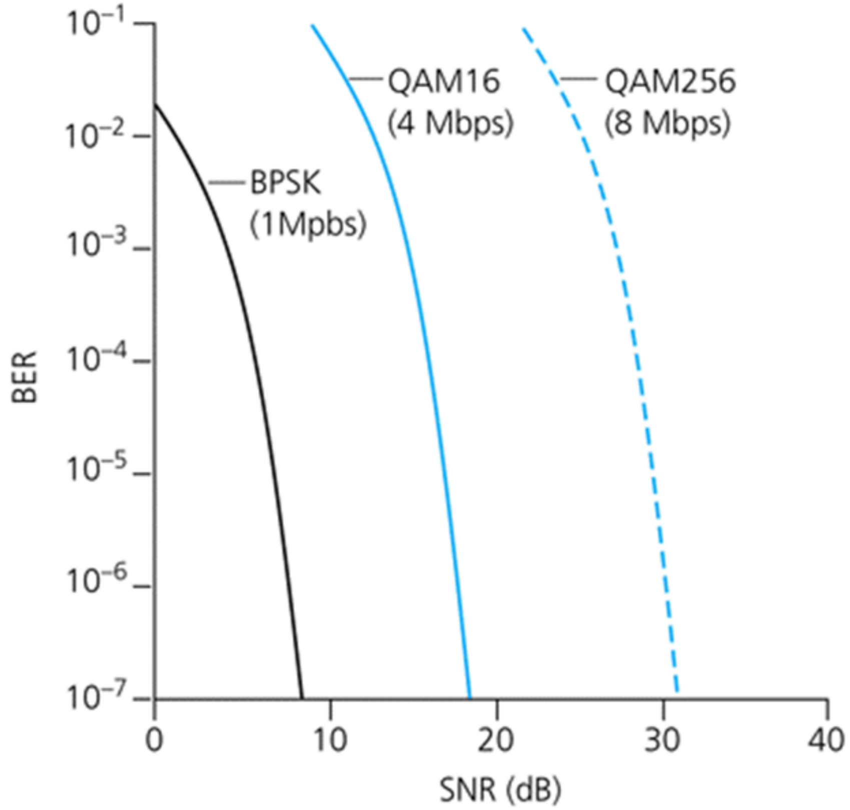
- 👍 More power → higher SNR → lower BER & longer range
- 👎 More power → higher energy consumption & stronger interference

- Channel bandwidth

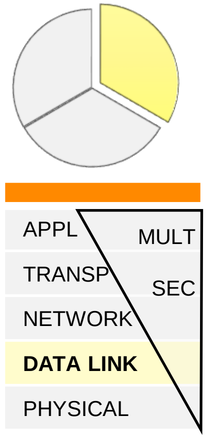
- 👍 Larger bandwidth → higher data rate
- 👎 Frequency bandwidth is a finite resource

- Modulation scheme

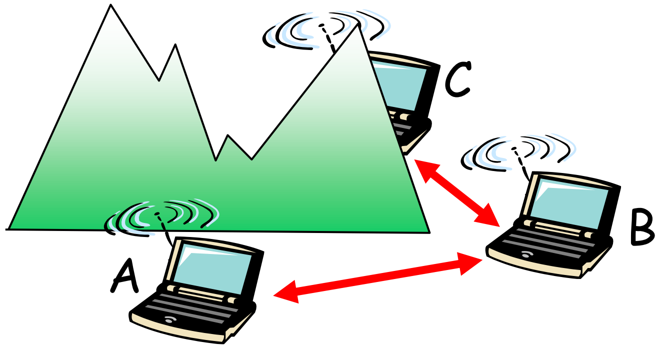
- For a given SNR, different modulation schemes produce different data transmission rates and bit error rates
  - Scheme producing higher data transmission rate will produce higher bit error rate for given SNR
- Adaptive modulation: dynamic selection of modulation technique to adapt to varying channel conditions as result of user mobility or changes in environment



Wireless link characteristics (3)

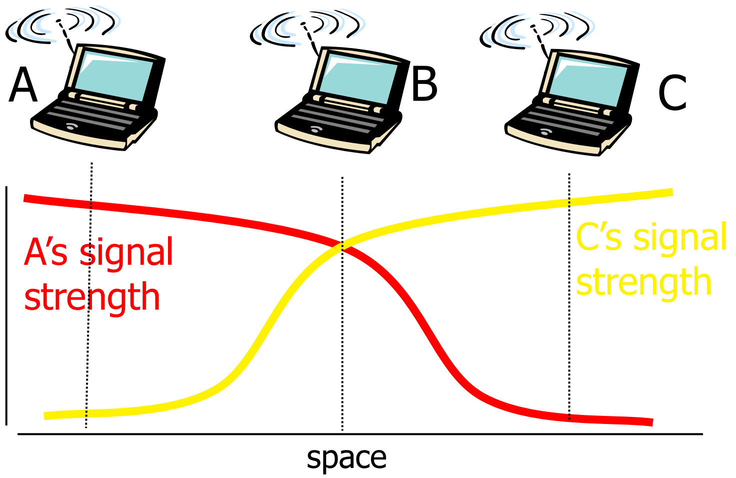


Multiple wireless senders and receivers create additional problems (beyond multiple access)



Hidden terminal problem

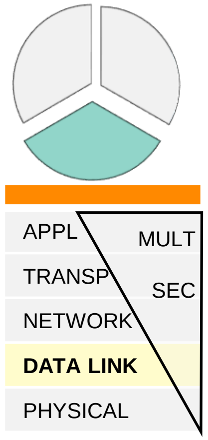
- B, A hear each other
- B, C hear each other
- A, C can not hear each other
- → A, C unaware of their interference at B



Signal fading

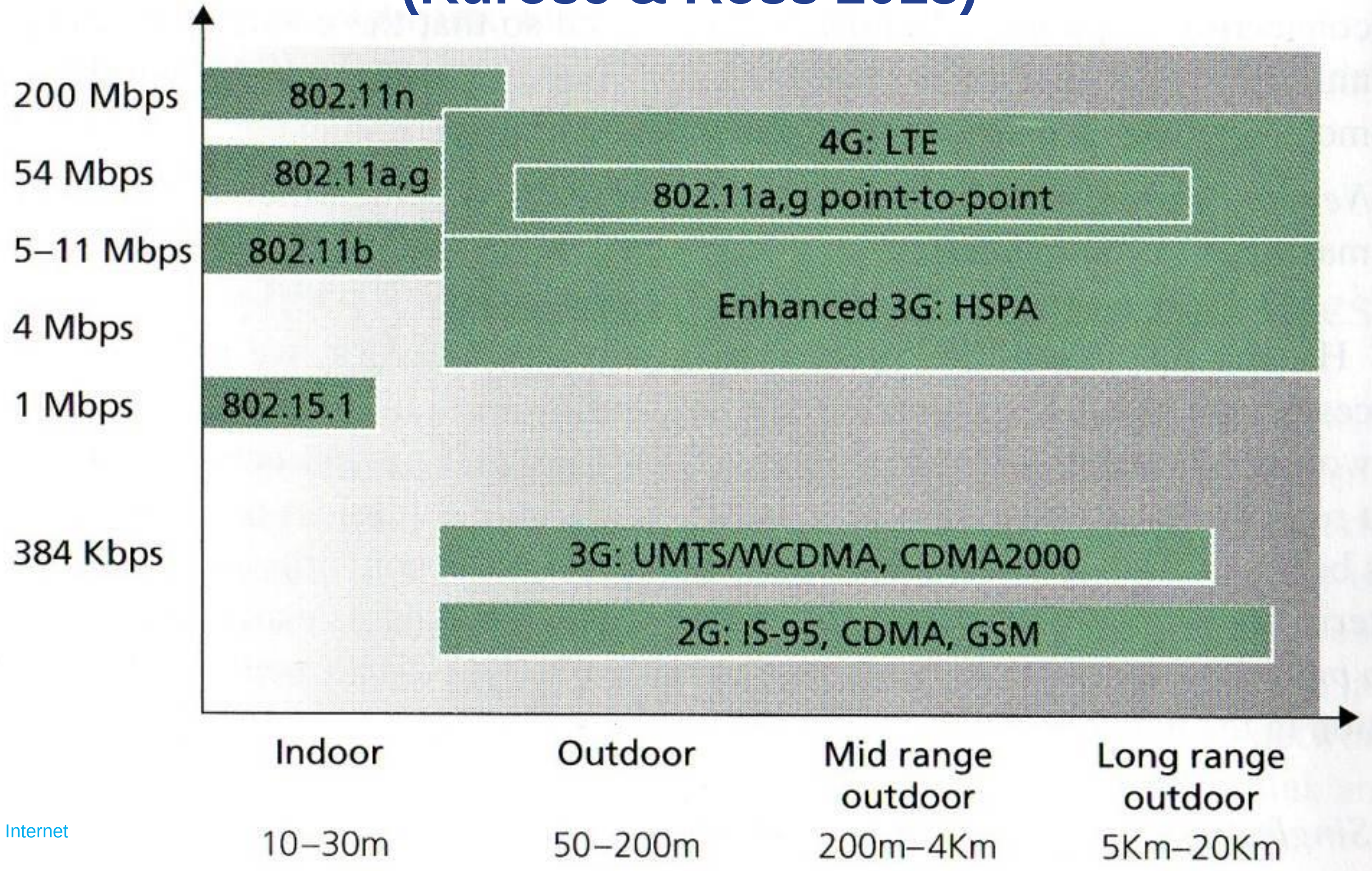
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Wireless link characteristics (4)



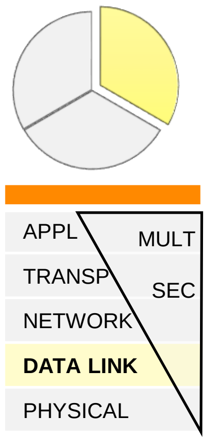
Characteristics of selected wireless network standards

(Kurose & Ross 2013)



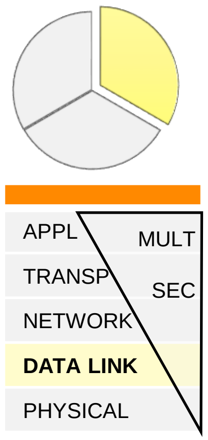
Wireless LAN (WLAN): Architecture & Services

IEEE 802.11 WLAN (Wireless LAN)

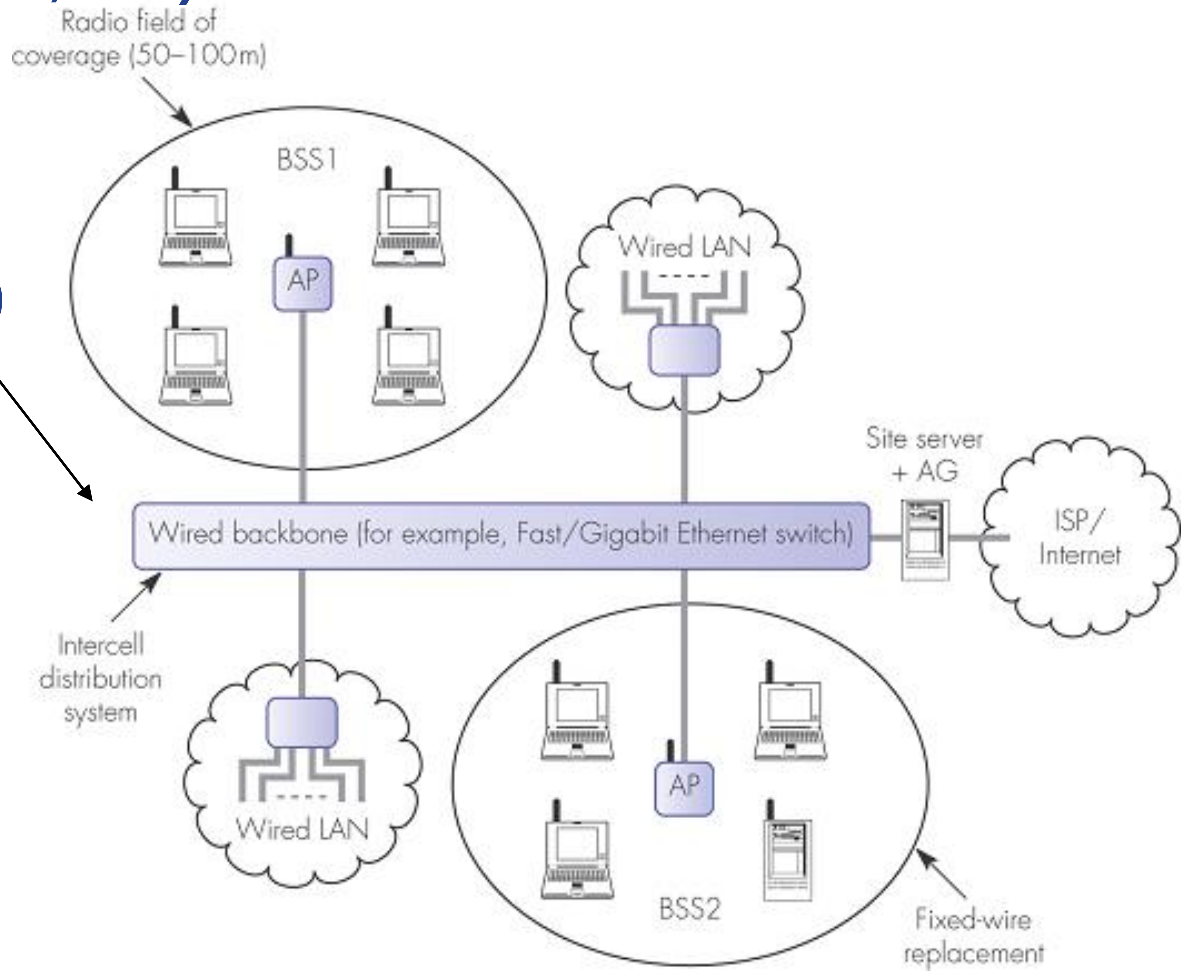


- ”Wireless Ethernet”
- Called WLAN (Europe) or WiFi (USA)
  - Wi-Fi Alliance (http://www.wi-fi.org/)
- Rapid growth of WLAN market
  - License exempt frequency band (anyone can set up WLAN)
  - Cheap technology
  - Mature technology (great interoperability)
  - Increasing user device support
    - ~100% of laptops have a WLAN radio
    - Majority of mobile phones also have a WLAN radio
  - ”New AP deployed every 4 seconds” (Intel)

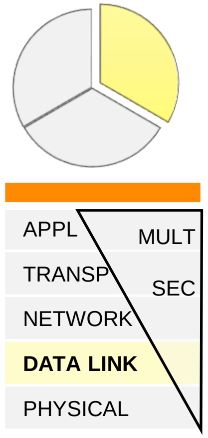
WLAN: Architecture (1)



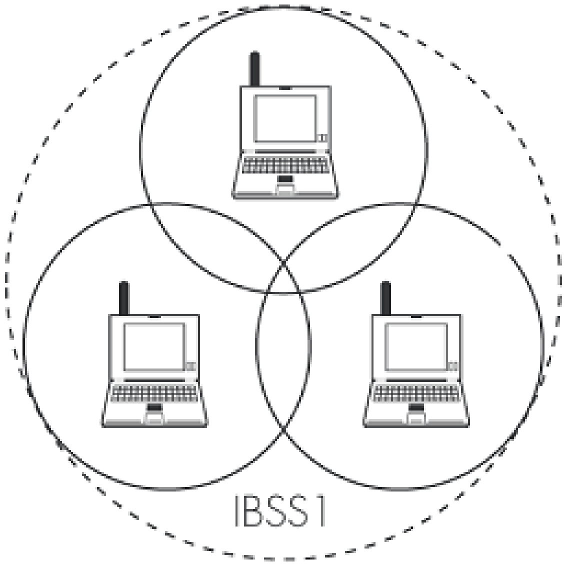
- **Infrastructure mode**
  - All communication takes place between AP (access points) and wireless devices (stations, STA)
  - AP takes care of medium access control
  - AP bridges to another cell and/or fixed LAN
  - DS (distribution system) supports mobility between cells
  - AP + stations form **BSS (Basic Service Set)**
  - Multiple cells connected by DS form **ESS (Extended Service Set)**



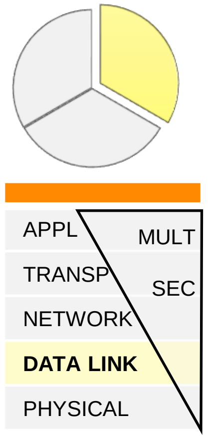
WLAN: Architecture (2)



- **Ad hoc mode**
  - **No AP**
  - **No distribution system**
  - **Communication takes place directly between stations**
  - **Stations take care of medium access control**
  - **Stations form IBSS (Independent Basic Service Set)**

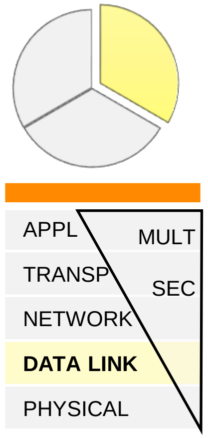


WLAN: Architecture (3)



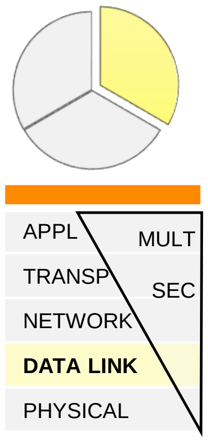
- **WiFi Direct mode**
  - **”Infrastructure mode with no dedicated AP”**
  - **Stations negotiate each other to decide which device will act as an AP**
  - **AP acts as a bridge to another wireless/wired network**

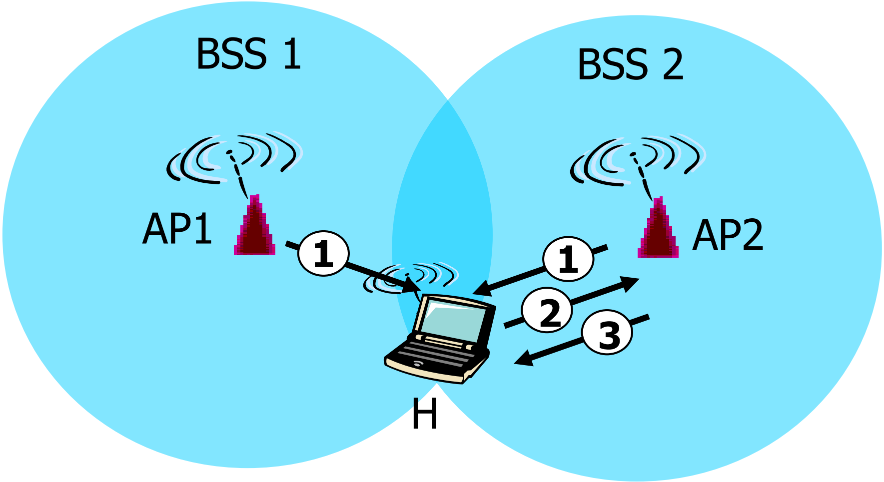
WLAN: Services (distribution system)

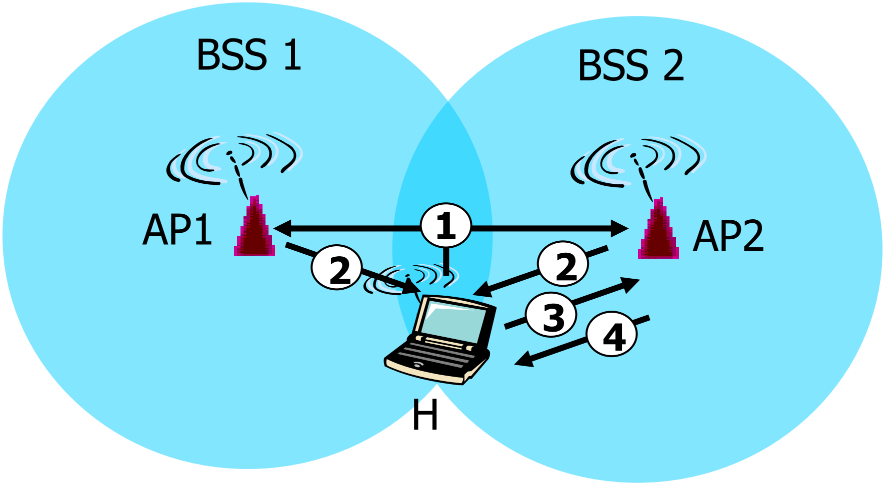


1. **Association**
   - **Used by stations to connect to APs**
   - **Frequency spectrum is divided to channels at different frequencies**
   - **AP is configured for a particular channel**
     - Interference possible (channel can be same as that chosen by nearby AP) → channel design needed in large WLAN networks of many APs
   - **Station scans channels, listening for beacon frames containing AP's name (SSID) and MAC address**
     - AP can advertise multiple SSID's (eduroam & panoulu on our campus)
   - **Selects AP to associate with, initiates association protocol**
2. **Disassociation**
   - **Either station or AP may break the relationship**
3. **Reassociation**
   - **Change of preferred AP when moving from one cell to another**
4. **Distribution**
   - **Determination of how to route the frames sent to AP**
5. **Integration**
   - **Translation of 802.11 frames to the format of destination network**

WLAN: Active/passive scanning







Passive scanning

(1) Beacon frames sent from APs

(2) Association Request frame sent (H to selected AP)

(3) Association Response frame sent (selected AP to H)

Active scanning

(1) Probe Request frame broadcast by H

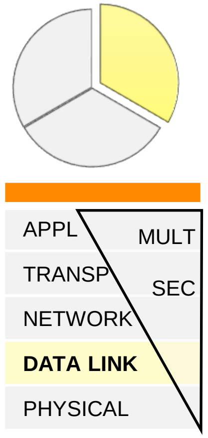
(2) Probe Response frame sent from APs

(3) Association Request frame sent (H to selected AP)

(4) Association Response frame sent (selected AP to H)

Note: same AP can provide multiple logical SSID's

WLAN: Services (intracell, provided by station)



1. Authentication

- A station may need to authenticate itself before it can send data
- AP sends a challenge frame to see if station knows the secret key (password) assigned to the AP

2. Deauthentication

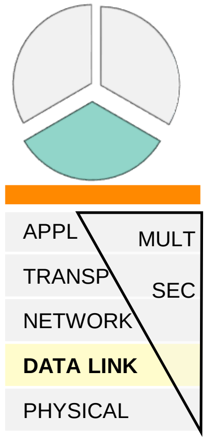
- Removes prior authentication

3. Privacy

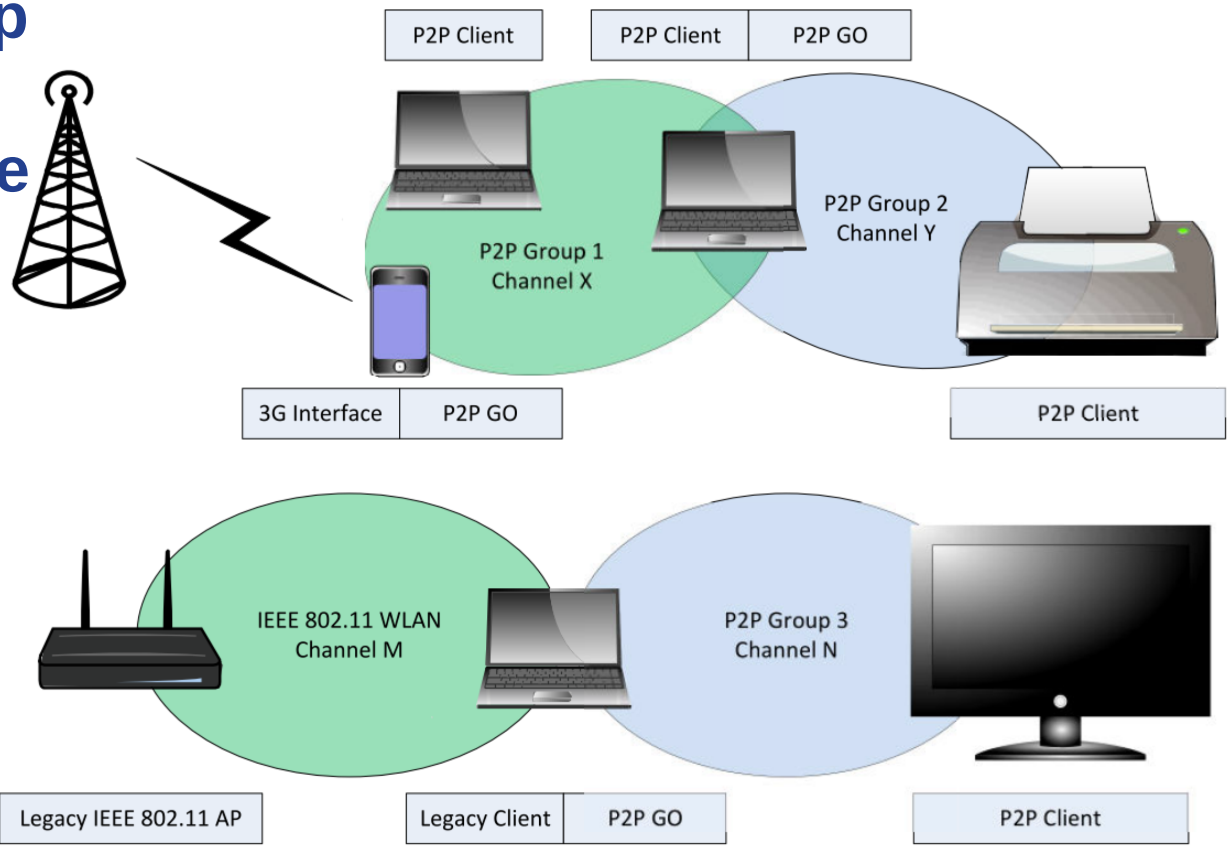
- Manages encryption and decryption of transmitted data

4. Data delivery

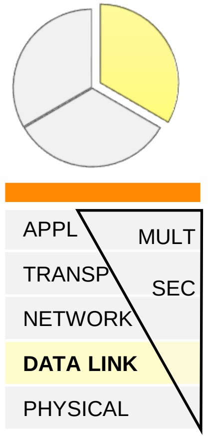
WLAN: Wi-Fi Direct ”Ad-Hoc mode”

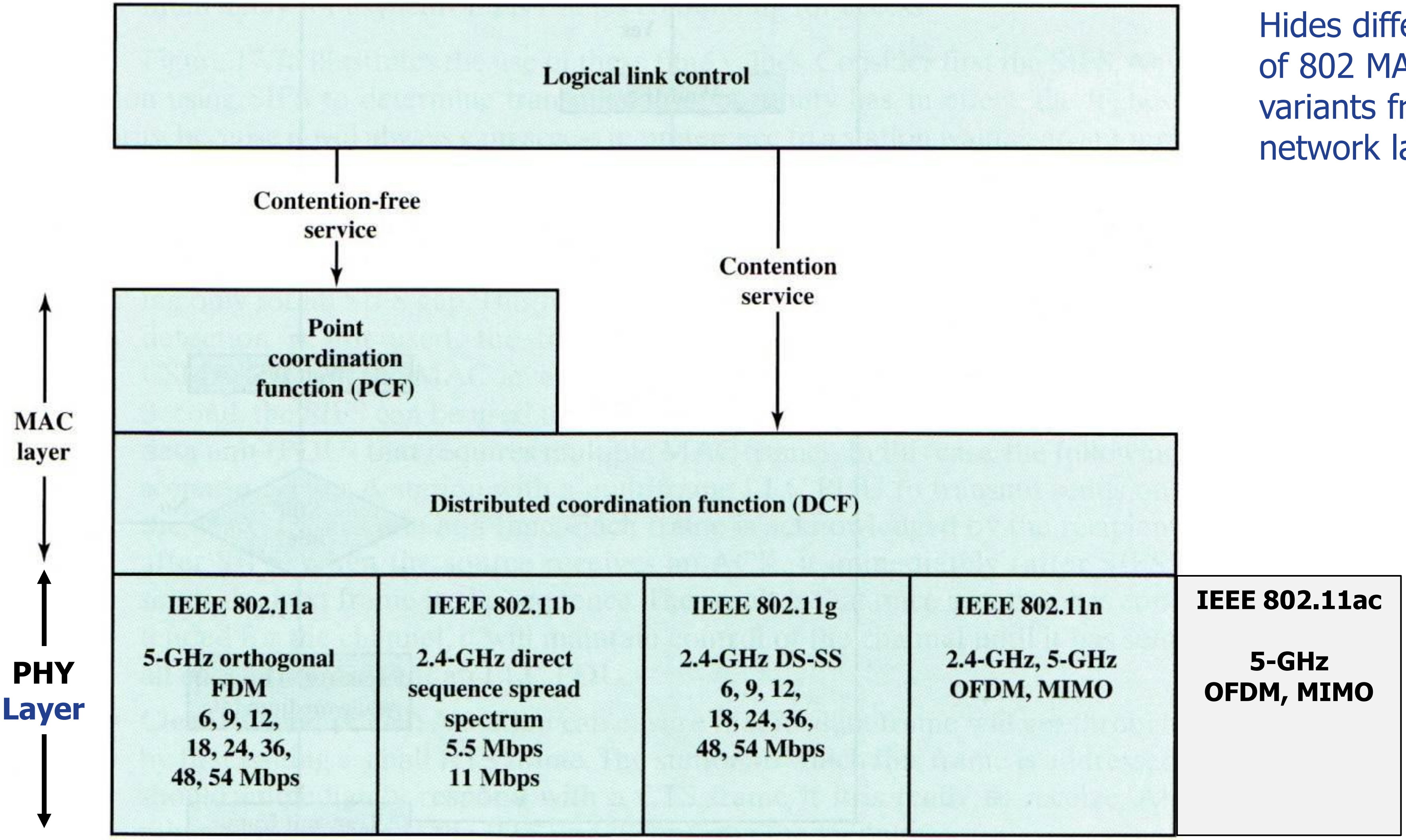


- **For connecting Wi-Fi devices directly (without AP) for sharing and exchanging content and applications**
- **In WiFi Direct, a Group Owner (GO) needs to be selected among the joined nodes**
  - P2P Standard group formation
  - P2P Autonomous group formation
  - P2P Persistent group formation
- **Example topologies:**

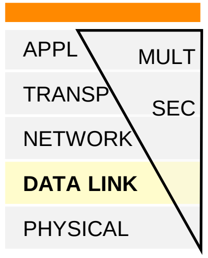


WLAN: Protocol architecture



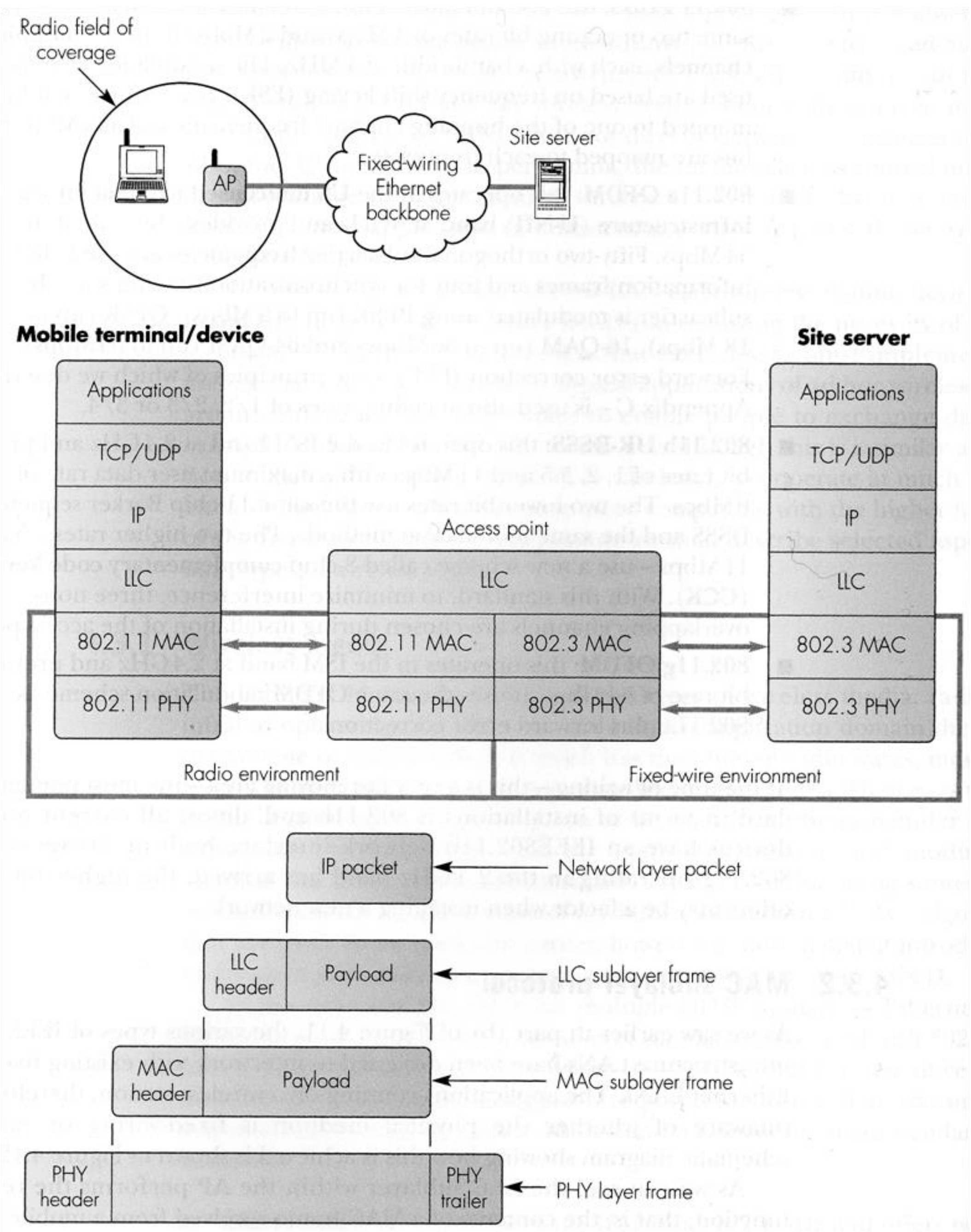


Hides differences of 802 MAC variants from network layer



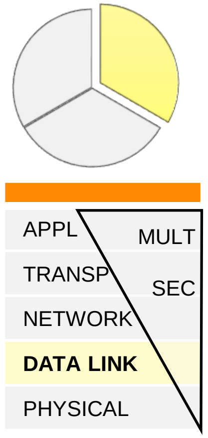
WLAN: Protocol architecture (2)

- IEEE 802.11/802.3 interworking schematic



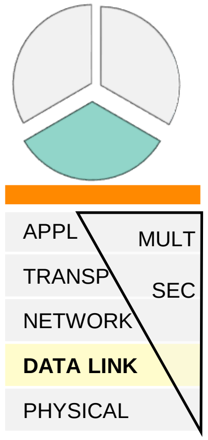
Wireless LAN (WLAN): MAC Sublayer & frame structure

WLAN: MAC sublayer

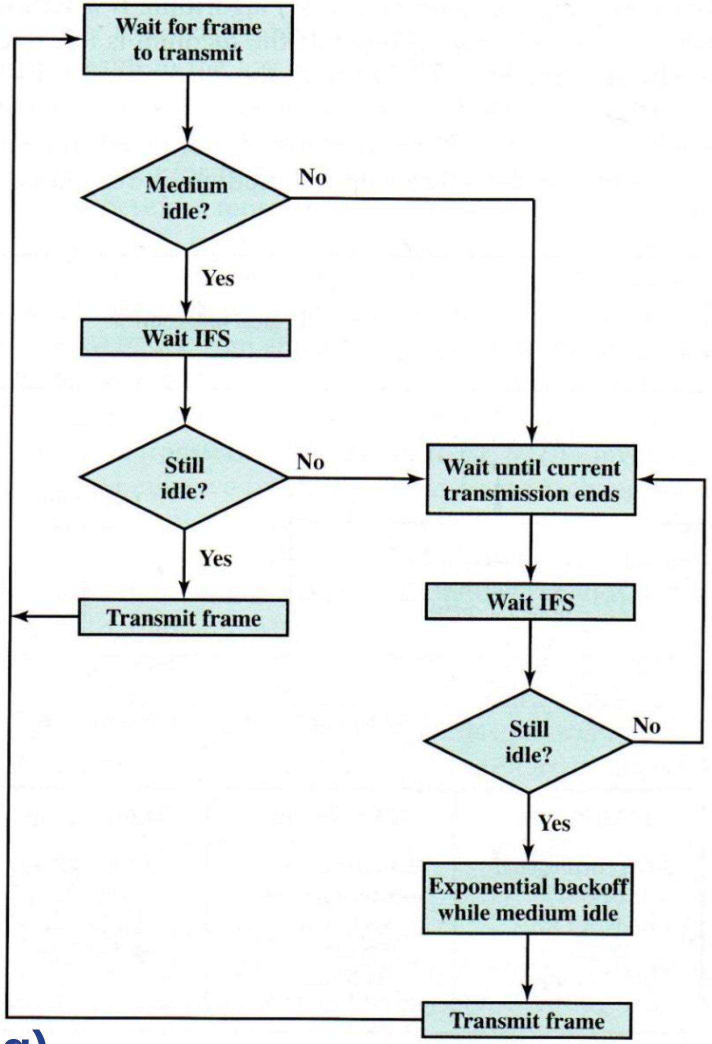


- Two modes of operation
  - DCF (Distributed Coordination Function)
    - No central control
    - CSMA/CA (Collision Avoidance) as medium access protocol
    - Asynchronous best-effort variable delay service
    - Mandatory
  - PCF (Point Coordination Function)
    - AP controls access to the shared radio medium in its cell
    - Time-bounded service
    - Optional

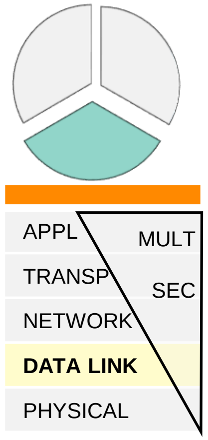
WLAN: MAC - DCF



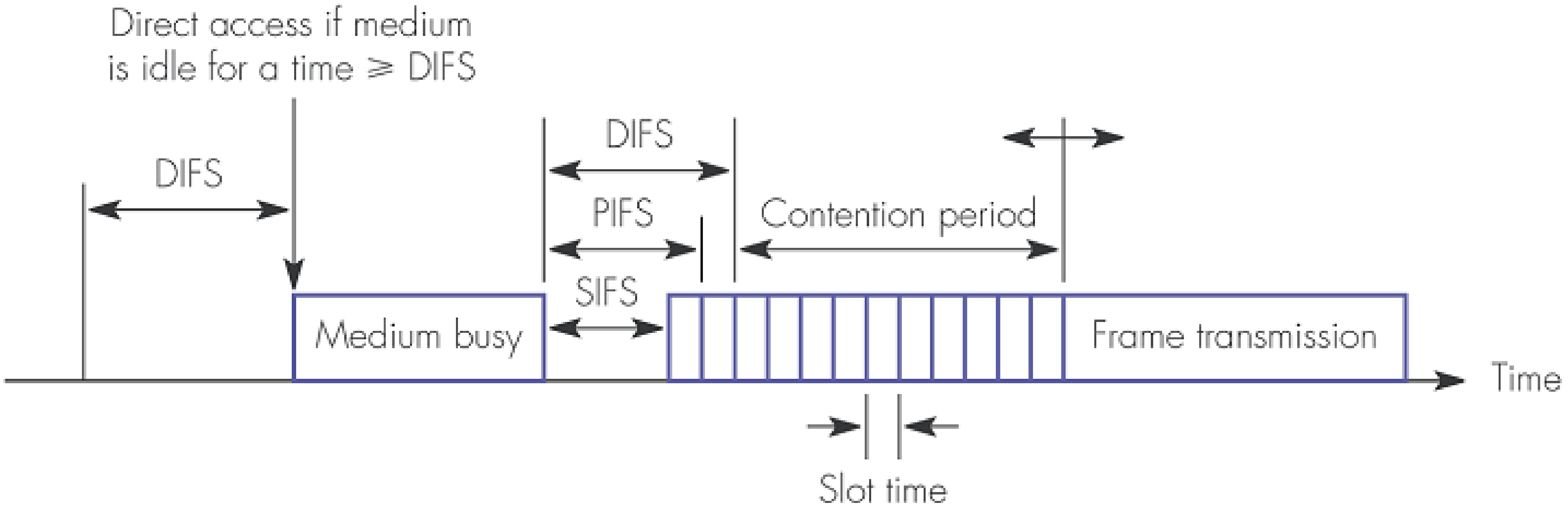
- Like Ethernet, uses CSMA
  - Random access
  - Carrier sense: do not collide with ongoing transmission
- Unlike Ethernet
  - No collision detection – transmit all frames to completion
  - Acknowledgment – because without collision detection, you do not know if your transmission collided or not?
- Why no collision detection?
  - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - Can not sense all collisions in any case (hidden terminals, fading)
- Goal: *avoid collisions ->* CSMA/C(ollision)A(voidance)



WLAN: MAC - DCF: Parameters



– **Definition of timing parameters**

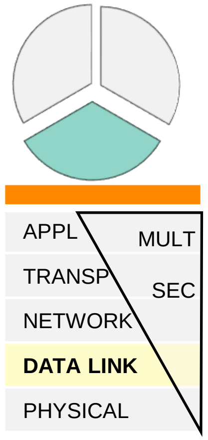


SIFS = short inter-frame waiting time (and hence highest priority)

DIFS = longest inter-frame waiting time (and hence lowest priority)

PIFS = a waiting time between SIFS and DIFS (and hence medium priority)

WLAN: MAC - DCF: Sending and receiving



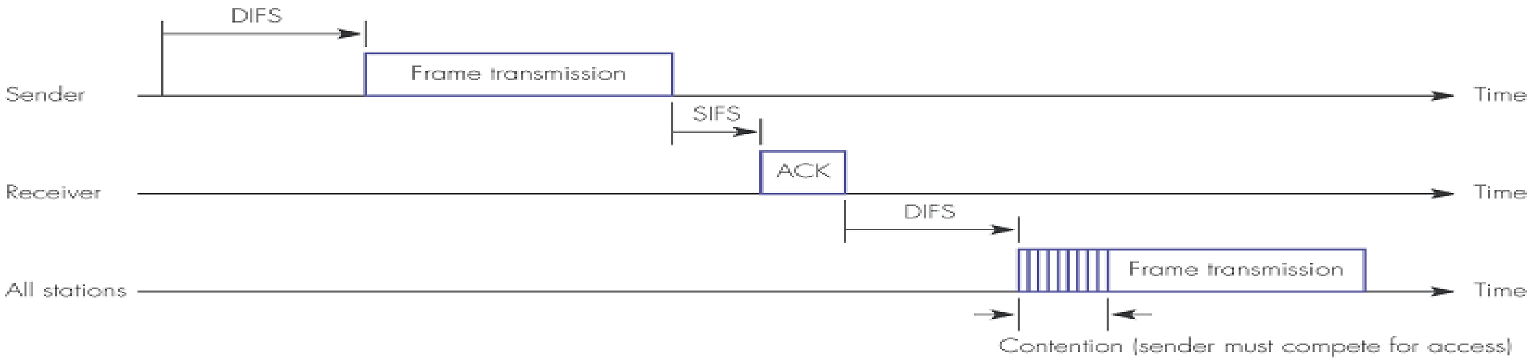
Sender

1. If sense channel idle (CCA) for **DIFS** then
   - Transmit entire frame
2. If sense channel busy then
   - Initialize size of **CW** (contention window) to a small value (# of slot times)
   - Enter contention period
     - Initialize **random backoff timer** to CW
     - Sense channel
       - If idle, timer counts down
       - If busy, wait for DIFS before resuming counting down from current value
     - When timer expires
       - If channel idle, transmit immediately
       - If channel busy, double the size of CW and reset timer to CW
         - If CW reaches the limit, inform LLC of transmission failure

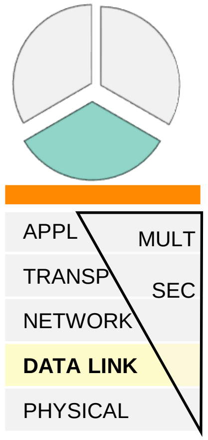
Receiver

If frame received OK

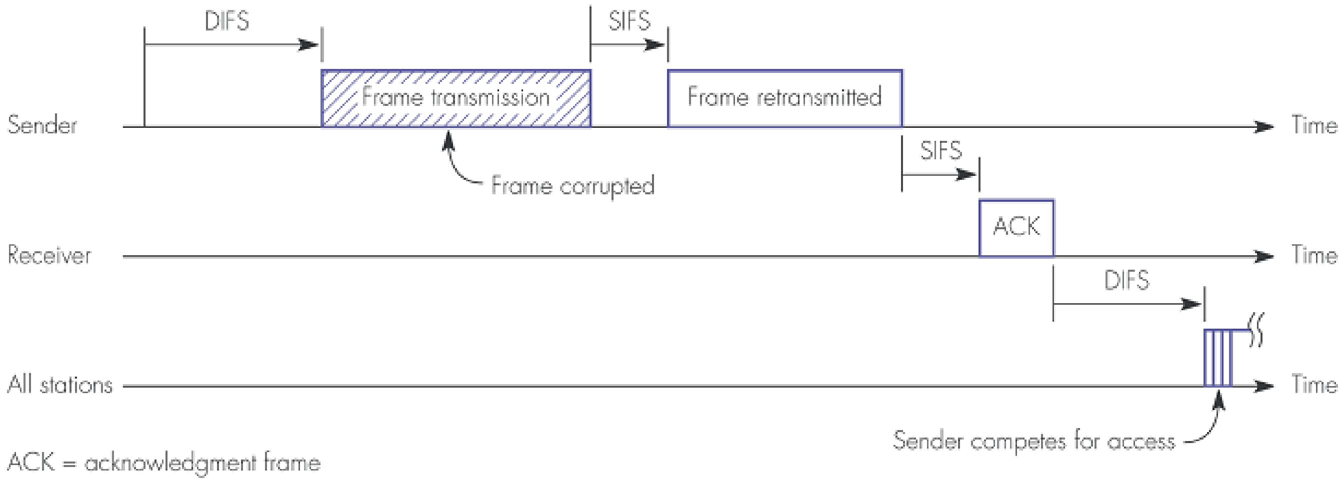
- Return ACK after **SIFS**
  - SIFS < DIFS, i.e. before other stations can seize the channel



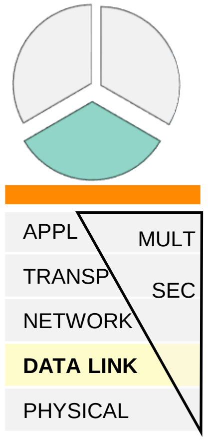
WLAN: MAC - DCF: Retransmission procedure



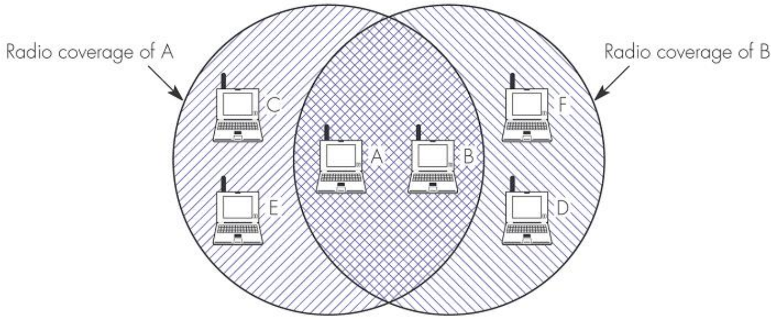
- Frame corrupted/lost:
  → No ACK from receiver
  → Sender detects the medium to be idle after SIFS
  → Sender immediately retransmits the frame
  - SIFS < DIFS, hence retransmit before other stations can seize the channel

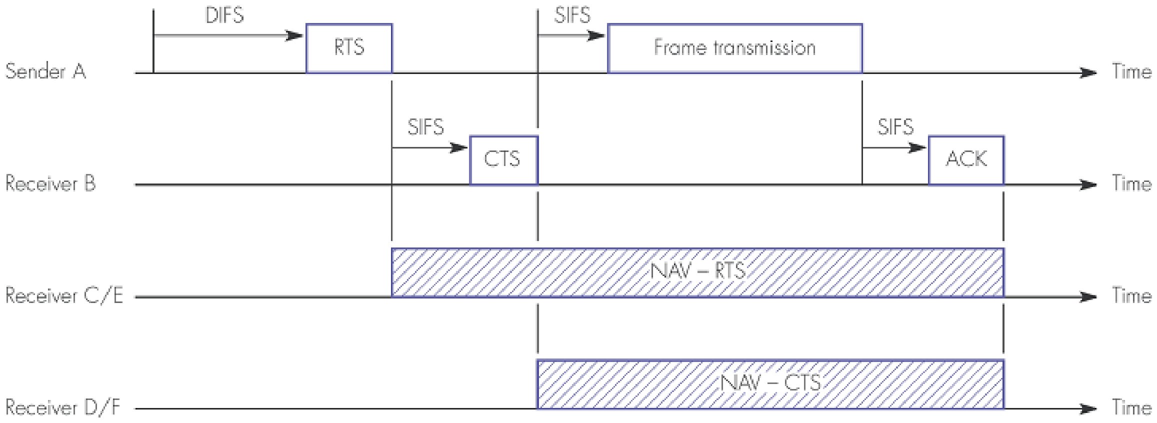


WLAN: MAC - DCF: RTS/CTS extension (optional)

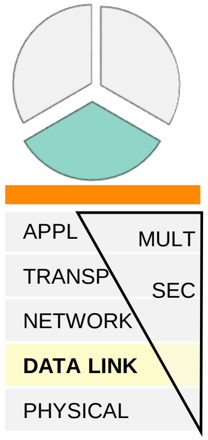


- Motivation: overcome hidden station problem by allowing a sender to “reserve” a channel to communicate with a particular receiver (try to avoid collisions altogether)
- Sender sends RTS (request-to-send) control frame
  - Contains ID of the receiver
  - NAV (network allocation vector) denotes the duration of the transmission (“virtual collision”)
- Receiver broadcasts CTS (clear-to-send) control frame
  - Heard by all stations, which defer transmitting for duration of NAV





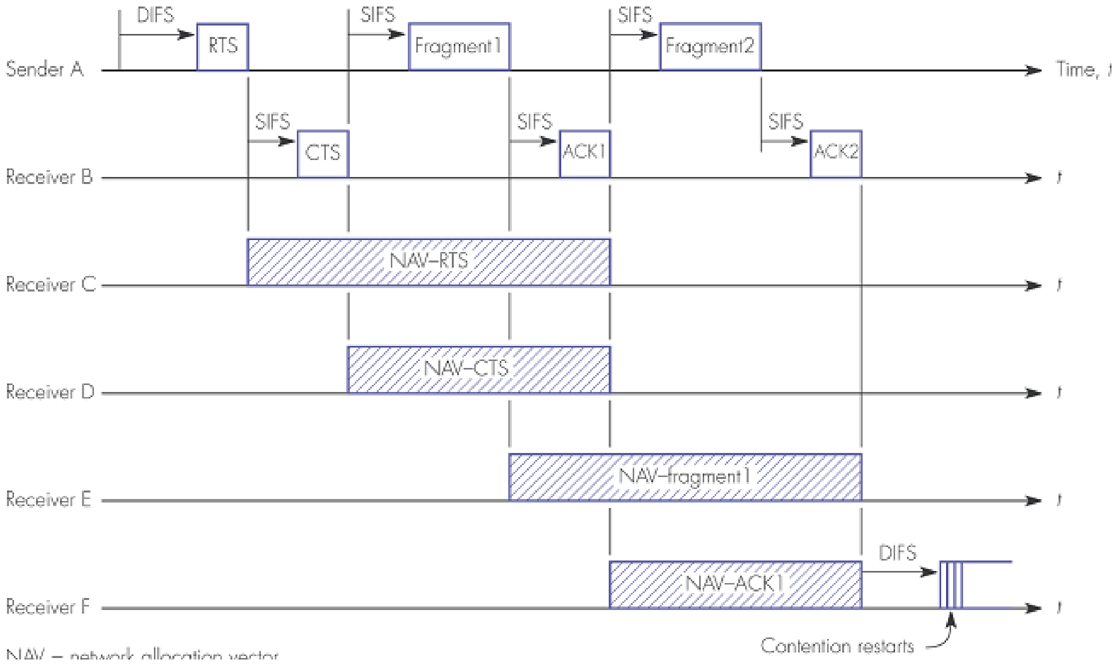
WLAN: MAC - DCF: Frame fragmentation



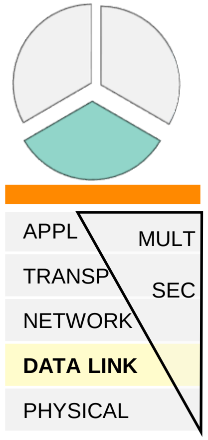
– **Wireless links are vulnerable to noise and interference**
  - High bit error rates in comparison to wired links

  → Long frames have low probability of being transmitted correctly

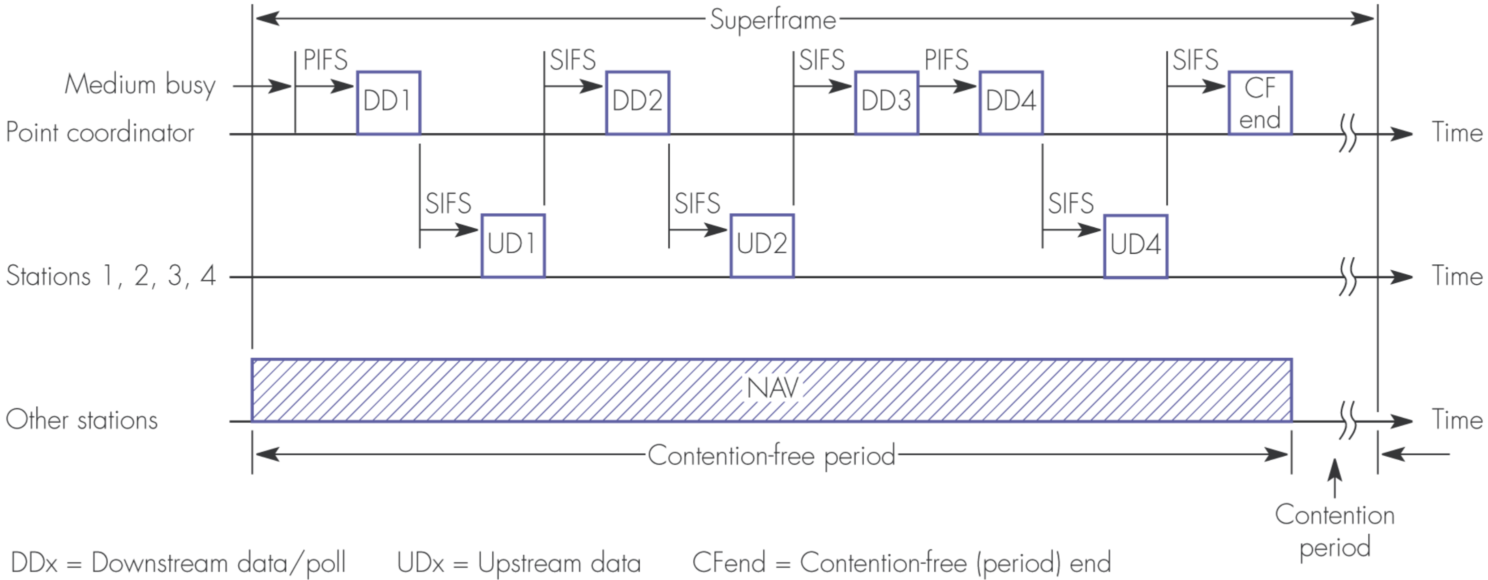
– **Solution: fragment frames**
  - Each fragment has a sequence number and checksum
  - Fragments are sent using idle RQ (stop-and-wait) protocol
  - Multiple frames are sent in a fragment burst



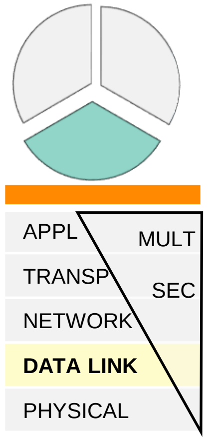
WLAN: MAC - PCF



- Optional time-bounded service for infrastructure mode
- AP controls access to the shared radio medium using a subsystem called point coordinator, which
  - Broadcasts at periodic intervals (range 1-65535 ms, typically 100 ms) a beacon frame (incl. control parameters), polling stations for data to send
  - Presents stations with a challenge frame containing a secret key, for a station to authenticate itself for polling service
  - Divides overall access times into contention free periods called superframes
  - Example with four stations authenticated for poll service



WLAN: 802.11 frame structure (1)

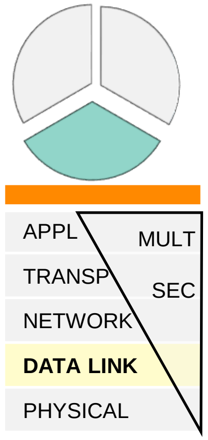


Bytes	2	2	6	6	6	2	6	0 - 2312	4
	frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Address 4: used only when sending frames between two APs/cells

For use of the addresses, see also
https://dalewifisec.wordpress.com/2014/05/17/the-to-ds-and-from-ds-fields

WLAN: 802.11 frame structure (2)



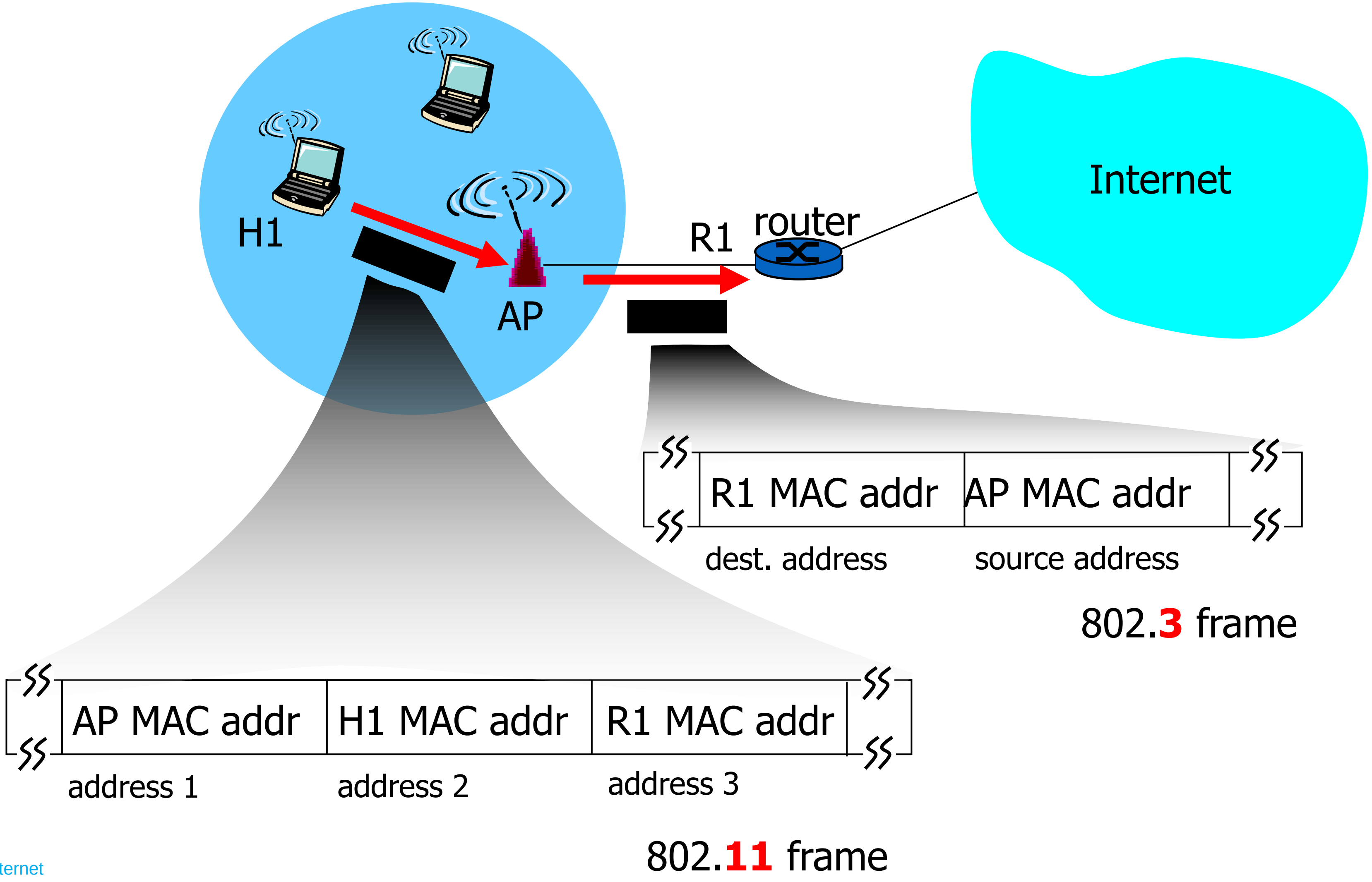
Address fields and their usage:

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Notes
0	0	DA Address of the wireless station/device receiving the frame	SA Address of the wireless station/device sending the frame	BSSID The BSSID of the cell	—	Ad-hoc and single-cell infrastructure LANs
0	1	DA Address of the receiving station within the BSSID	BSSID BSSID/AP address of the cell receiving the frame from the DS	SA Address of the mobile/static station sending the frame	—	Frame sent via the DS to the AP within the cell identified by the BSSID
1	0	BSSID Address of destination BSSID/AP attached to the DS	SA Address of the wireless station sending the frame	DA Address of the wireless station receiving the frame	—	Frame sent via the DS to an AP within a different cell identified by the BSSID
1	1	RA Address of the receiving AP within the DS	TA Address of the transmitting AP within the DS	DA Address of the wireless station receiving the frame	SA Address of the wireless station sending the frame	For frames sent between two APs/cells over the DS

DA = destination address SA = source address BSSID = basic service set identifier
RA = receiver AP address TA = transmitter AP address DS = distribution system

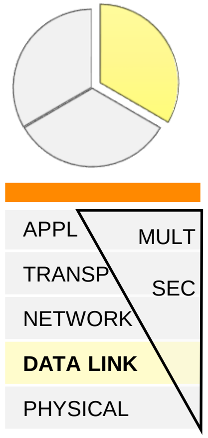
WLAN: 802.11 frame structure (3)

Address fields and their usage: example

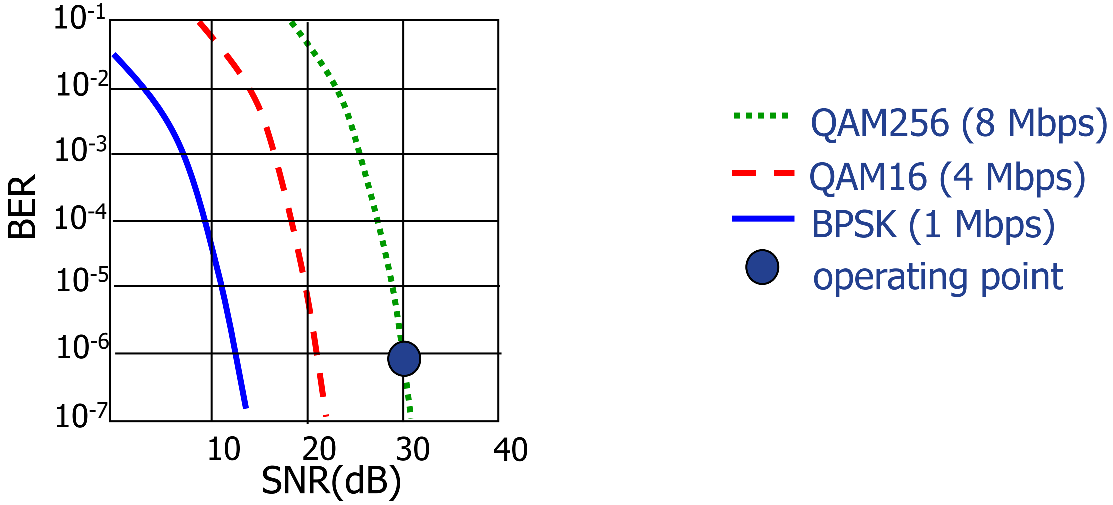


Wireless LAN (WLAN): Performance, power management mobility, security, QoS

WLAN: Rate adaptation



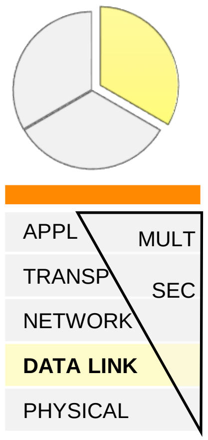
AP and mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies



1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

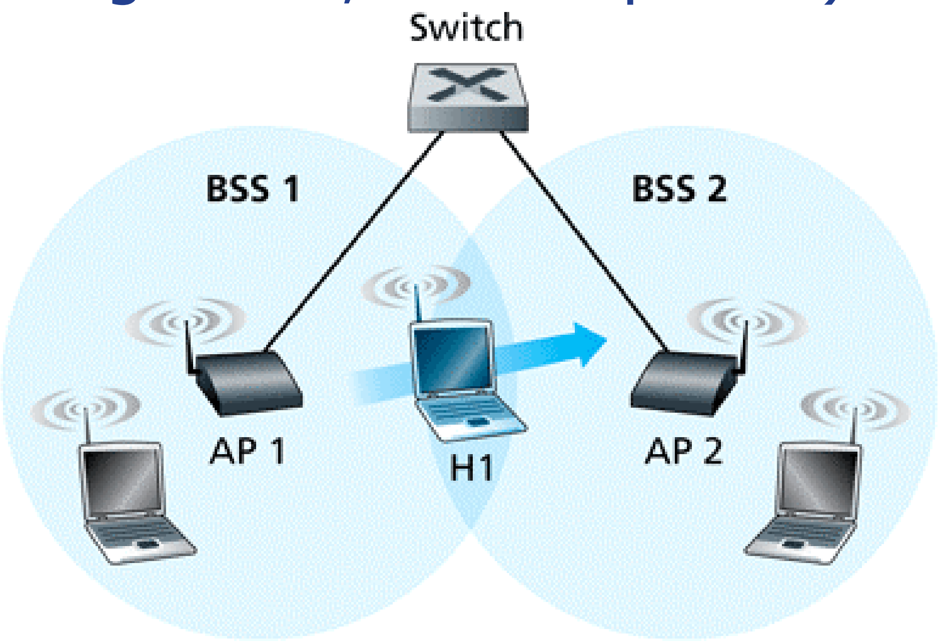
WLAN: Power management



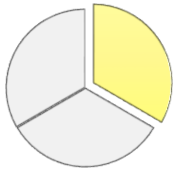
- Node is able to alternate between sleep and wakeup states
- Node-to-AP: “I am going to sleep until next beacon frame”
  - Power-management bit in 802.11 frame header set to 1
  - AP knows not to transmit frames to this node but buffers them
  - Node wakes up before next beacon frame using timer
- Beacon frame contains list of mobiles with AP-to-mobile frames waiting to be sent
  - Node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame
- Considerable energy savings
  - Beacon frames typically every 100 ms while wakeup time is 250 µs
  - Node without frames to send/receive can sleep ~99% of time

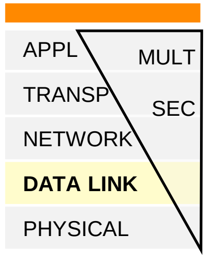
WLAN: Mobility within same subnet (1)

- H1 remains in same IP subnet → IP address can remain same
- Switch: which AP is associated with H1?
  - Self-learning (lecture #04): switch will see frame from H1 and “remember” which switch port can be used to reach H1
- Host’s decision to roam from current AP to new AP can be triggered by (depends on host configuration, vendor specific!)
  - Drop in signal strength
  - Loss of beacons
  - Data retry count (several non-acknowledged frames)
  - Drop in data rate



WLAN: Mobility within same subnet (2)

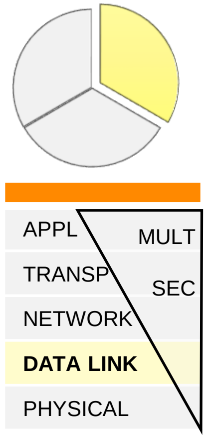




- **Two alternatives for finding the new AP to roam to**
  - **Pre-emptive discovery: host scans constantly for alternate APs**
    - Takes up most resources
    - During scanning host can not communicate with the ’current’ AP, as radio is reserved for scanning other channels !
  - **Reactive discovery: host starts scanning at roam time**
    - Does not affect normal transmission/reception
    - Provides up-to-date information of the available APs
    - May lead to higher latency than pre-emptive discovery
    - Most implementations use this

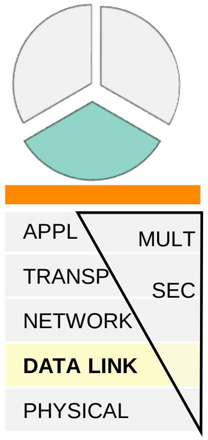
- **Decision on which AP to roam to can be based on different things (again, vendor specific!)**
  - **Signal strength**
  - **Transmitter load**
  - **Number of clients**

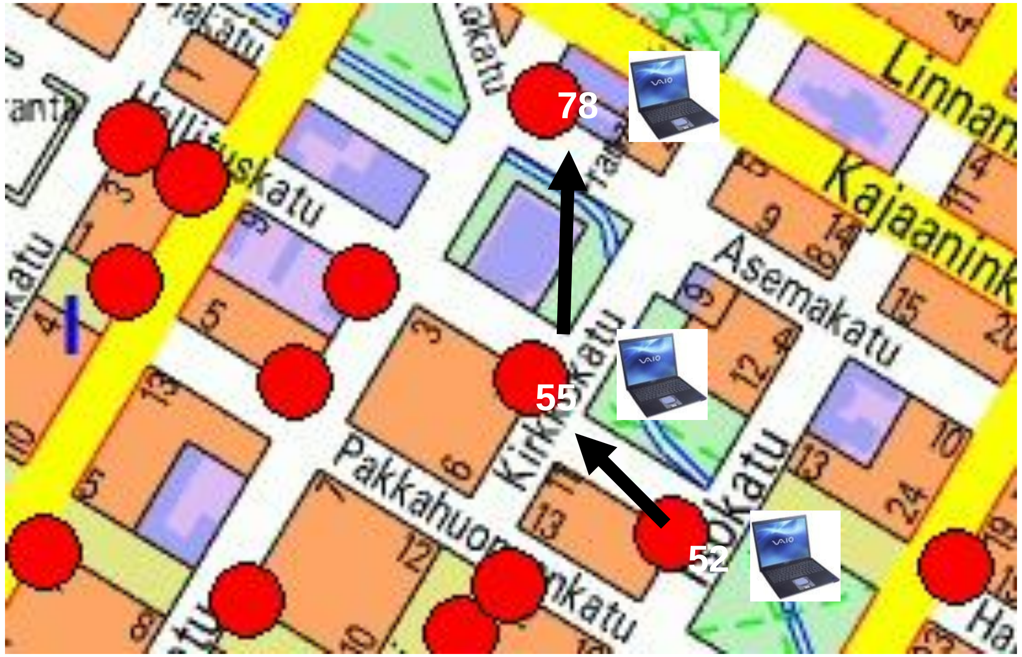
WLAN: Mobility within same subnet (3)



- Roaming involves
  - Finding the new AP to roam to and deciding when to roam
  - Associating with the new AP
  - Carry out authentication (depending on the security policies involved)
  - Inform the network about roaming (AP to AP communication, not included in the original 802.11 specification)
- Roaming can be slow
  - L2 handover takes typically only few tens of ms
  - But at application layer roaming can take several seconds !
    - Can cause glitches in real-time interactive services (e.g. VoIP)
  - Example from a host roaming in panOULU network (in 2008)
    - Host is configured to send 160 byte UDP packets at 20 ms intervals (typical for VoIP) to a server logging their arrival
    - Host machine Lenovo T60S with Ubuntu OS
    - Host roams between two Cisco 1200 series APs
    - Min host ”offline” time 2.8 s (141 packets lost)
    - Max host ”offline” time 5.1 s (252 packets lost)

WLAN: Mobility within same subnet (4)





Station roaming in panOULU WLAN at downtown Oulu at 3:55am in the morning

Feb 27 05:55:07 ap55.panoulu.local. 294: Feb 27 03:55:06.680: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 0002.2d1f.e8a7 Reassociated KEY_MGMT[NONE]

Feb 27 05:55:07 ap52.panoulu.local. 2833: Feb 27 03:55:06.701: %DOT11-6-ROAMED: Station 0002.2d1f.e8a7 Roamed to 0007.50d6.4c34

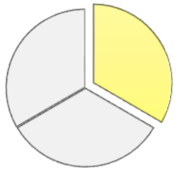
Feb 27 05:55:07 ap52.panoulu.local. 2834: Feb 27 03:55:06.701: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 0002.2d1f.e8a7 Reason: Disassociated because sending station is leaving (or has left) BSS

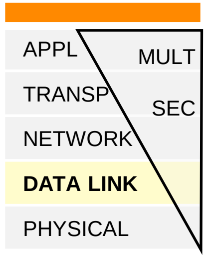
Feb 27 05:55:43 ap78.panoulu.local. 226: Feb 27 03:55:42.349: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 0002.2d1f.e8a7 Reassociated KEY_MGMT[NONE]

Feb 27 05:55:43 ap55.panoulu.local. 295: Feb 27 03:55:42.369: %DOT11-6-ROAMED: Station 0002.2d1f.e8a7 Roamed to 000d.29f0.a63a

Feb 27 05:55:43 ap55.panoulu.local. 296: Feb 27 03:55:42.369: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 0002.2d1f.e8a7 Reason: Disassociated because sending station is leaving (or has left) BSS

WLAN: Roaming challenges

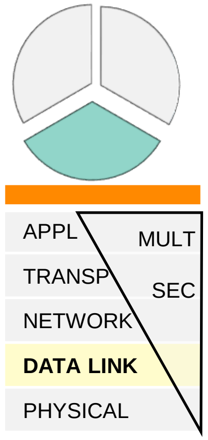




- **Roaming problems in legacy 802.11 specifications**
  - **Roaming is too slow for applications such as VoIP**
  - **Roaming client cannot know if necessary QoS resources are available at a new AP until after a transition**

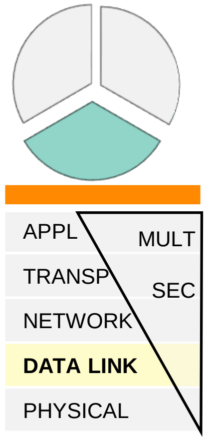
- **Standardization efforts to improve 802.11 roaming**
  - **IEEE 802.11f (IAPP, Inter-Access Point Protocol)**
    - Trial standard published in 2003, withdrawn in 2006
  - **IEEE 802.11r (”Fast BSS transitions”)**
    - Client can use the current AP as a conduit to other access points
    - Allow client to establish a security and QoS state at a new access point before making a transition
    - Published in 2008

WLAN: Throughput estimation (1)



- Based on TCP transaction of 1460 byte payload & ACK
  - TCP/IP headers add 40 bytes, 802.11 MAC header adds 28 bytes and 802 LLC header adds 8 bytes →TCP data frame is 1536 bytes, ACK frame is 76 bytes
- Frame exchange sequence
  - TCP data: DIFS → 802.11 data (TCP data) → SIFS → 802.11 ACK
  - TCP ACK: DIFS → 802.11 data (TCP ACK) → SIFS → 802.11 ACK
- Assumptions
  - No contention for the medium, no collisions
  - No simultaneous transmissions by upper layer protocols
  - Each TCP data segment is acknowledged by recipient
  - Hence, obtained estimates are optimistic

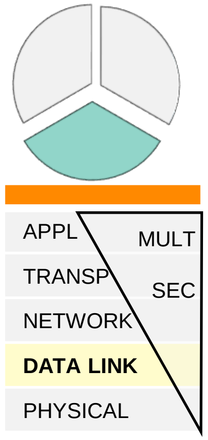
WLAN: Throughput estimation (2)



- 802.11b (nominal 11 Mbps data rate)
  - Symbol size: 8 bits/symbol
    → TCP data frame is 1536 symbols, TCP ACK frame is 76 symbols
  - Symbol rate: 1.375 M symbols/s
  - Assume long preamble (default): 192 µs

	TCP data	TCP ACK
DIFS	50 µs	50 µs
802.11 data	192 µs + 1536/1.375 Msps = 192 µs + 1118 µs = 1310 µs	192 µs + 76/1.375 Msps = 192 µs + 56 µs = 248 µs
SIFS	10 µs	10 µs
802.11 ACK	192 µs + 14/1.375 Msps = 192 µs + 11 µs = 203 µs	203 µs
Frame exchange total	1573 µs	511 µs
Transaction total	1573 µs + 511 µs = 2084 µs	
Throughput	1460 x 8 bits / 2084 µs = **5.6 Mbps**	

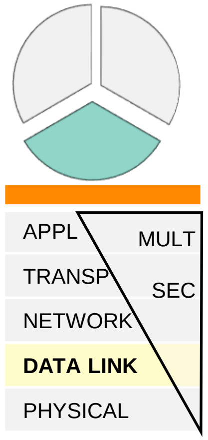
WLAN: Throughput estimation (3)



- 802.11a (nominal 54 Mbps data rate)
  - Adds 6-bit tail → TCP data frame is 12296 (1536x8+6) bits, TCP ACK frame is 614 (76x8+6) bits
  - Symbol size is 216 bits → TCP data frame is 57 symbols, TCP ACK frame is 3 symbols
  - Symbol time: 4.0 µs
  - Preamble: 20 µs

	TCP data	TCP ACK
DIFS	34 µs	34 µs
802.11 data	20 µs + 57x4 µs = 20 µs + 228 µs = 248 µs	20 µs + 3x4 µs = 20 + 12 µs = 32 µs
SIFS	16 µs	16 µs
802.11 ACK	20 µs + 1x4 µs = 20 µs + 4 µs = 24 µs	24 µs
Frame exchange total	322 µs	106 µs
Transaction total	322 µs + 106 µs = 428 µs	
Throughput	1460 x 8 bits / 428 µs = **27.3 Mbps**	

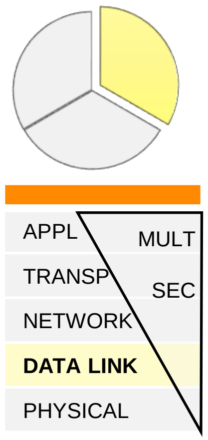
WLAN: Security & QoS



- **Security**
  - **WEP → WPA → WPA2**
  - **Discussed in security lecture**
- **QoS**
  - **IEEE 802.11e: QoS enhancements**
    - Wi-Fi certification: WMM (Wi-Fi Multimedia)
      - Typically implementes subset of 802.11e specification
  - **Discussed in Multimedia and QoS lecture**

Wireless LAN (WLAN): Standards

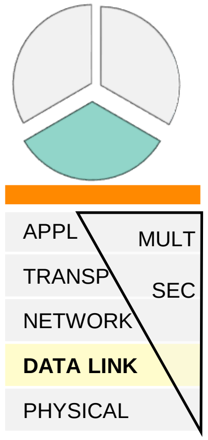
IEEE 802.11: Why new standards are needed?



- **802.11 is most popular and successful WLAN technology**
  - **Success factors: maturity, interoperability, low unit price, license free spectrum, ...**
  - **Billion $ business with >10% annual growth**
    - But most of the revenue comes from consumer market
  - **Example WLAN products certified by Wi-Fi alliance (Feb 24, 2015)**
    - 2538 AP's for consumer market (home and small office)
    - 1718 AP's for enterprise market
    - 1225 mobile AP's (battery powered)
    - 643 laptop computers
    - 930 multi-mode (WiFi+cellular) phones
    - 3764 multi-mode (WiFi+cellular) smartphones
    - 90 projectors

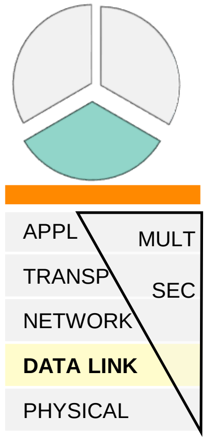
- **Legacy standards dated back to 1999 (802.11a) and 2003 (802.11g) – their shortcomings have been exposed over the years**

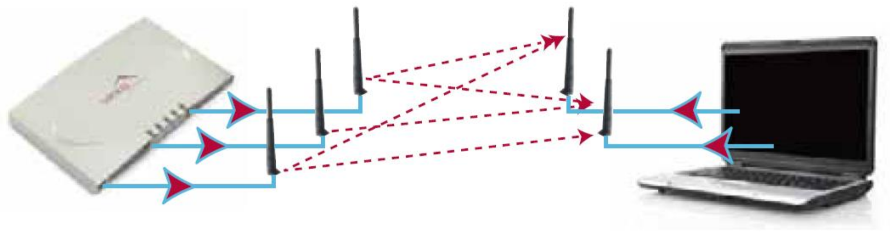
IEEE 802.11n: In brief



- Standard published in Oct 2009 (standardization took ~7 years)
- Targeted to update technology and to conquer large-scale enterprise market
- Key improvements over legacy systems (802.11a/g)
  - Physical layer
    - MIMO (multiple antennas) (legacy systems ”SISO”) → higher data rates
    - Channel bonding for 40 MHz channels (legacy systems have 20 MHz channels) → doubles data rates (but reduces number of available channels)
    - Improved modulation and coding → higher data rates
  - Link layer: improved MAC protocol
    - Block acknowledgement (confirm receipt of multiple unicast blocks) → reduces number of ACK frames i.e. overhead
    - Frame aggregation (larger payloads) → reduces overhead
    - Reduced Interframe Spacing (RIFS, 2 µs) (legacy systems 10/16 µs) → reduces idle time
- Nominal maximum physical layer data rates
  - Per stream: 150 Mbps
  - Number of streams: 4
  - Aggregate capacity: 600 Mbps

IEEE 802.11n: MIMO

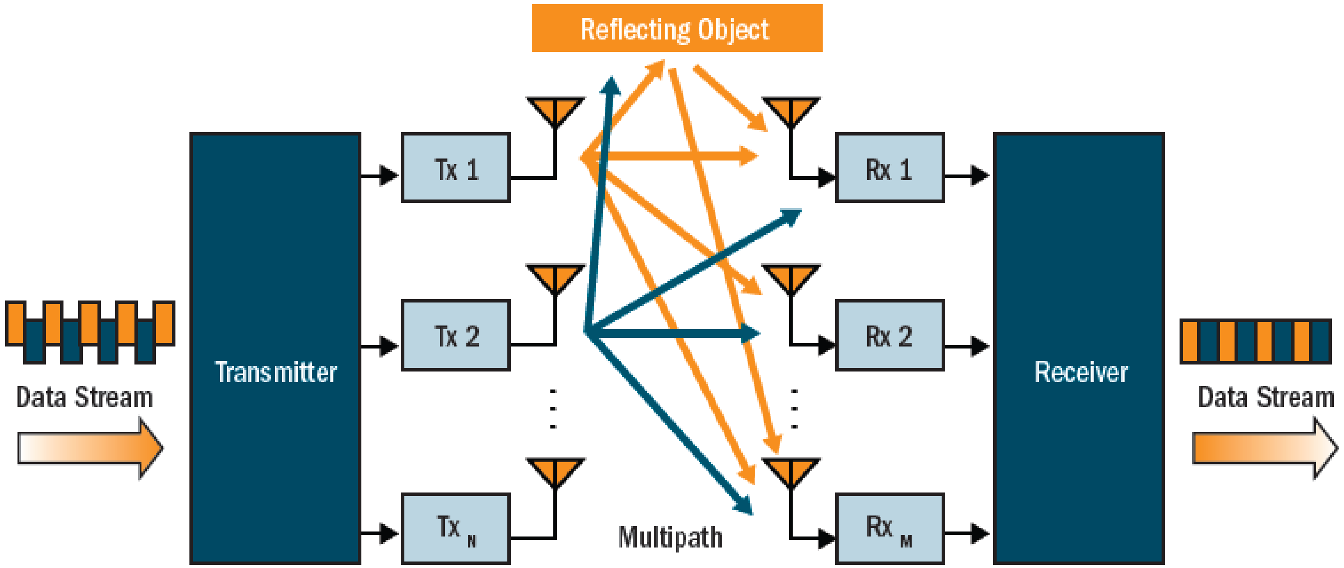




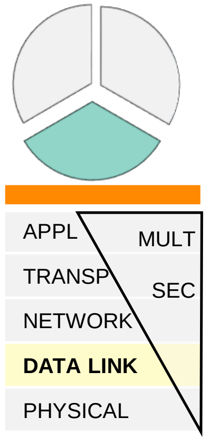
- Multiple Input Multiple Output
  - Sender & receiver have multiple radios with spatially displaced antennas
  - Tx-Rx pairs see multiple signal paths with different characteristics
  - Aggregate signal at receiver has higher SNR → higher data rates

- Spatial Division Multiplexing (SDM) to multiply data rate
  - Multiple (2-4) source data streams are multiplexed
  - Multiplexed data stream is divided and sent simultaneously over different transmit antennas on the same RF channel

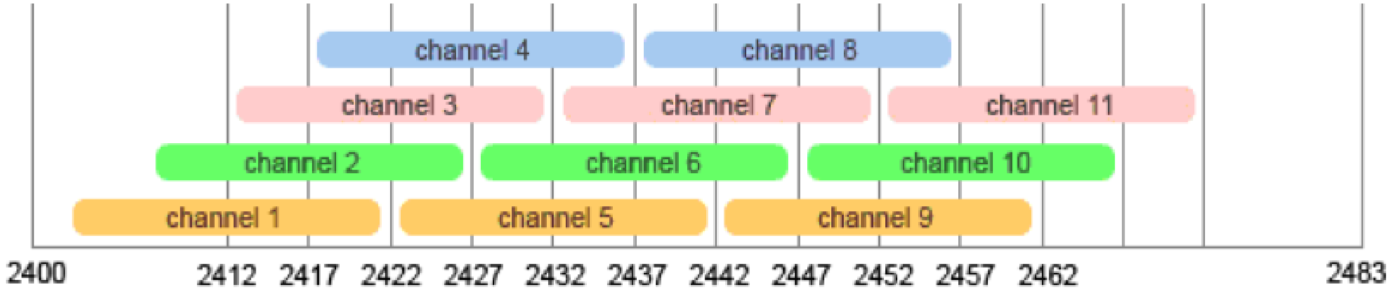
- MIMO attributes: TxR:S
  - T: # of transmitter radios
  - R: # of receiver radios
  - S: # of streams
  - 802.11n AP
    - Max: 4x4:4
    - Typical: 2x2:2



IEEE 802.11n: Channel bonding



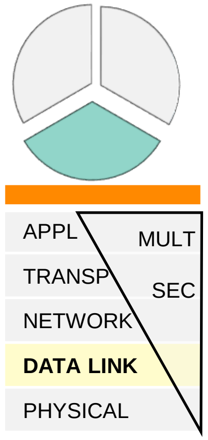
- Two adjacent 20 MHz channels are combined into single 40 MHz channel
  - Doubles achievable data rate, but decreases number of available channels
- 2.4 GHz ISM band (legacy systems 802.11b/g)



  - Only 3 nonoverlapping 20 MHz channels (1, 6, 11)
    → only 1(!) 40 MHz channel which consumes 9(!) 20 MHz channels
    → 802.11n devices using 40 MHz channels have to listen to legacy devices
- 5 GHz UNII band (legacy system 802.11a)

  - 11 nonoverlapping 40 MHz channels
  - 5 GHz band has much less interference than 2.4 GHz band
  - Eventually, 802.11n will be used mostly on 5 GHz band

IEEE 802.11be: In brief



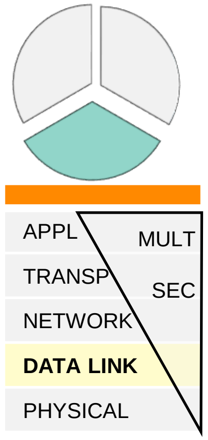
- Newest standard, published in 2020
- Extremely High Throughput (EHT)
- Details in: https://en.wikipedia.org/wiki/IEEE_802.11be :

Wi-Fi Generations

Generation	IEEE Standard	Maximum Linkrate (Mbit/s)	Adopted	Radio Frequency (GHz)[6]
Wi-Fi 7	**802.11be**	40000	TBA	2.4/5/6
Wi-Fi 6E	802.11ax	600 to 9608	2020	2.4/5/6
Wi-Fi 6			2019	2.4/5
Wi-Fi 5	802.11ac	433 to 6933	2014	5
Wi-Fi 4	802.11n	72 to 600	2008	2.4/5
(Wi-Fi 3*)	802.11g	6 to 54	2003	2.4
(Wi-Fi 2*)	802.11a	6 to 54	1999	5
(Wi-Fi 1*)	802.11b	1 to 11	1999	2.4
(Wi-Fi 0*)	802.11	1 to 2	1997	2.4

*: (Wi-Fi 0, 1, 2, 3, are unbranded common usage.[7][8])

IEEE 802.11: Comparison of standards



http://en.wikipedia.org/wiki/IEEE_802.11

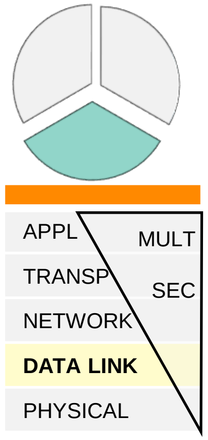
V·T·E IEEE 802.11 network PHY standards [hide]

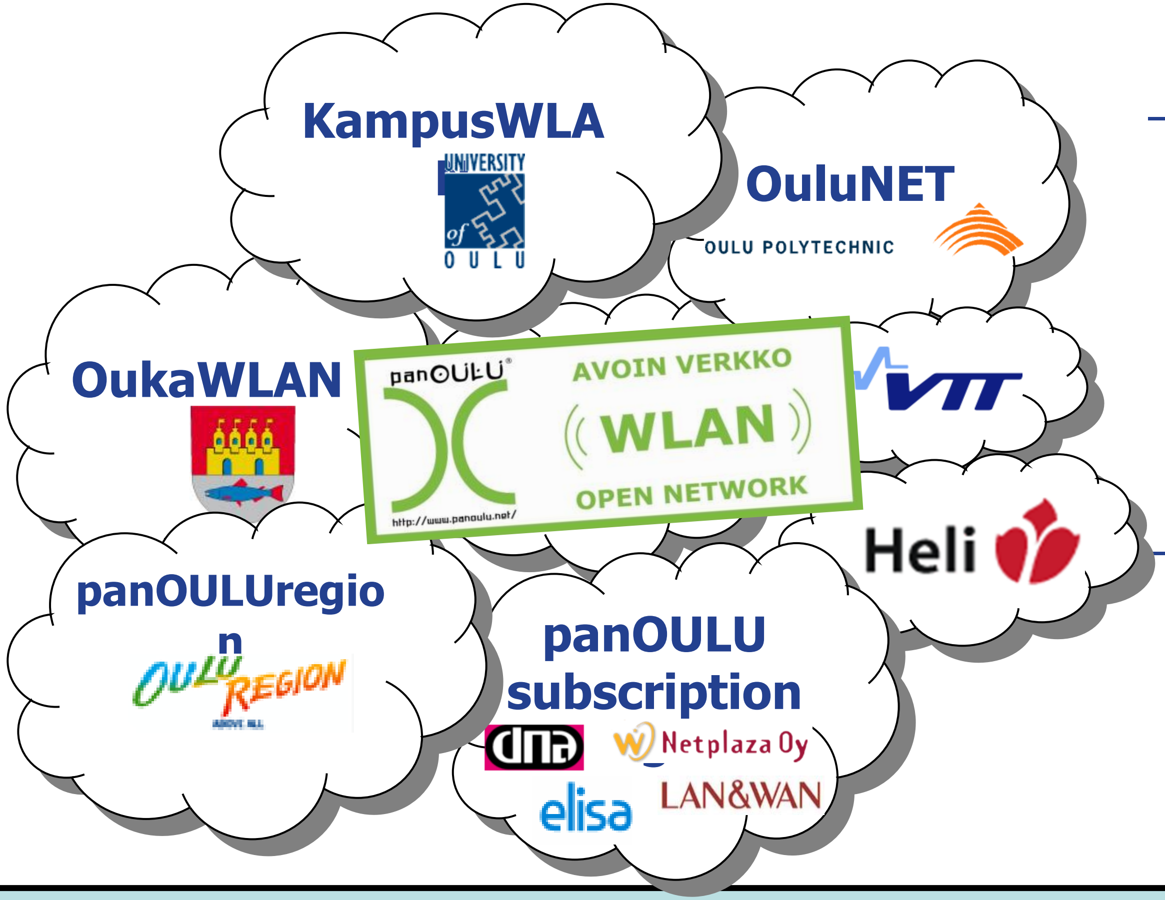
Frequency range, or type	PHY	Protocol	Release date[12]	Frequency (GHz)	Bandwidth (MHz)	Stream data rate[13] (Mbit/s)	Allowable MIMO streams	Modulation	Approximate range[citation needed] Indoor	Approximate range[citation needed] Outdoor
1–6 GHz	DSSS/FHSS[14]	802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
	HR-DSSS[14]	802.11b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
	OFDM	802.11a	Sep 1999	5	5/10/20	6, 9, 12, 18, 24, 36, 48, 54 (for 20 MHz bandwidth, divide by 2 and 4 for 10 and 5 MHz)	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		802.11j	Nov 2004	4.9/5.0[D][15][failed verification]					?	?
		802.11p	Jul 2010	5.9					?	1,000 m (3,300 ft)[16]
		802.11y	Nov 2008	3.7[A]					?	5,000 m (16,000 ft)[A]
	ERP-OFDM(, etc.)	802.11g	Jun 2003	2.4					38 m (125 ft)	140 m (460 ft)
	HT-OFDM[17]	802.11n	Oct 2009	2.4/5	20	Up to 288.8[B]	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft)[18][failed verification]
					40	Up to 600[B]				
	VHT-OFDM[17]	802.11ac	Dec 2013	5	20	Up to 346.8[B]	8	MIMO-OFDM	35 m (115 ft)[19]	?
					40	Up to 800[B]				
					80	Up to 1733.2[B]				
					160	Up to 3466.8[B]				
	HE-OFDM	802.11ax	September 2019 [20]	2.4/5/6	20	Up to 1147[F]	8	MIMO-OFDM	30 m (98 ft)	120 m (390 ft) [G]
					40	Up to 2294[F]				
					80	Up to 4803[F]				
					80+80	Up to 10530[F]				
mmWave	DMG[21]	802.11ad	Dec 2012	60	2,160	Up to 6,757[22] (6.7 Gbit/s)	N/A	OFDM, single carrier, low-power single carrier	3.3 m (11 ft)[23]	?
		802.11aj	Apr 2018	45/60[C]	540/1,080[24]	Up to 15,000[25] (15 Gbit/s)	4[26]	OFDM, single carrier[26]	?	?
	EDMG[27]	802.11ay	Est. May 2020	60	8000	Up to 20,000 (20 Gbit/s)[28]	4	OFDM, single carrier	10 m (33 ft)	100 m (328 ft)
Sub-1 GHz IoT	TVHT[29]	802.11af	Feb 2014	0.054–0.79	6–8	Up to 568.9[30]	4	MIMO-OFDM	?	?
	S1G[29]	802.11ah	Dec 2016	0.7/0.8/0.9	1–16	Up to 8.67 (@2 MHz)[31]	4		?	?
2.4 GHz, 5 GHz	WUR	802.11ba[E]	Est. Sep 2020	2.4/5	4.06	0.0625, 0.25 (62.5 kbit/s, 250 kbit/s)	N/A	OOK (Multi-carrier OOK)	?	?
Light (Li-Fi)	IR	802.11-1997	Jun 1997	?	?	1, 2	N/A	PPM	?	?
	?	802.11bb	Est. Jul 2021	60000-790000	?	?	N/A	?	?	?

Wireless LAN (WLAN): Example system

Example WLAN: panOULU

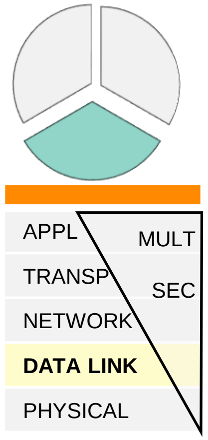
http://www.panoulu.net





- panOULU ~ Campus networks of municipalities and other public organisations + panOULU subscriptions sold by ISPs
  - Each provider is responsible for maintenance and expenses of its WLAN zone
  - Common core services are sponsored by City of Oulu and University of Oulu
- ~1400 IEEE 802.11 APs
  - Appear as one large uniform WLAN to users (SSID: panoulu)
  - Provide open (no authentication) and free (no payment) Internet access to the general public

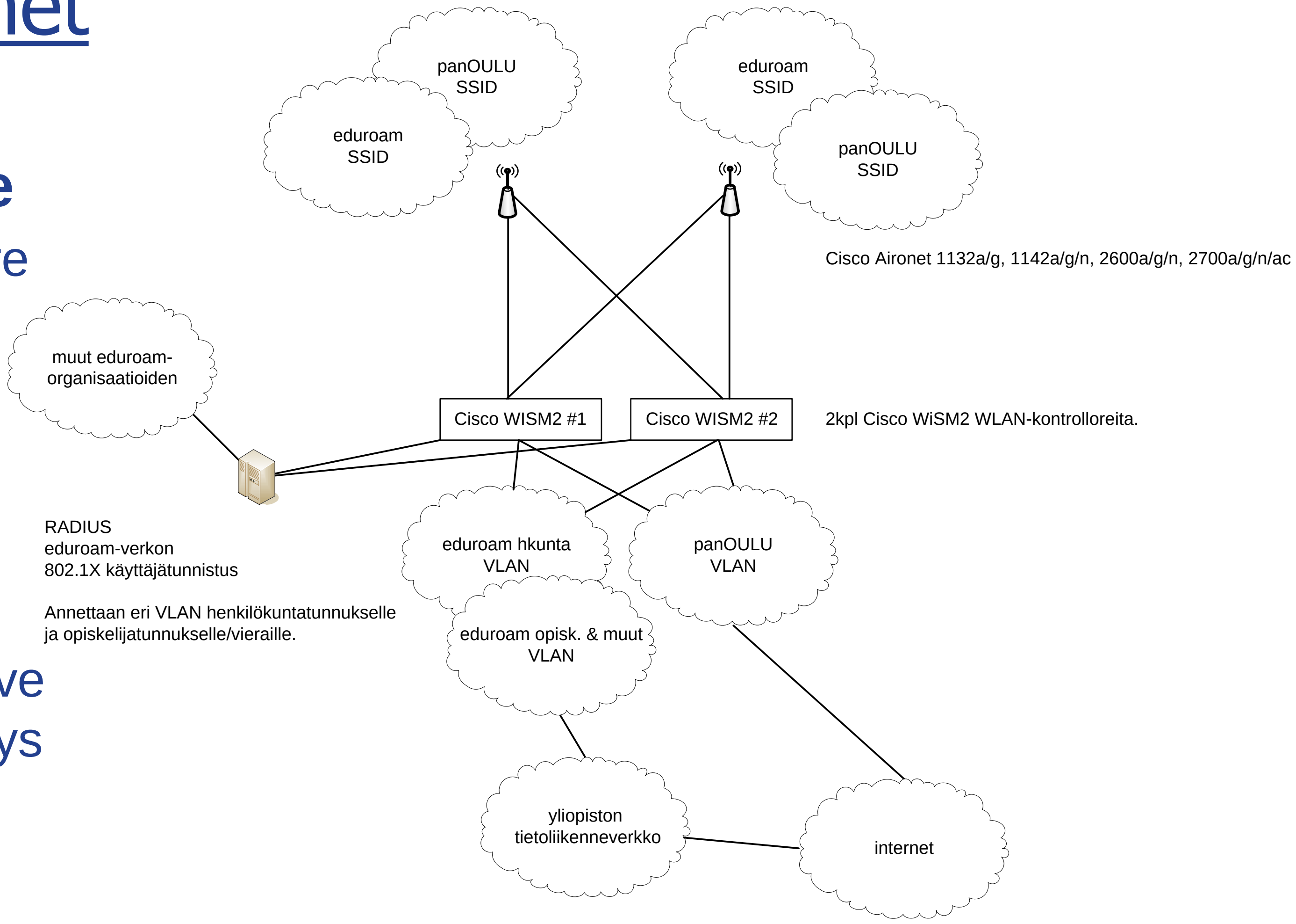
Ojala T, Orajärvi J, Puhakka K, Heikkinen I & Heikka J (2011) **panOULU: Triple helix driven municipal wireless network providing open and free Internet access.** Proc. C&T 2011, Brisbane, Australia, 118-127.



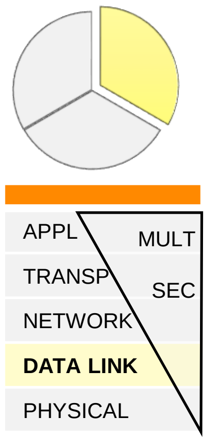
Example WLAN: panOULU

http://www.panoulu.net

- **One WLAN infrastructure**
  - Controller-based architecture
  - Covers several campuses
- **Two logical networks (SSID’s)**
  - **eduroam**: authentication
  - **panoulu**: no authentication
  - Traffic is routed via respective VLANs and internet gateways



Key points to remember



1. Basics of wireless networks
2. Basic concepts and functions of IEEE 802.11 WLAN
   - Architecture
   - Medium access control (DCF, CSMA/CA, RTS/CTS)
   - Technology evolution

Thank you!