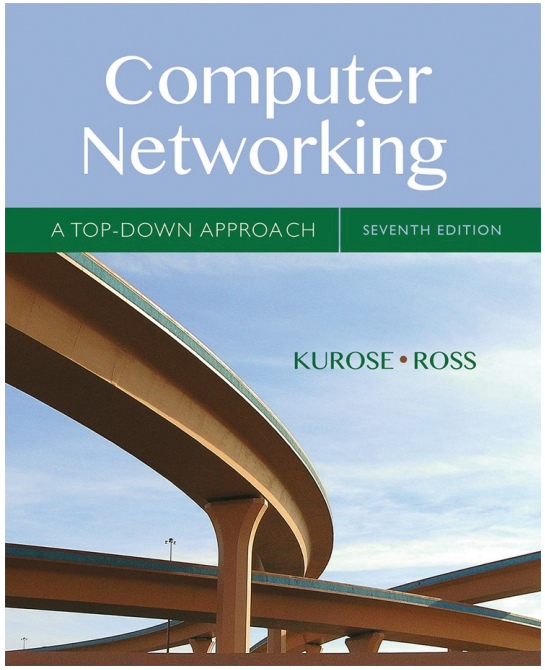
Information Technology Fundamentals

Mohammad Hossein Manshaei

manshaei@gmail.com

Networking: WiFi Networks
Module 2: Part 2

Reference: Chapter 7 Wireless and Mobile Networks



Computer Networking: A Top Down Approach

7th edition
Jim Kurose, Keith Ross
Pearson/Addison Wesley
April 2016

A note on the use of these Powerpoint slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a lot of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Chapter 7 outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics
- CDMA

7.3 IEEE 802.11 wireless LANs ("Wi-Fi")

7.4 Cellular Internet Access
- architecture
- standards (e.g., 3G, LTE)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

7.7 Handling mobility in cellular networks

7.8 Mobility and higher-layer protocols

IEEE 802.11 Wireless LAN

802.11b
- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

802.11a
- 5-6 GHz range
- up to 54 Mbps

802.11g
- 2.4-5 GHz range
- up to 54 Mbps

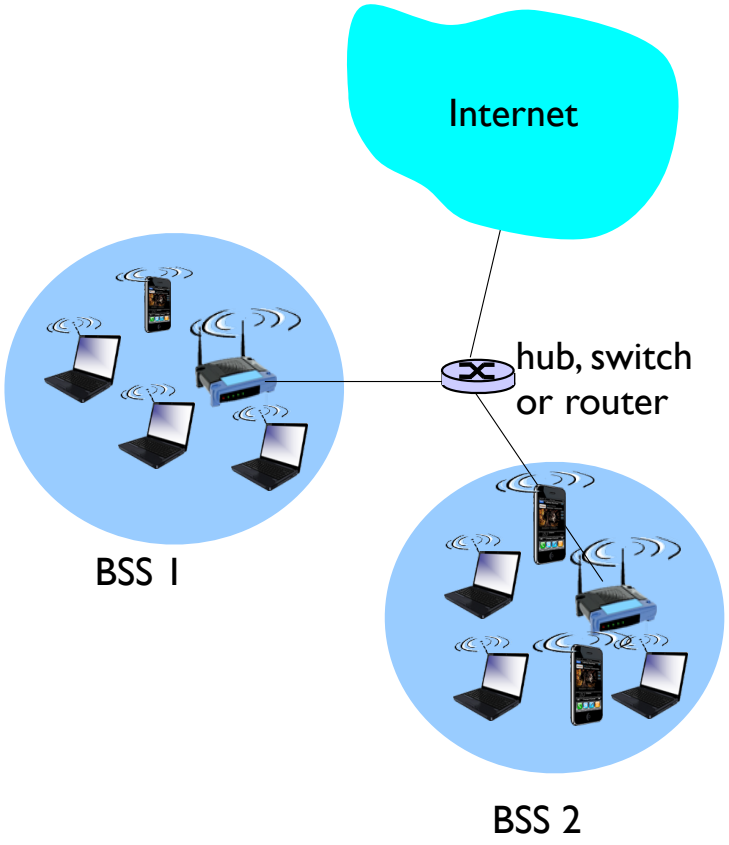
802.11n: multiple antennae
- 2.4-5 GHz range
- up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

Standards and amendments

- Within the IEEE 802.11 Working Group,the following IEEE Standards Association Standard and Amendments exist:
- • IEEE 802.11-1997: The WLAN standard was originally 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 Mbit/s 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 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)
- • IEEE 802.11k: Radio resource measurement enhancements (2008)
- • IEEE 802.11n: Higher-throughput improvements using MIMO (multiple-input, multiple-output antennas) (September 2009)
- • IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- • IEEE 802.11r: Fast BSS transition (FT) (2008)
- • IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)
- • IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled
- • IEEE 802.11u: Improvements related to HotSpots and 3rd-party authorization of clients, e.g., cellular network offload (February 2011)
- • IEEE 802.11v: Wireless network management (February 2011)
- • IEEE 802.11w: Protected Management Frames (September 2009)
- • IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- • IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)

802.11 LAN architecture

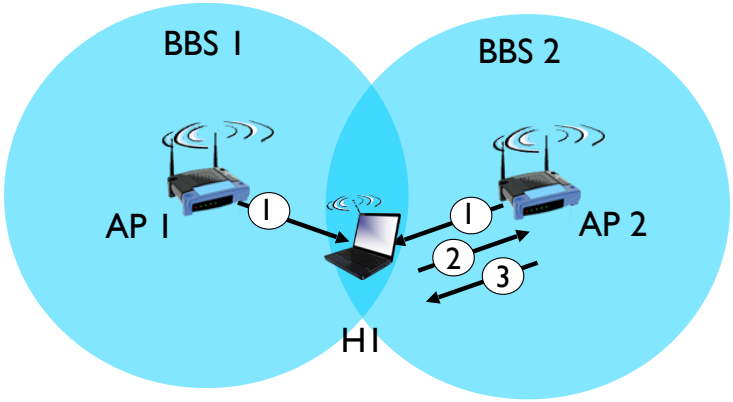


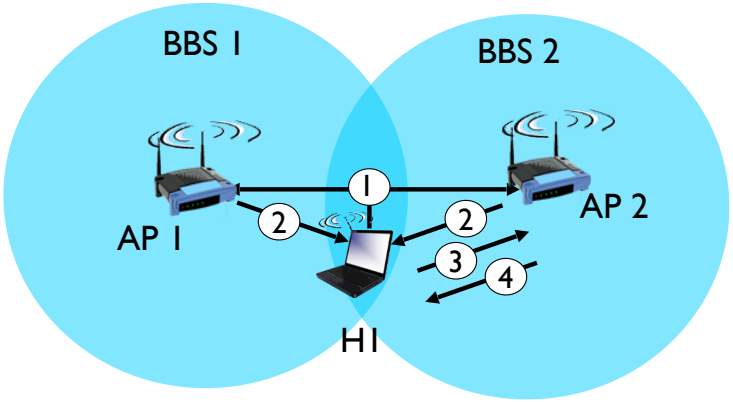
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication [Chapter 8]
  - will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning





passive scanning:

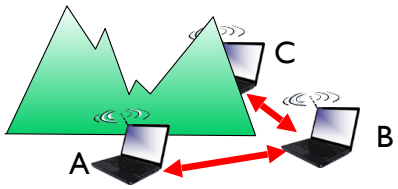
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

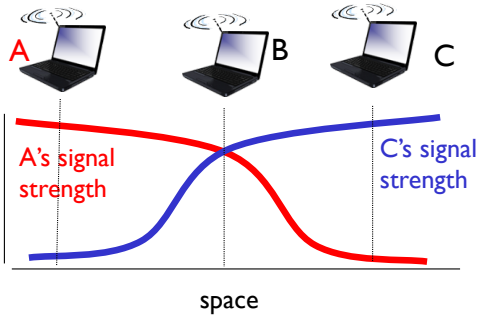
active scanning:

(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

IEEE 802.11: multiple access

- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC Protocol: CSMA/CA

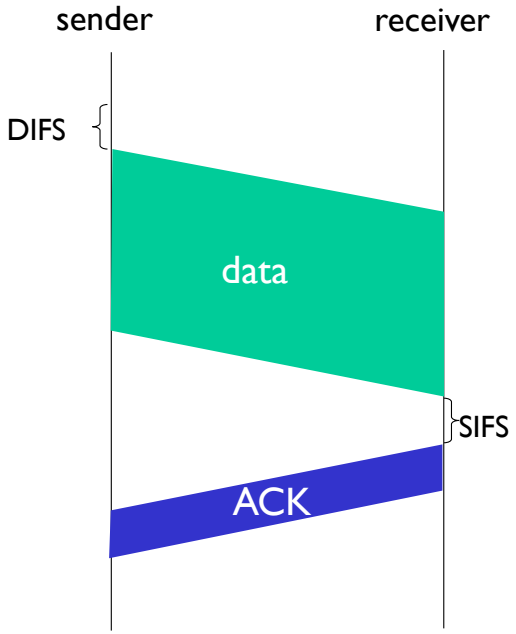
802.11 sender

1 if sense channel idle for DIFS then
  transmit entire frame (no CD)

2 if sense channel busy then
  start random backoff time
  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 (ACK needed due to hidden terminal problem)



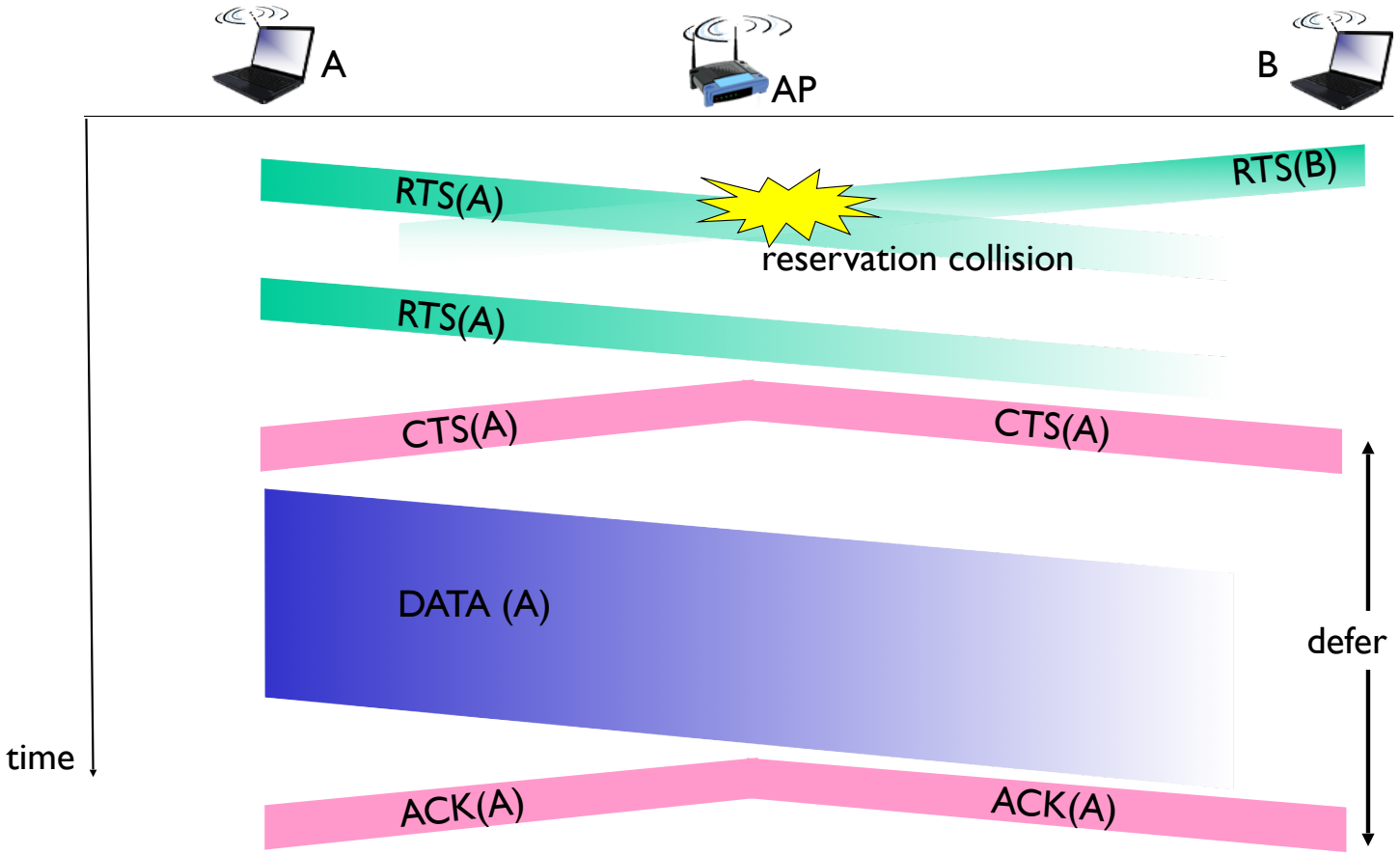
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

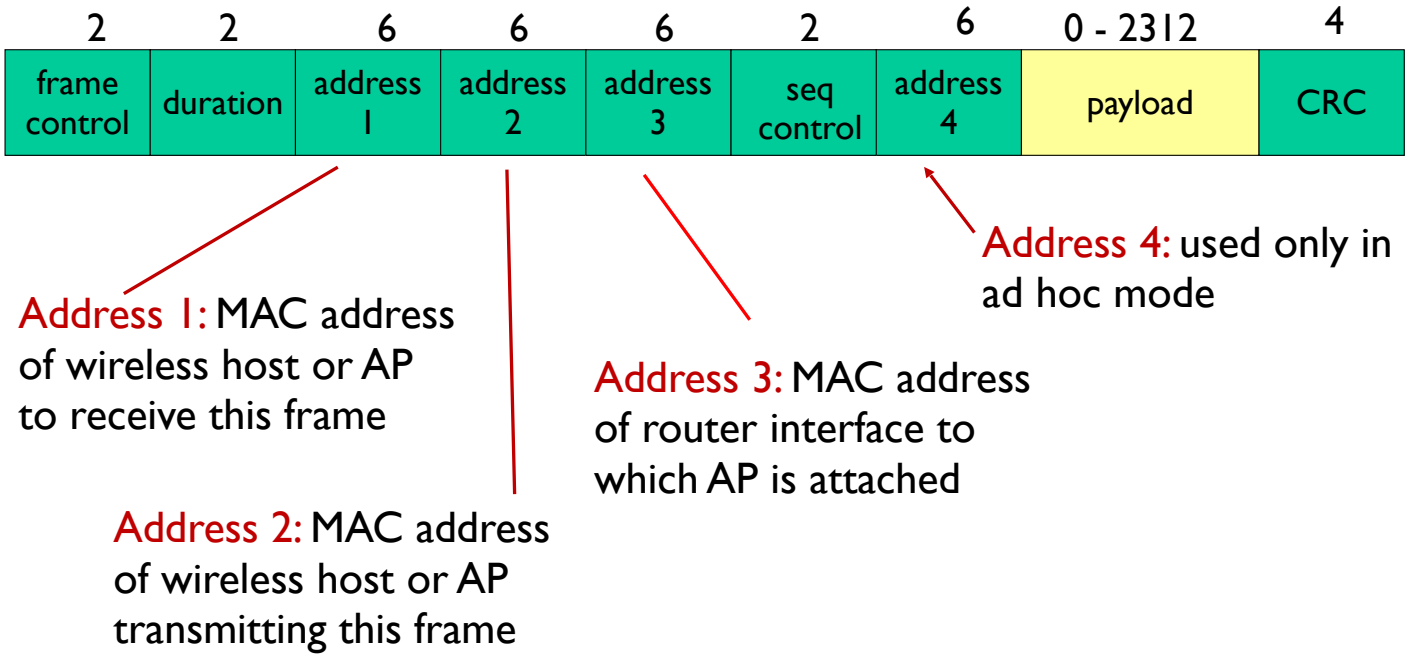
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

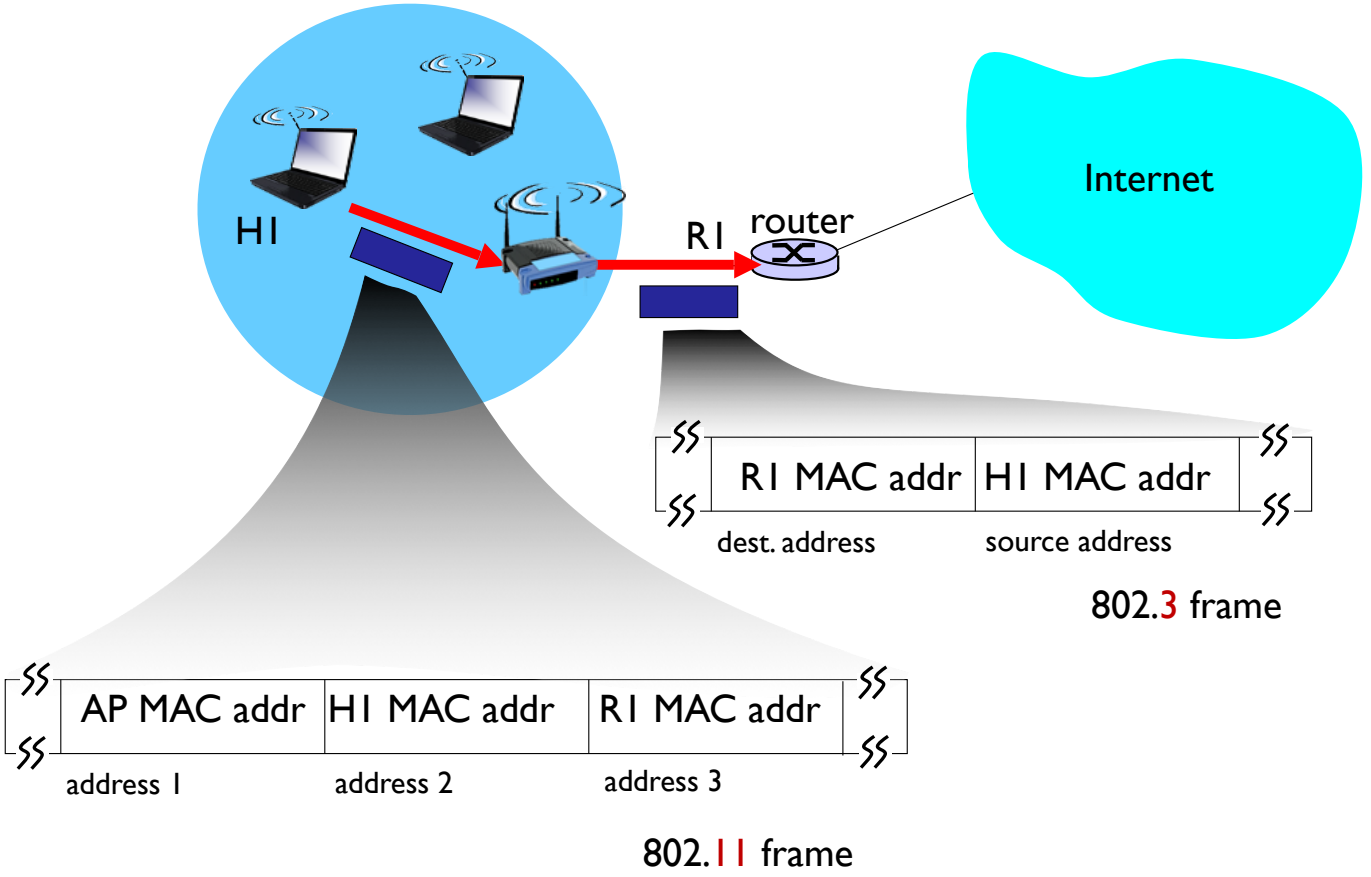
Collision Avoidance: RTS-CTS exchange



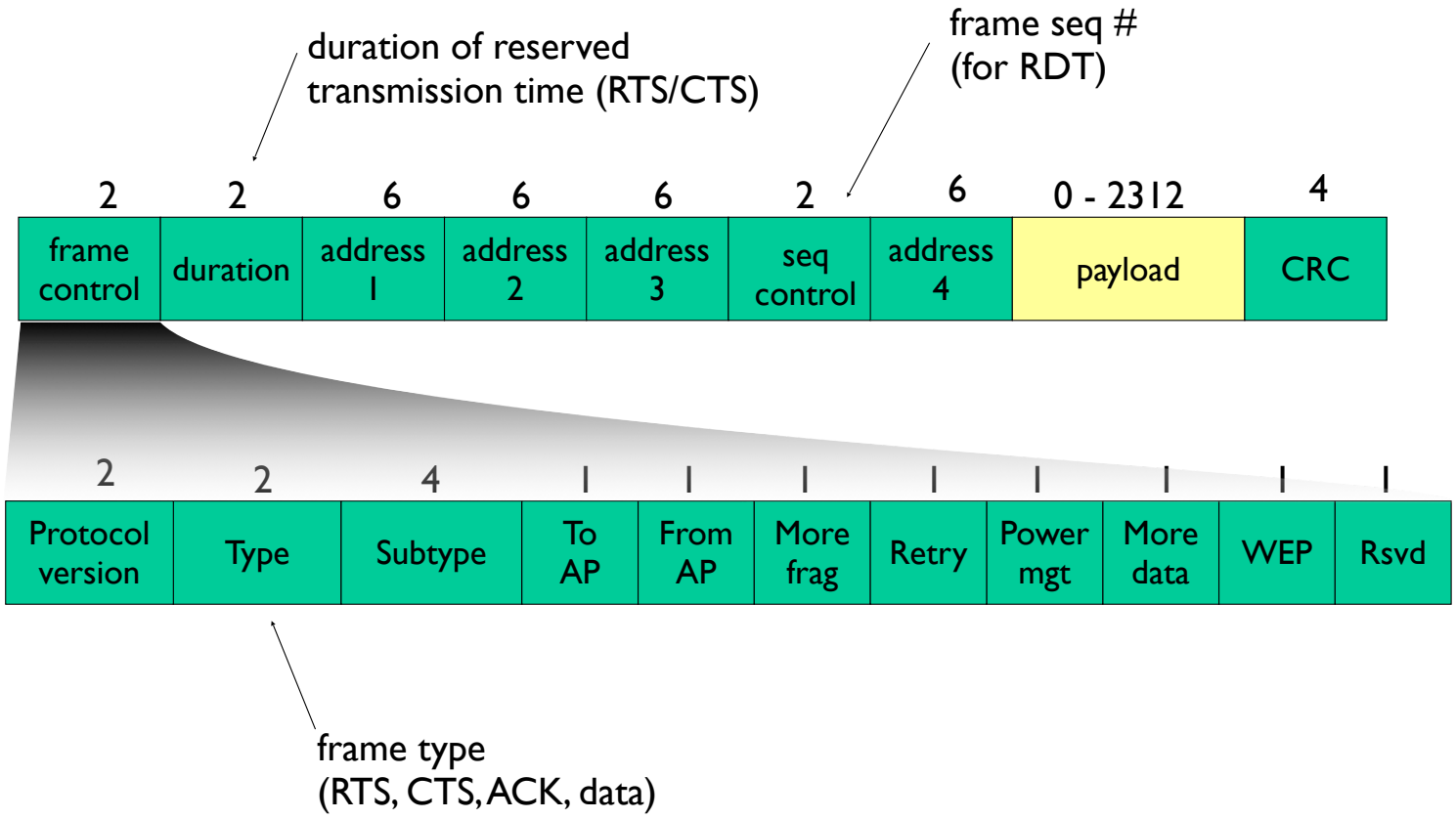
802.11 frame: addressing



802.11 frame: addressing

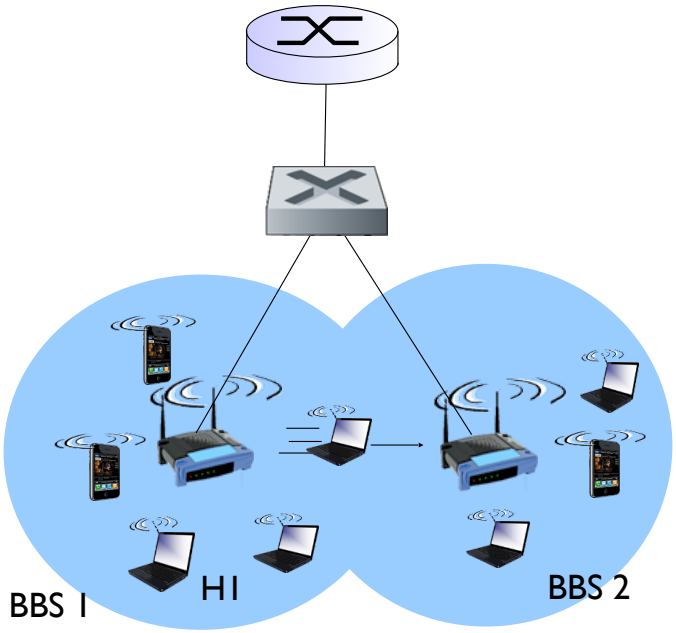


802.11 frame: more



802.11: mobility within same subnet

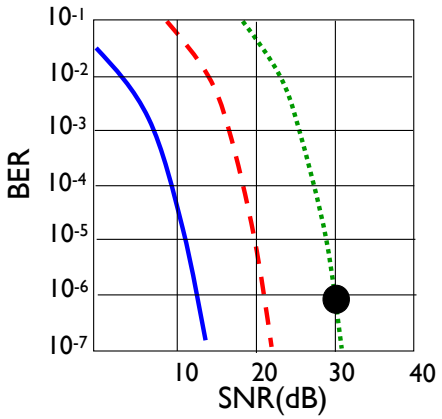
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1

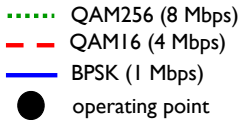


802.11: advanced capabilities

Rate adaptation

- base station, 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

802.11: advanced capabilities

power management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- 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

802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps