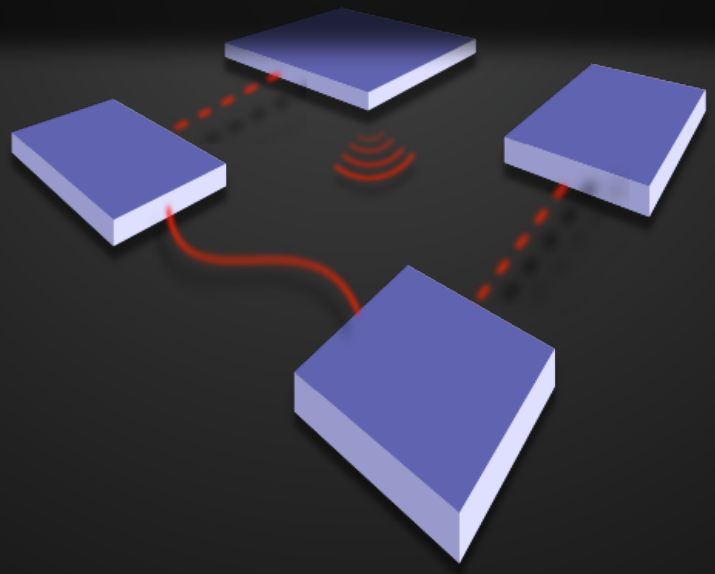
CS-435

spring semester 2025

Network Technology & Programming Laboratory

University of Crete
Computer Science Department

Stefanos Papadakis

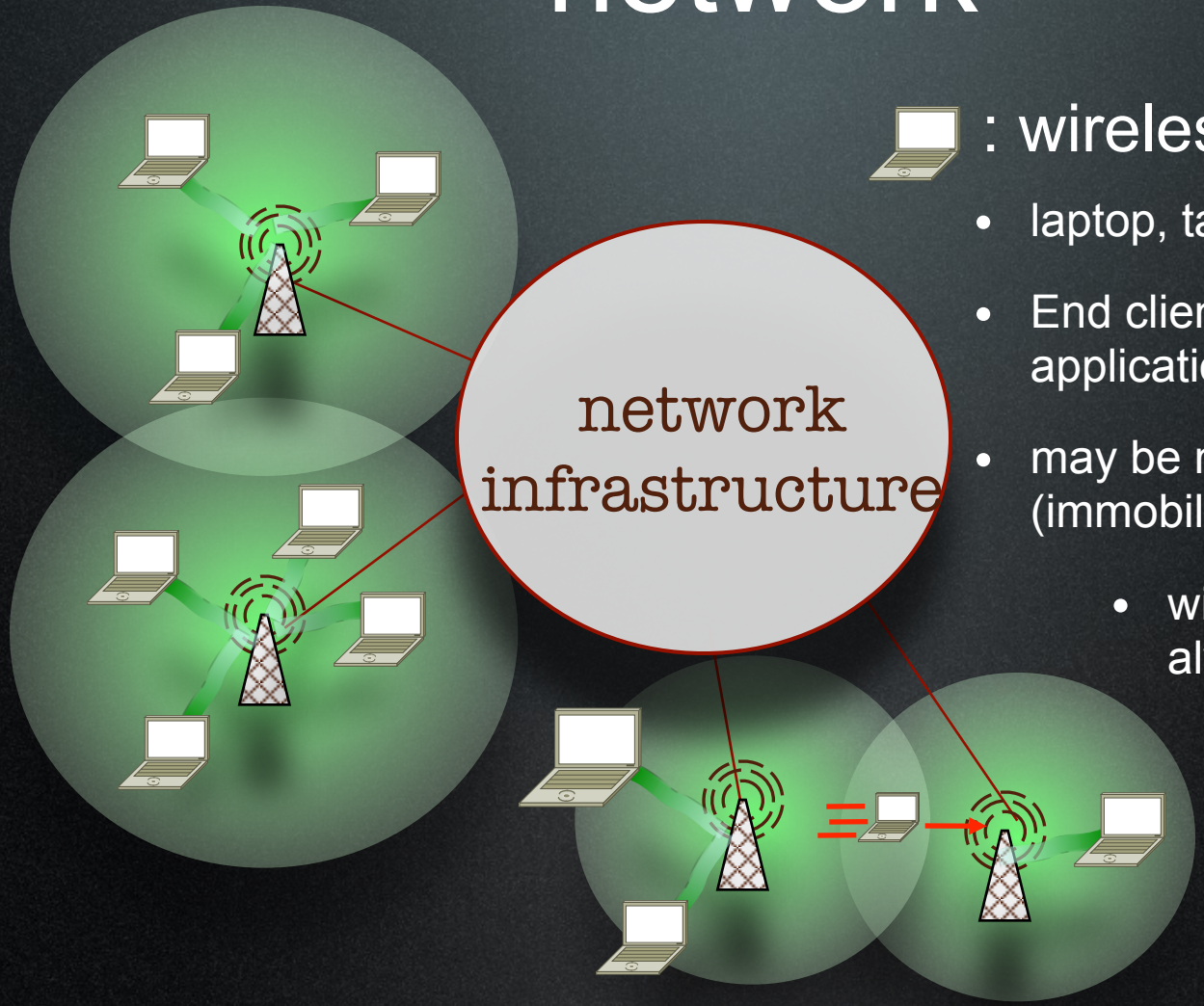


CS-435

Lecture #11 preview

- Wireless Networking
- IEEE 802.11

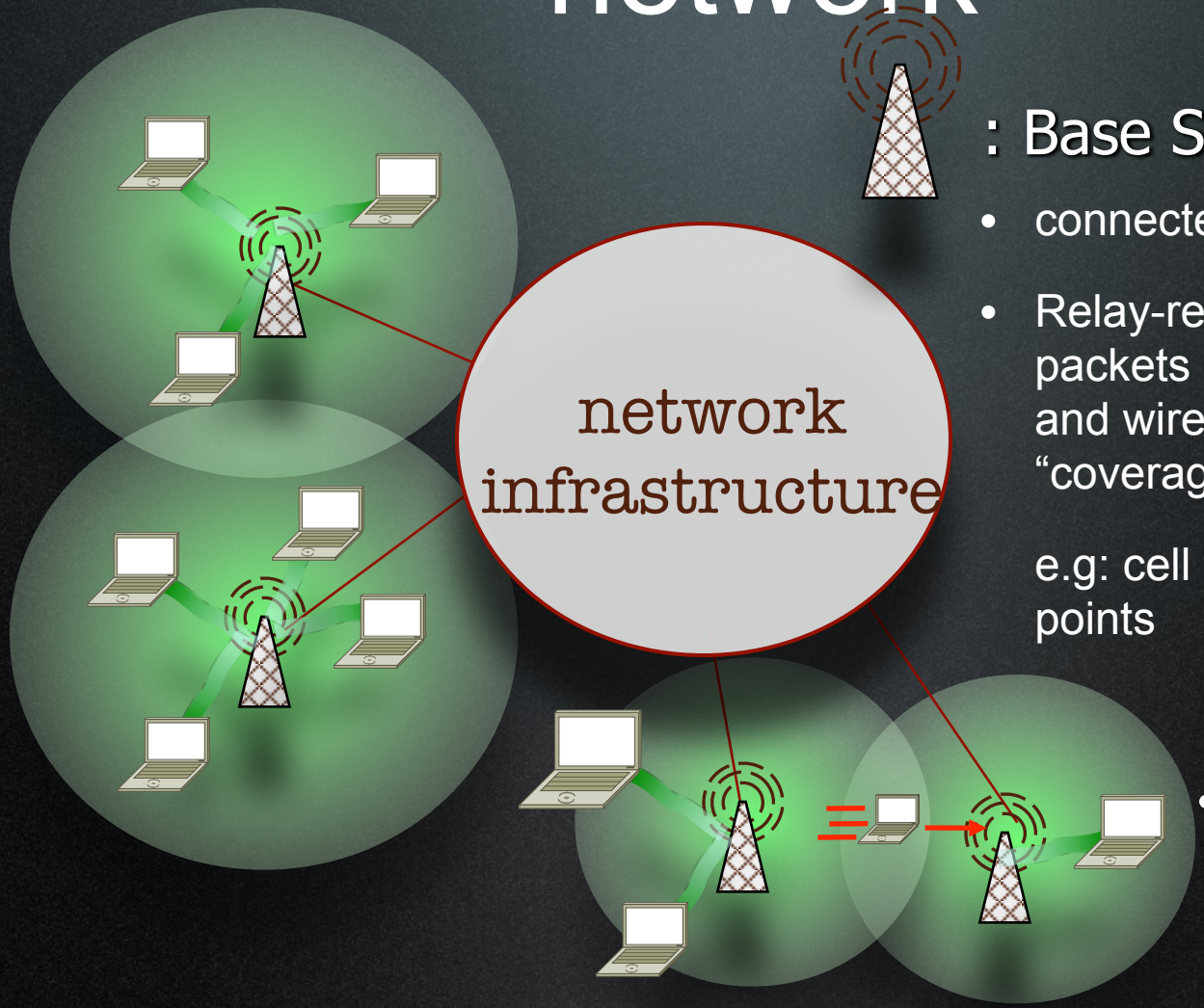
The Elements of a wireless network



: wireless hosts

- laptop, tablet, smart phone, etc
- End clients running applications
- may be mobile or fixed (immobile)
  - wireless does not always mean mobility

The Elements of a wireless network



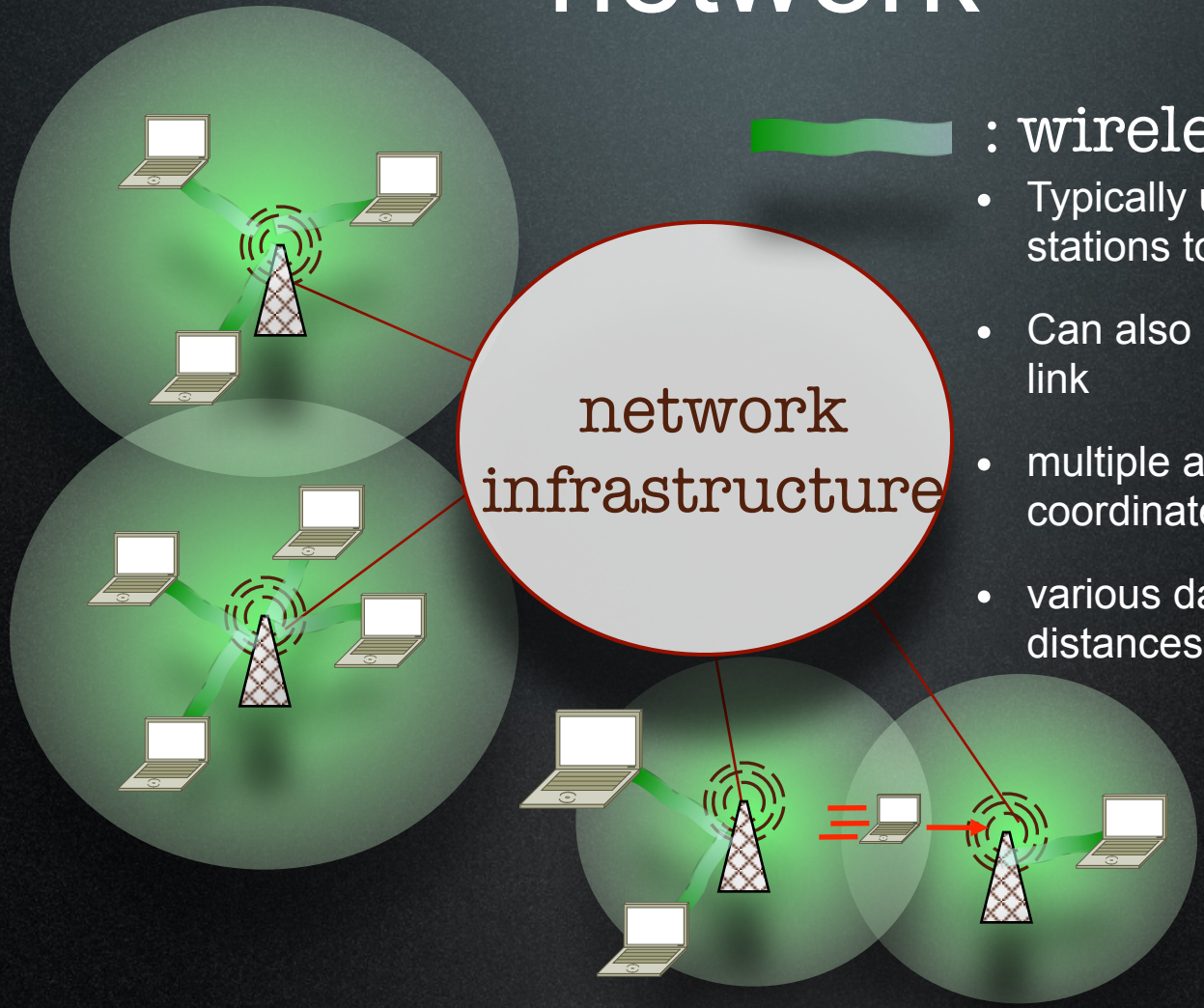
: Base Stations

- connected to wired network
- Relay-responsible for sending packets between wired network and wireless host(s) in its "coverage area"

  e.g: cell towers, 802.11 access points

- **handoff:** mobile changes base station providing connection into wired network

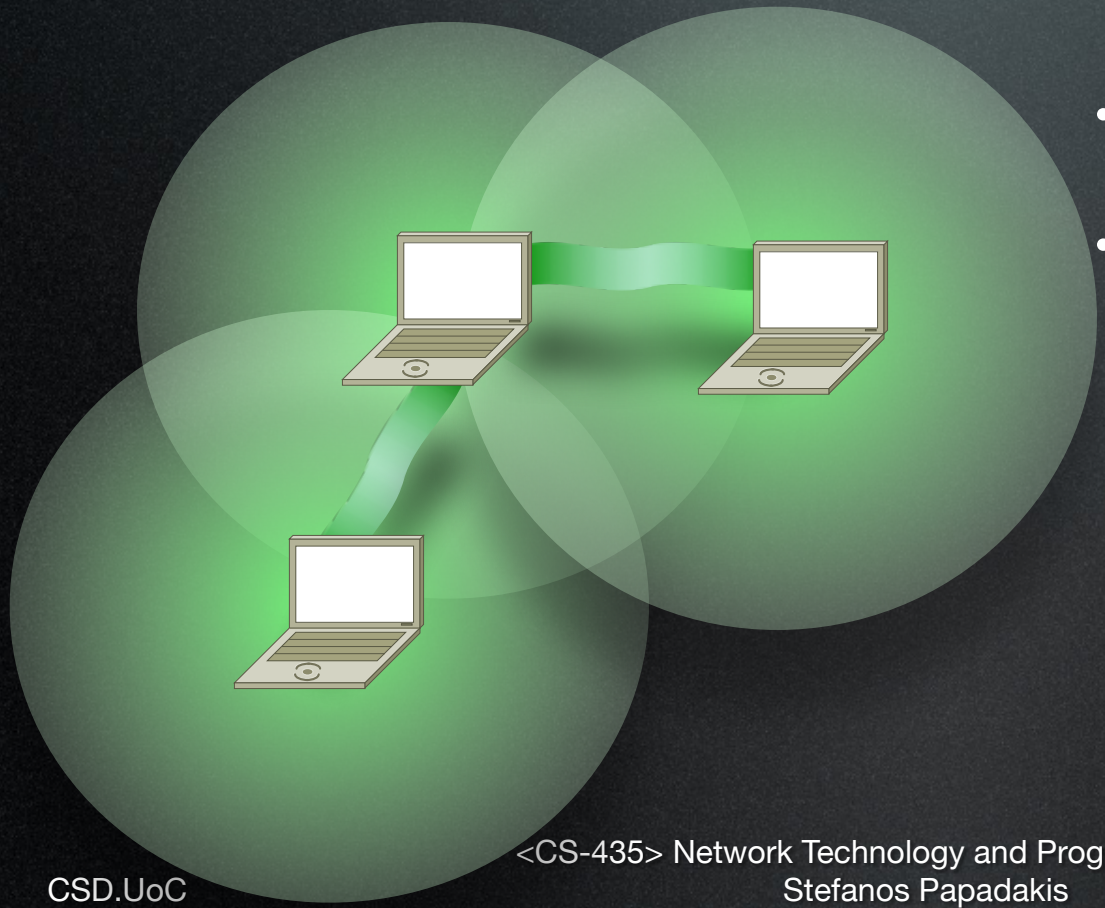
The Elements of a wireless network



: wireless link

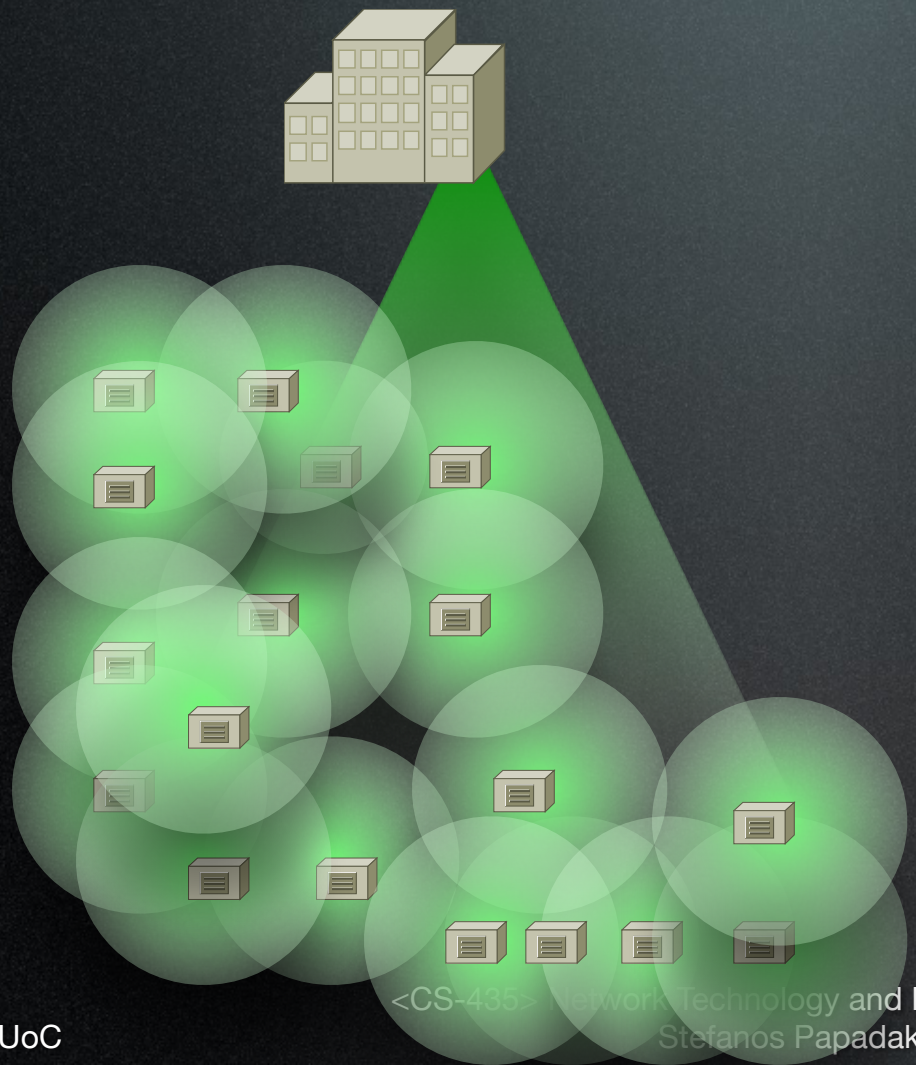
- Typically used to connect end stations to base station
- Can also be used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distances

The Infrastructure-less Wireless paradigm: Wireless Ad Hoc Networking



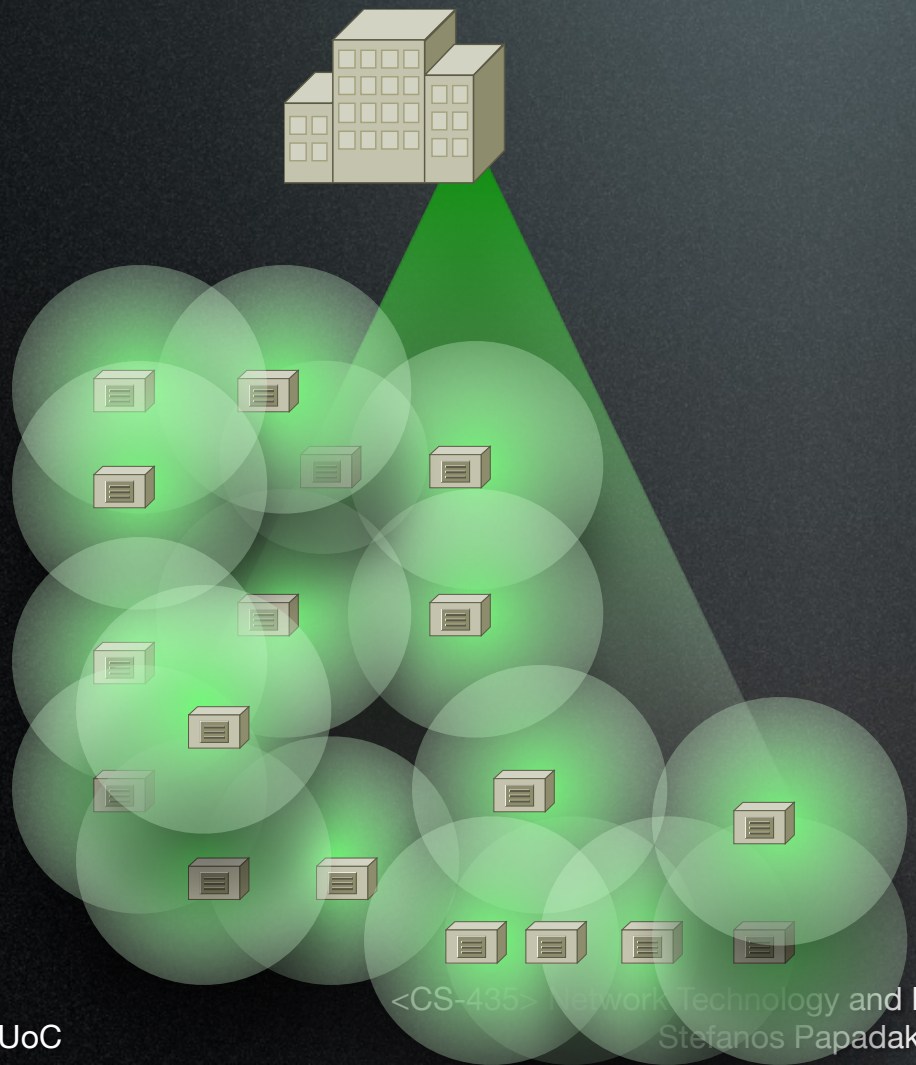
- Requires no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves
- Is typically a
  - Special purpose
  - Short lived
  - Heavily constrained w.r.t.:
    - Battery resources
    - Radio Resources
    - Computational/storage abilities

A special Case: Sensor Networks



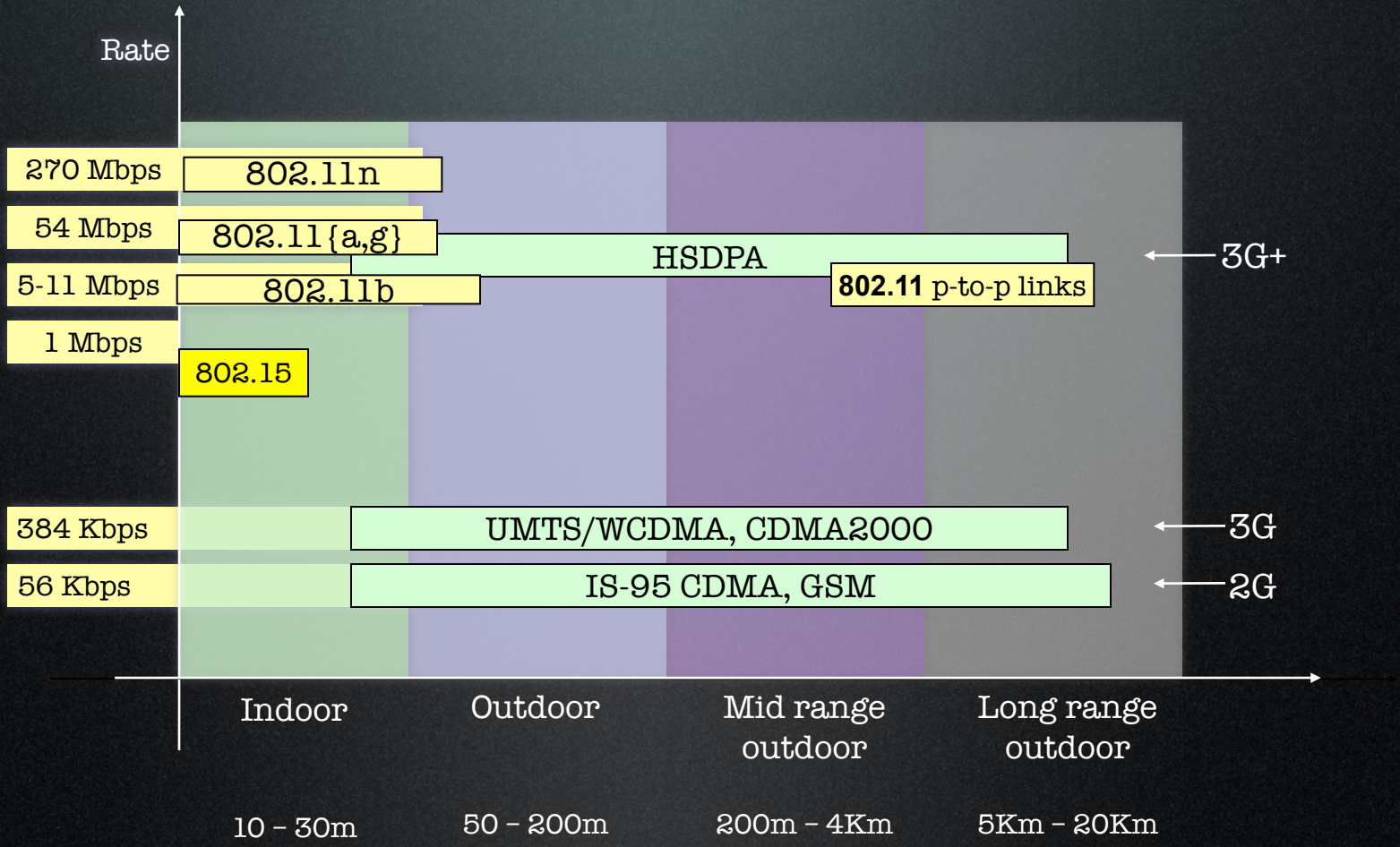
- Application specific networks
  - Monitoring
  - Safety
  - Event Detection
- Lots of tiny inexpensive devices (not always)
- Key Difference: Gateways / Processing nodes
- Connection to some infrastructure
- Bottlenecks

One step further… Mesh Networking



- Application specific networks
  - Monitoring
  - Safety
  - Event Detection
- Lots of tiny inexpensive devices (not always)
- Key Difference: Gateways / Processing nodes
- Connection to some infrastructure
- Bottlenecks

Some well known link layer standards

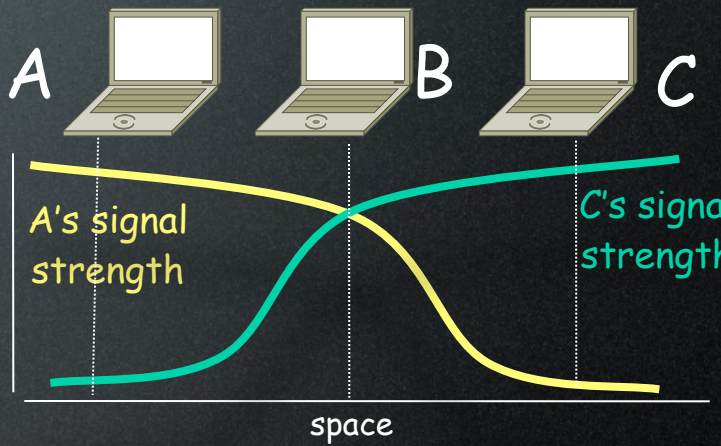


Wireless Link Characteristics

- Differences from wired links…
  - **the signal strength notion:** radio signal attenuates as it propagates in space (**path loss**)
  - **interference** from other sources: standard wireless network frequencies
    - e.g., 2.4 GHz: shared by other devices (e.g., phone); devices (motors) interfere as well
    - e.g., 5 GHz: Radars
  - **multipath** propagation: radio signal bounces off different objects, the ground etc, arriving at the destination at slightly different times
- ….make communication across (even a point to point) wireless links more challenging

Wireless network characteristics

Multiple wireless senders and receivers create additional problems (not just the multiple access ones):



Hidden terminal problem

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

means A, C unaware of their interference at B

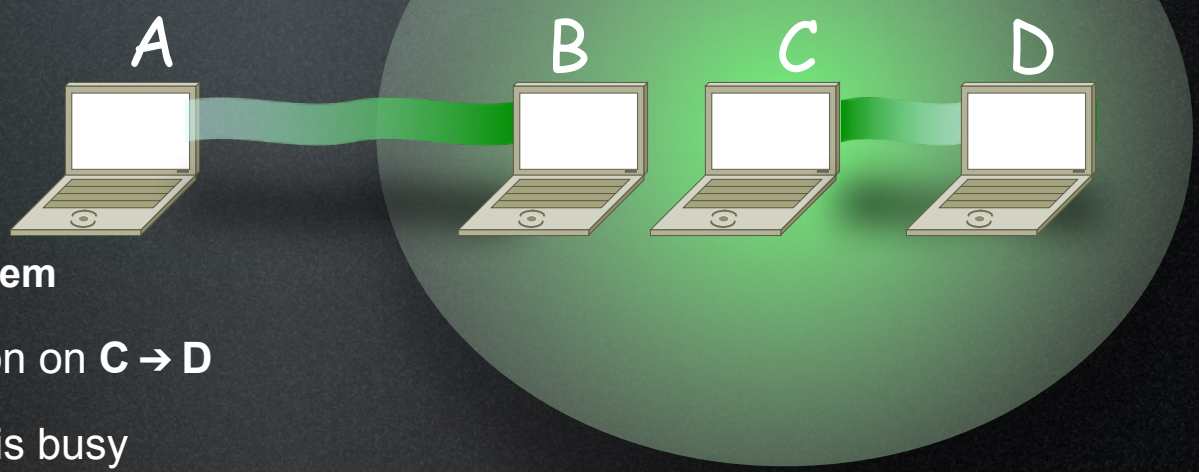
Due to Signal fading:

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

interfering at B

Wireless network characteristics

Multiple wireless senders and receivers create additional problems (not just the multiple access ones):



Exposed terminal problem

- **B** hears the transmission on **C → D**
  - Assumes channel is busy
  - Defers from accessing the channel to avoid collisions
- **A** could well accept any transmission from **B**…

IEEE 802.11 Wireless : the household names

IEEE	aka	year	GHz	modulation & constellation		MIMO / BW	Data Rate (20 MHz)
802.11		1997	2.4	DSSS	Barker“BPSK”	1x1 / 20 MHz	2
802.11b		1999	2.4	DSSS	CCK“QPSK”	1x1 / 20 MHz	11
802.11a		1999	5	OFDM	64-QAM	1x1 / 20 MHz	54
802.11g		2003	2.4	OFDM	64-QAM	1x1 / 20 MHz	54
802.11n	Wi-Fi 4	2008	2.4/5	OFDM	64-QAM	4x4 (3) / 40 MHz	65/130/260
802.11ac	Wi-Fi 5	2014	5	OFDM	256-QAM	8x8 (4) / 160 (80) MHz	78/156/312
802.11ax	Wi-Fi 6(E)	2020	2.4/5/6	OFDMA	1024-QAM	8x8 (4) / 160 (80) MHz	135/270/540
802.11be	Wi-Fi 7	2025?	2.4/5/6	OFDMA	4096-QAM	16x16 / 320 MHz	163/326/652

IEEE 802.11 Wireless: is there more?

- IEEE 802.11 - THE WLAN STANDARD was original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared [IR] standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)

IEEE 802.11 Wireless: is there more?

- IEEE 802.11-2007 - A new release of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- IEEE 802.11k - Radio resource measurement enhancements (2008)
- IEEE 802.11l - (reserved and will not be used)
- IEEE 802.11m - Maintenance of the standard. Recent edits became 802.11-2007. (ongoing)
- IEEE 802.11n - Higher throughput improvements using MIMO (multiple input, multiple output antennas) (November 2009)
- IEEE 802.11o - (reserved and will not be used)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (working - 2009?)
- IEEE 802.11q - (reserved and will not be used, can be confused with 802.1Q VLAN tagging)
- IEEE 802.11r - Fast roaming Working "Task Group r" - (2008)
- IEEE 802.11s - Mesh Networking, Extended Service Set (ESS) (working - Jul 2010?)
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics Recommendation (2008)

IEEE 802.11 Wireless: is there more?

- IEEE 802.11u - Interworking with non-802 networks (for example, cellular) (proposal evaluation - Mar 2010?)
- IEEE 802.11v - Wireless network management (early proposal stages - Sept 2010?)
- IEEE 802.11w - Protected Management Frames (early proposal stages - 2009?)
- IEEE 802.11x - (reserved and will not be used, can be confused with 802.1x Network Access Control)
- IEEE 802.11y - 3650-3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z - Extensions to Direct Link Setup (DLS) (Aug 2007 - Dec 2011)
- IEEE 802.11aa - Robust streaming of Audio Video Transport Streams (Mar 2008 - May 2011)

- IEEE 802.11ac - Very High Throughput <6GHz (Sep 2008 - Dec 2012)
- IEEE 802.11ad - Extremely High Throughput 60GHz (Dec 2008 - Dec 2012)
- IEEE 802.11ax - WiFi 6 / WiFi 6e (6 GHz band) (2020)
- IEEE 802.11be - WiFi 7 (…2024?)

802.11: Channels, association

- **802.11b:** 2.4GHz-2.485GHz spectrum divided into 11/13/14 **channels** at different frequencies
  - AP admin chooses frequency (channel) for AP
  - interference possible: frequency can be neighboring to the one chosen by neighboring AP!
- host: must **associate** with an AP
  - scans channels, listening for **beacon** frames containing AP's SSID (Service Set Id) & MAC address
  - selects AP to associate with
  - may perform authentication
  - may run DHCP to get IP address in AP's subnet

IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

if channel sensed idle for **DIFS** then

- transmit entire frame (no CD)

if sensed channel busy then

- start random back-off:
  - timer counts down while sensing channel
  - As long as channel idle then:
    - transmit when timer expires
  - Otherwise increase random back-off interval …up to?
  - When all else fails after a maximum number of failed retries send packet anyways.

802.11 receiver

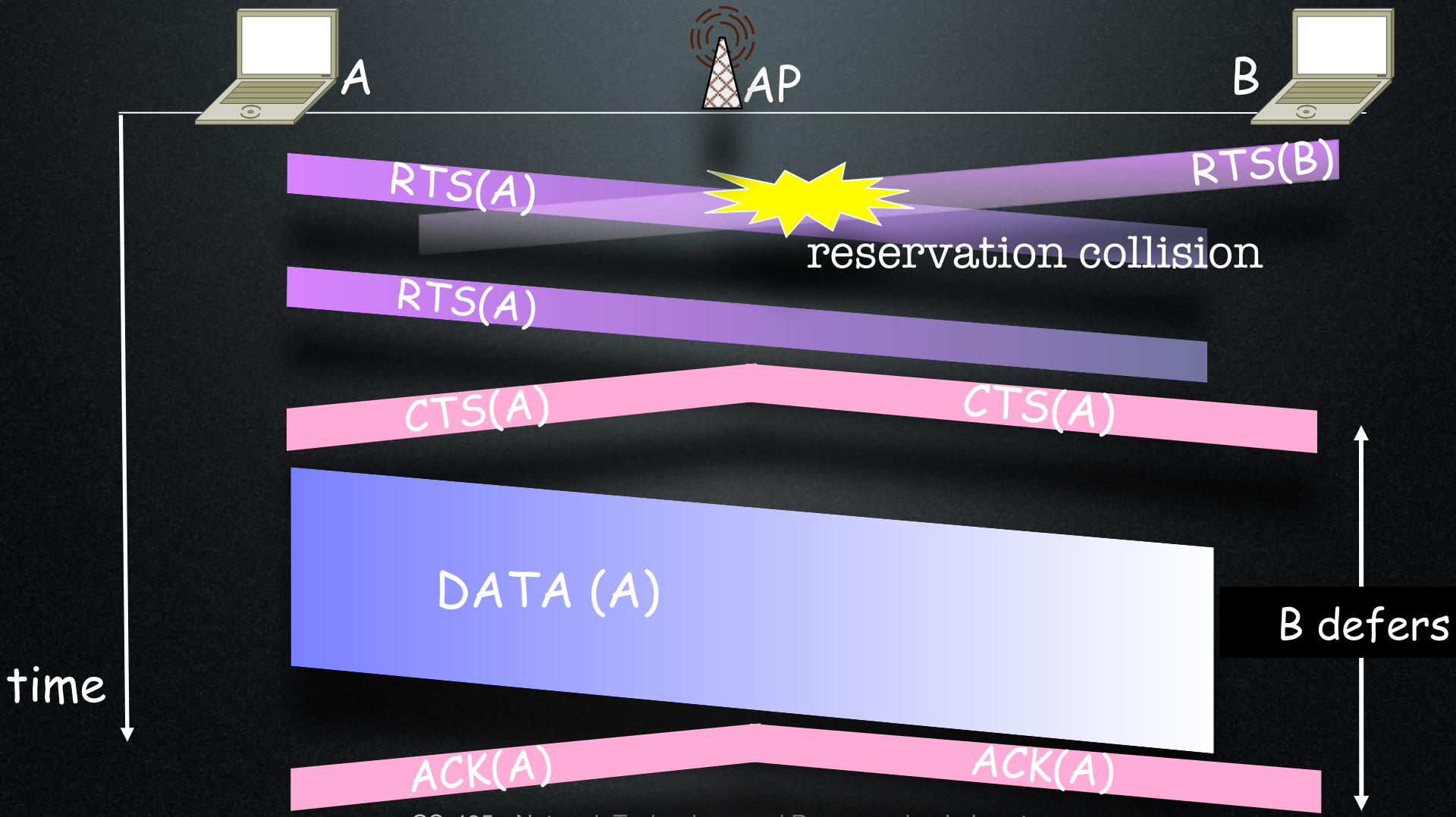
- if frame received OK
- Wait for **SIFS** (why??)
- return ACK after ACK needed also due to hidden terminal problem

Avoiding collisions (the ‘CA’ part in CSMA/CA)

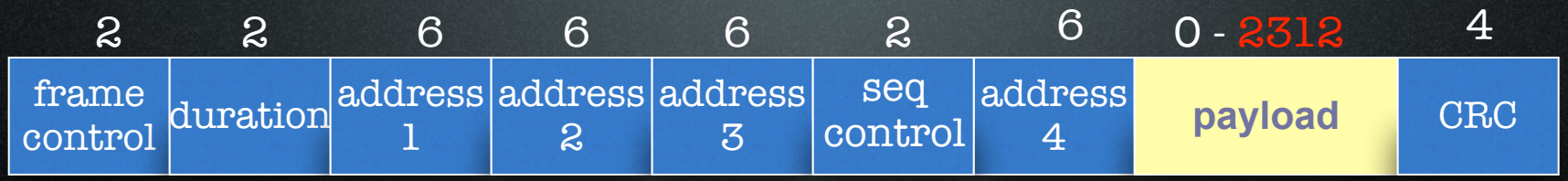
- **idea:** allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

1. sender first transmits **small** request-to-send (RTS) packets to BS using CSMA
    - RTSs may still collide with each other (but they’re short ➔ chances are slim for RTS collisions)
2. BS broadcasts clear-to-send CTS in response to RTS
3. CTS heard by all nodes
    - sender transmits data frame
    - other stations defer transmissions

RTS-CTS exchange



802.11 frame: addressing



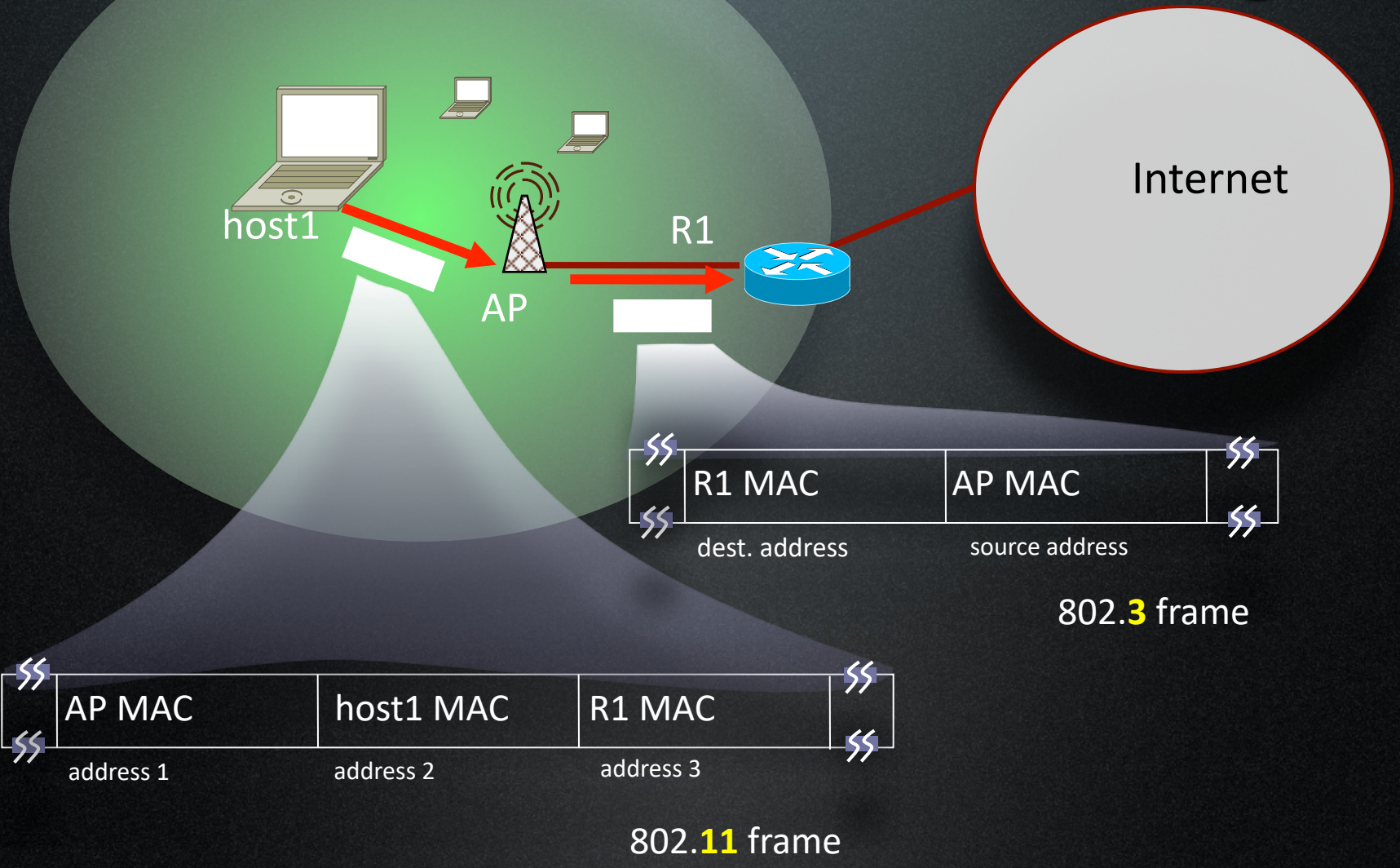
Address 1: MAC address of wireless host or **AP** to **receive** this frame

Address 2: MAC address of **wireless host** or AP **transmitting** this frame

Address 3: MAC address of **initial transmitter or final recipient**

Address 4: used only in ad hoc mode

802.11 frame: addressing



802.11 frame: more