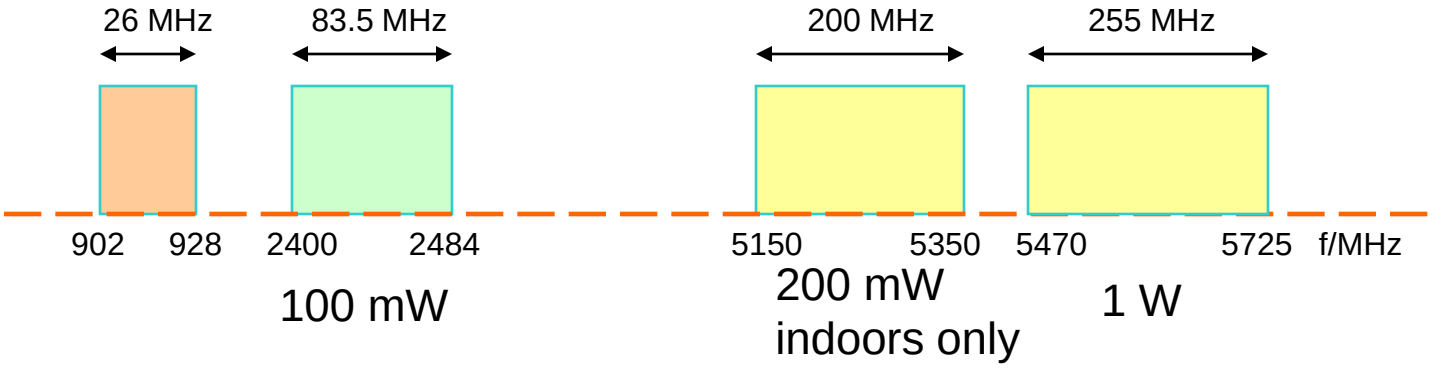
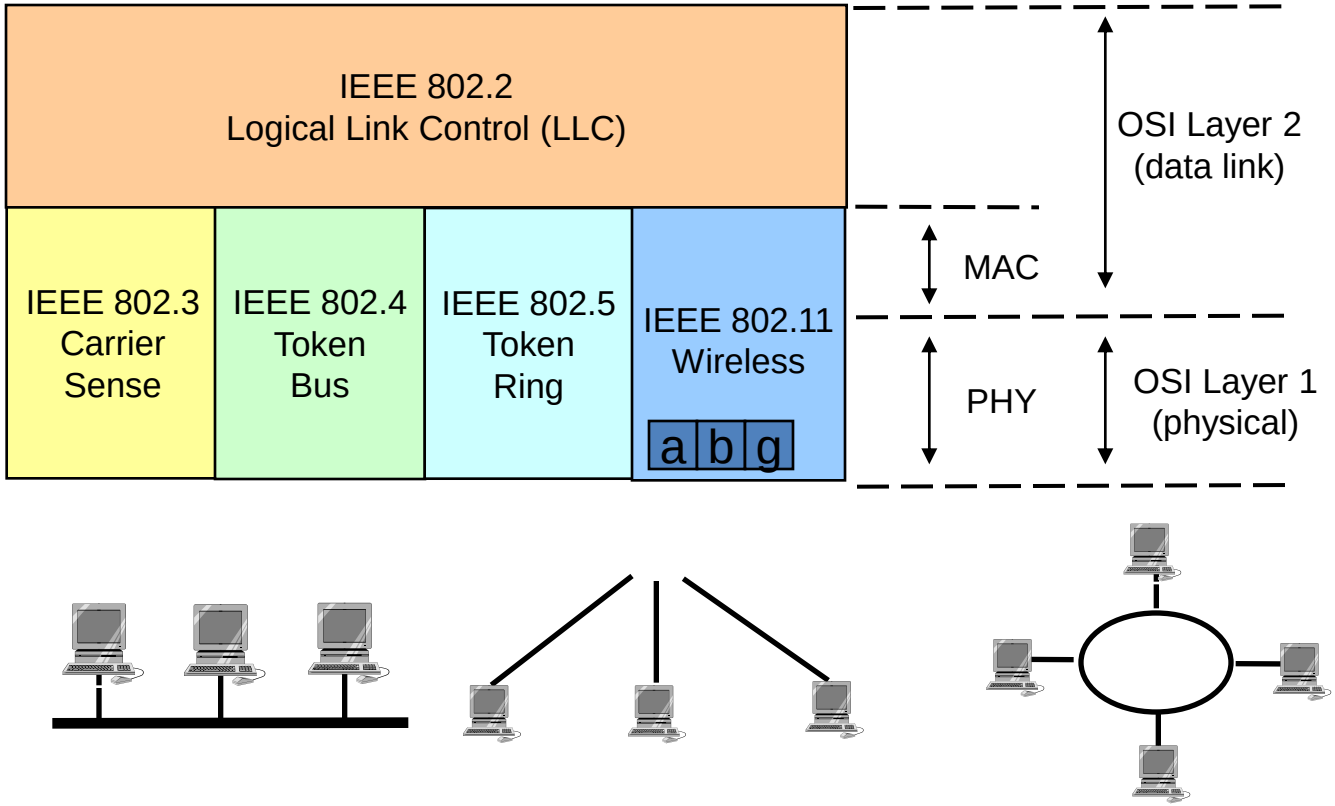
Wireless Local Area

802.11 WLAN technologies

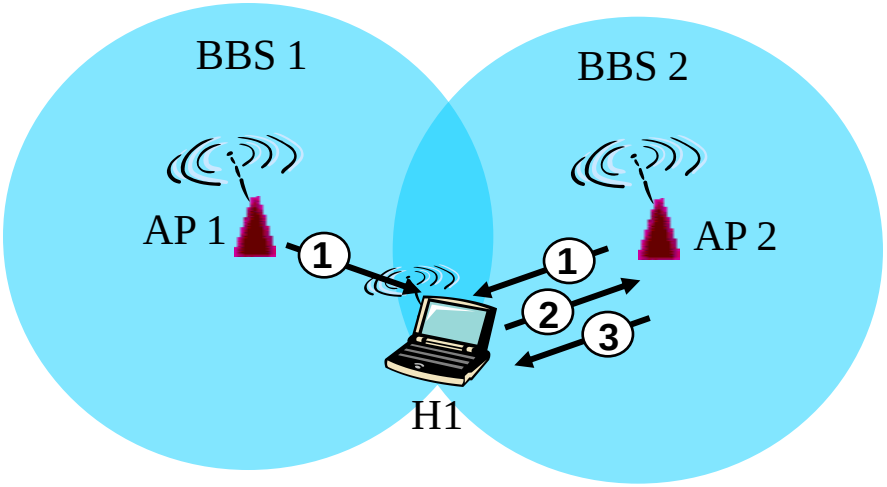
- IEEE 802.11 standards and rates
  - IEEE 802.11 (1997) 1 Mbps and 2 Mbps (2.4 GHz band)
  - IEEE 802.11b (1999) 11 Mbps (2.4 GHz band) = Wi-Fi
  - IEEE 802.11a (1999) 6, 9, 12, 18, 24, 36, 48, 54 Mbps (5 GHz band)
  - IEEE 802.11g (2001 ... 2003) up to 54 Mbps (2.4 GHz) backward compatible to 802.11b
- IEEE 802.11 networks work on license free industrial, science, medicine (ISM) bands:

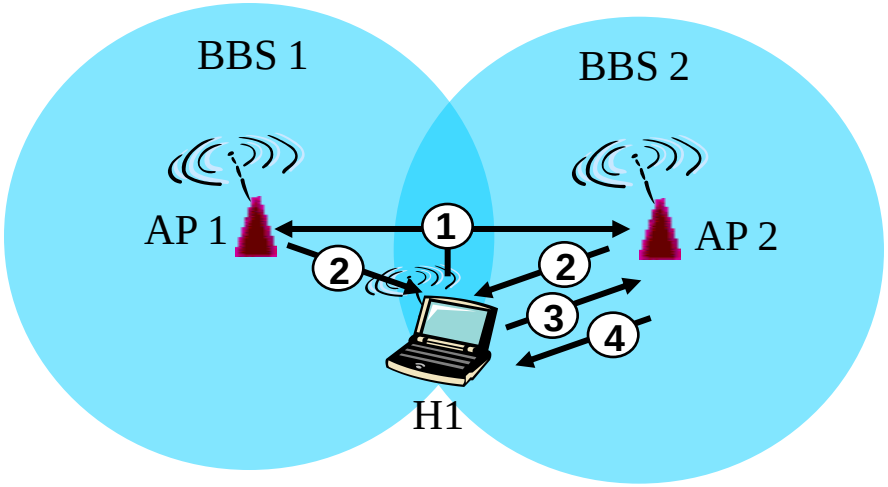


The IEEE 802.11 and supporting LAN Standards



802.11: passive/active scanning





Passive Scanning:

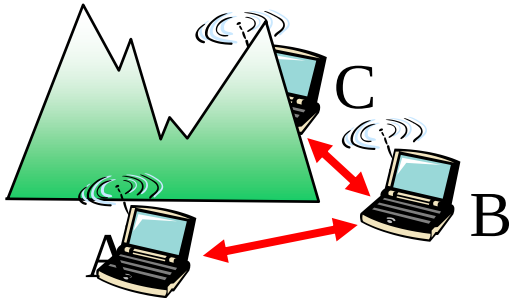
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent: H1 to selected AP

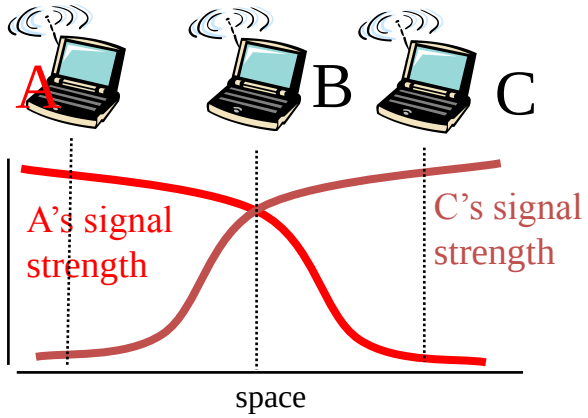
Active Scanning:

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

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

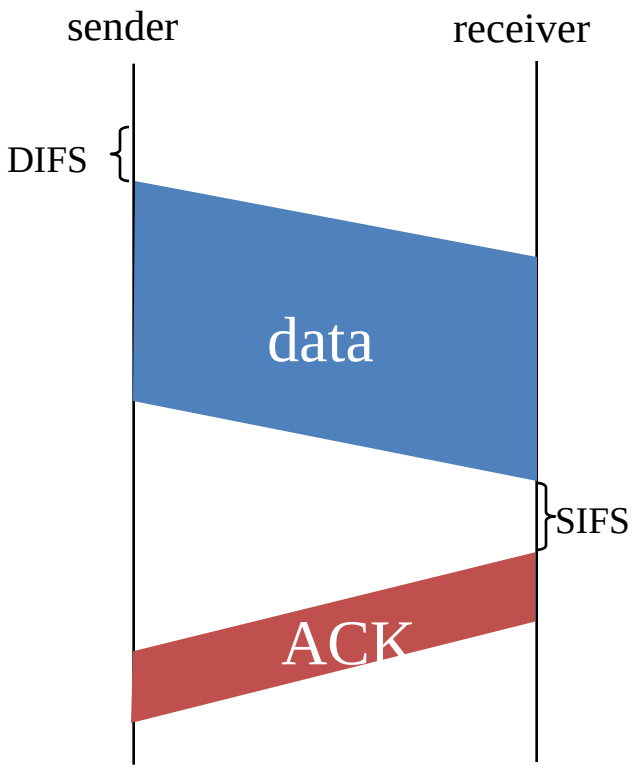
transmit when timer expires

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)



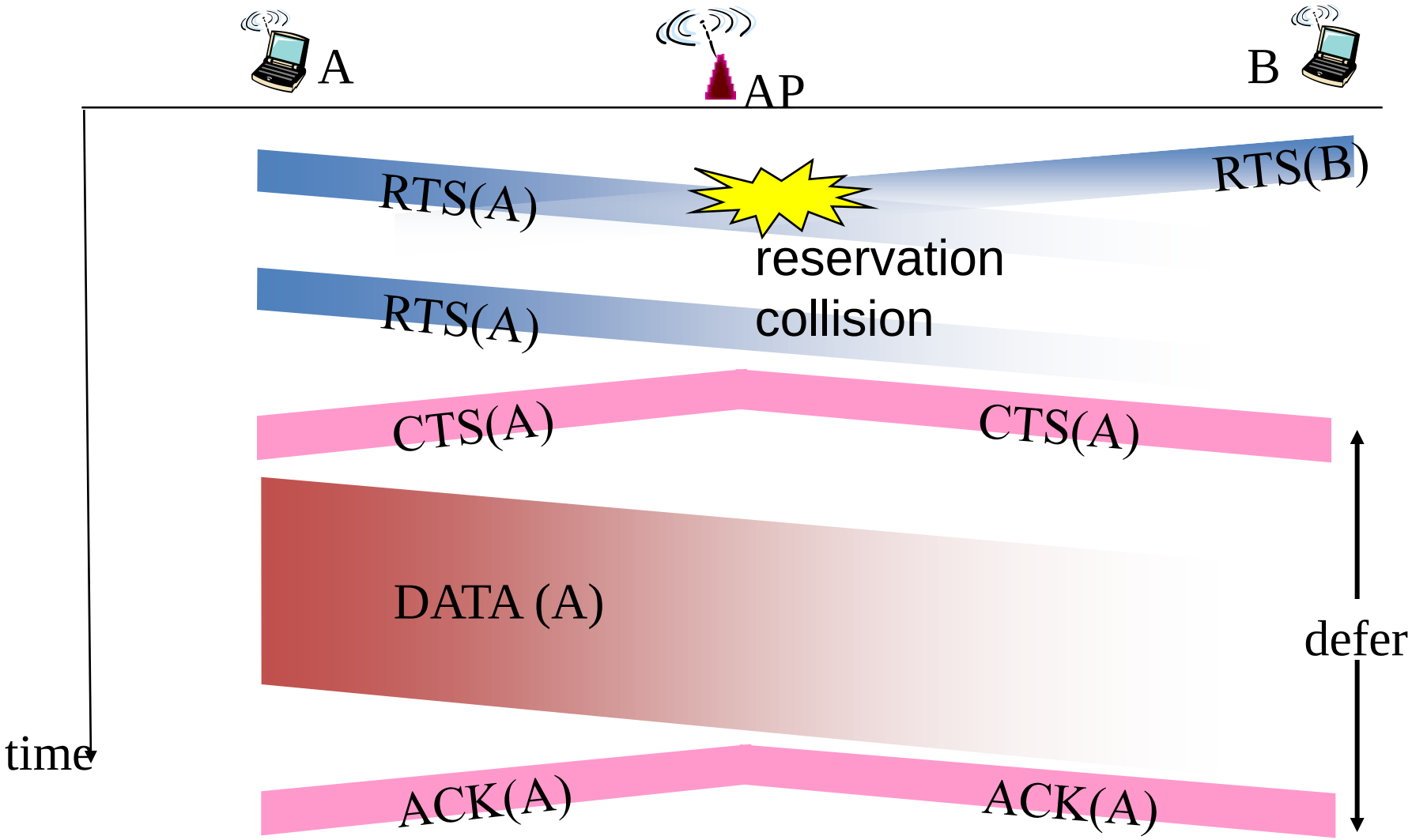
Avoiding collisions (more)

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

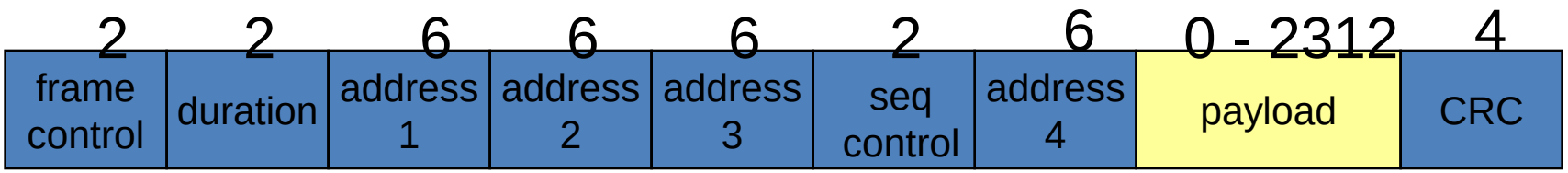
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



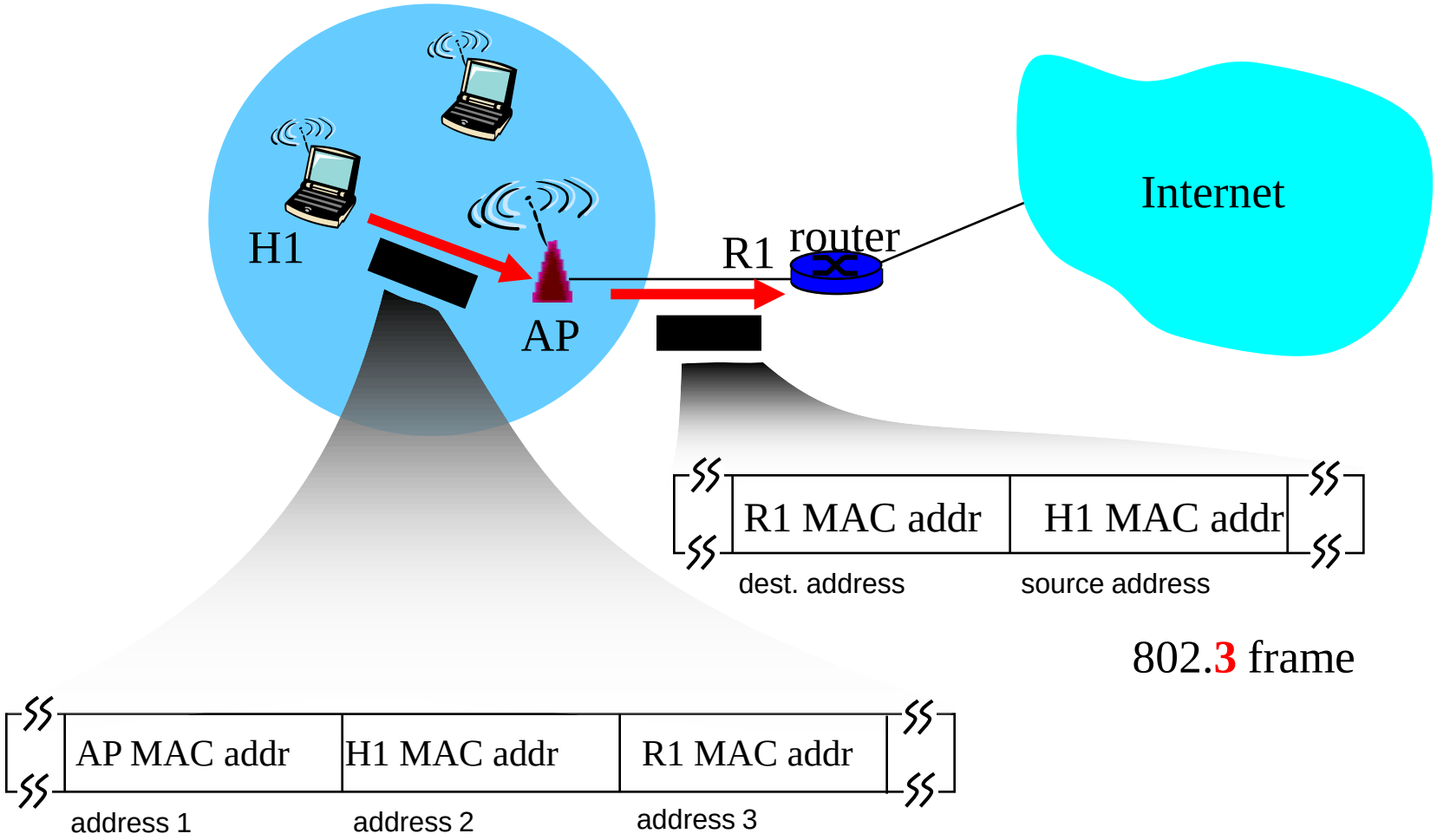
Address 1: MAC address of wireless host or AP to receive this frame

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

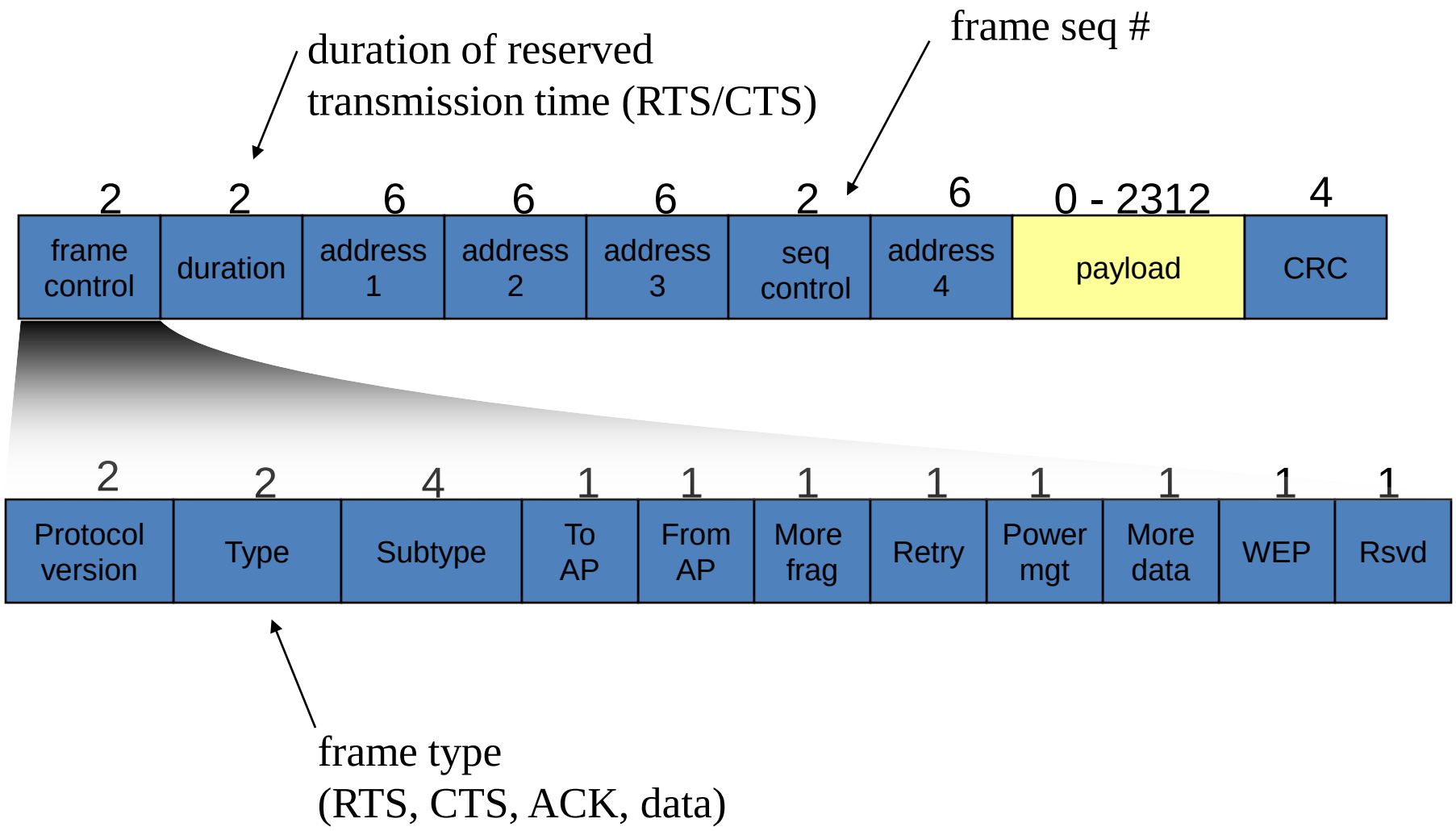
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

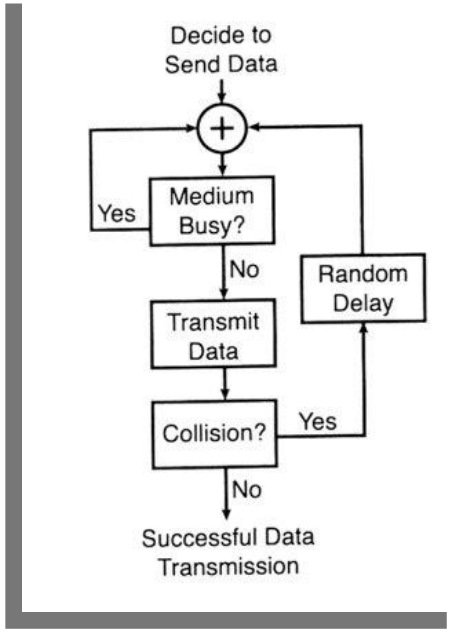
802.11 frame: addressing



802.11 frame: more

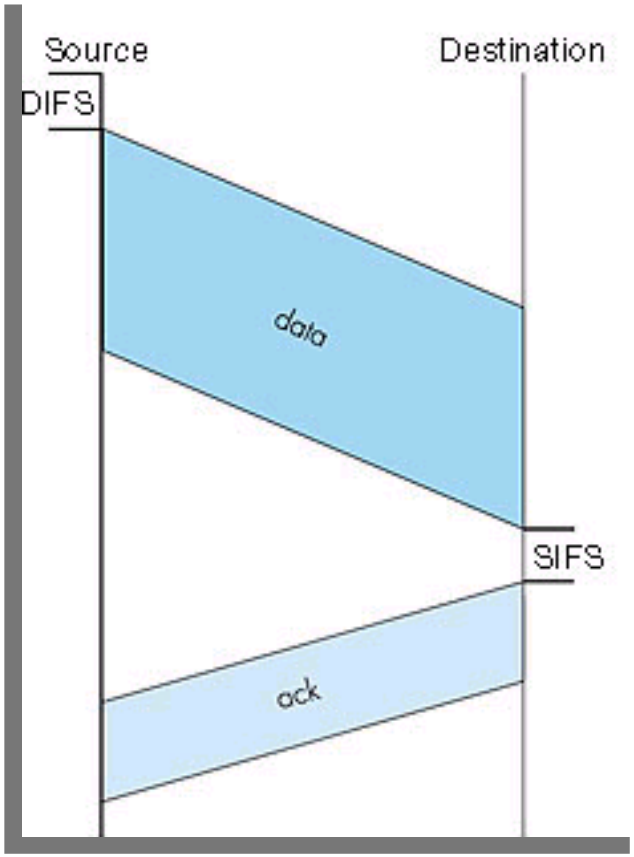


IEEE 802.11 Media Access Control (MAC)



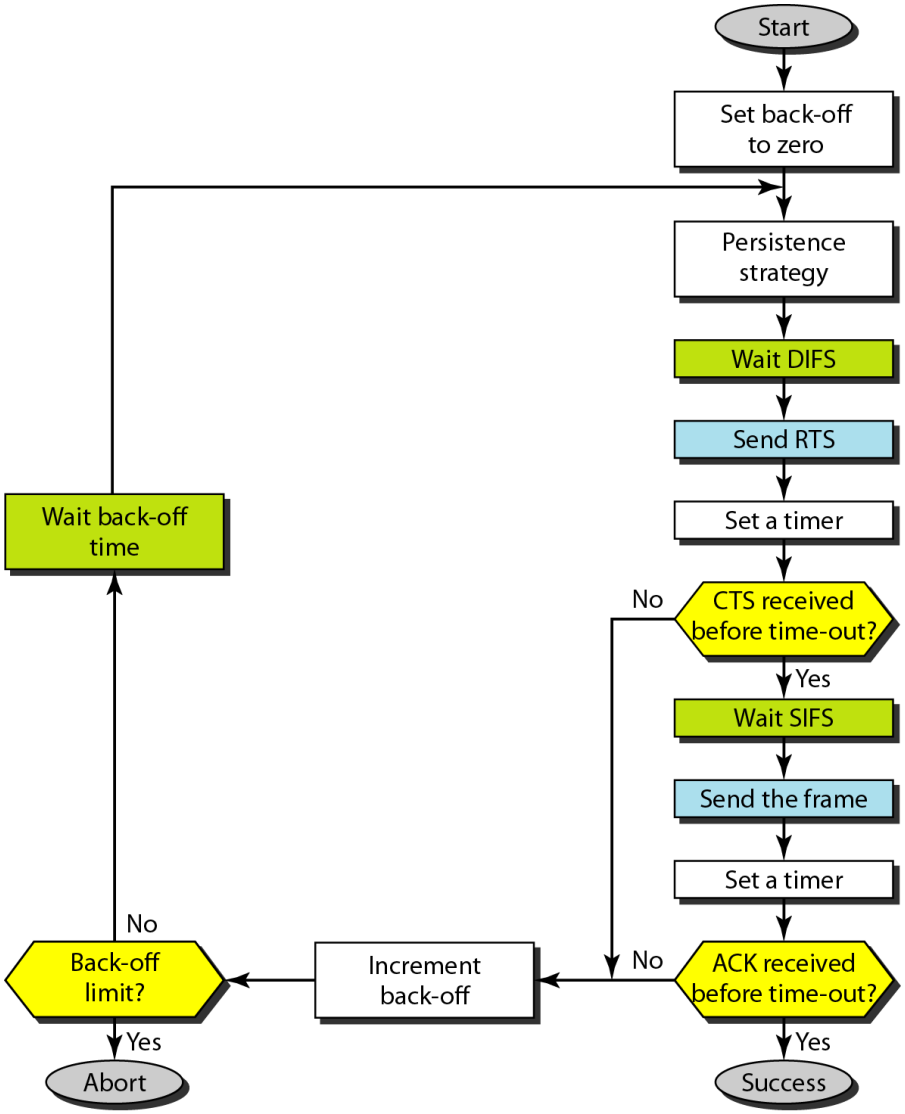
Carrier-sense multiple access protocol with collision avoidance (CSMA/CS)

1. An adapter may begin to transmit at any time, that is, no slots are used.
2. An adapter never transmits a frame when it senses that some other adapter is transmitting, that is, it uses carrier-sensing.
3. A transmitting adapter aborts its transmission as soon as it detects that another adapter is also transmitting, that is, it uses collision detection.
4. Before attempting a retransmission, an adapter waits a random time that is typically small compared to a frame time.

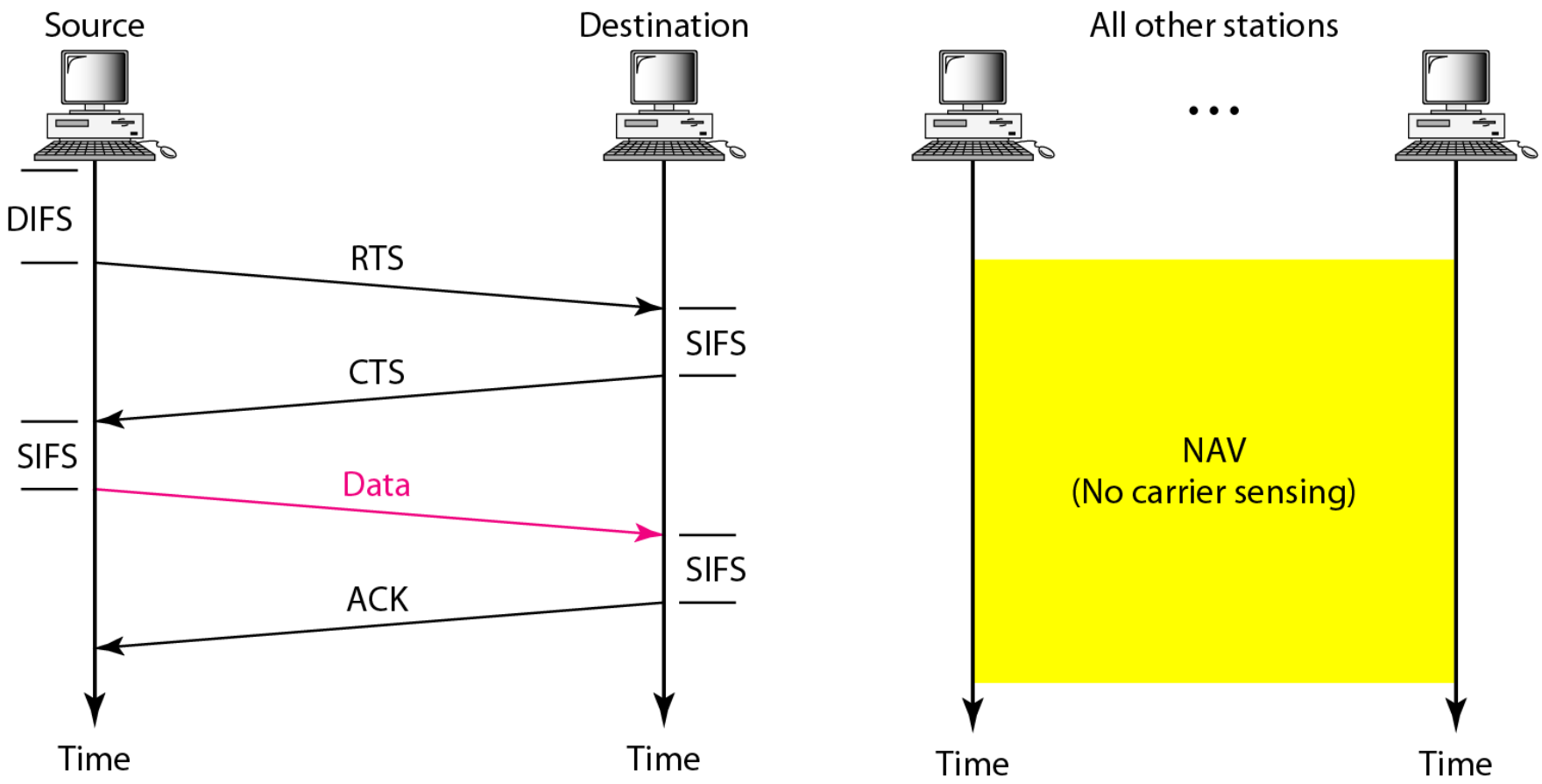


DIFS: Distributed Inter-Frame Spacing
SIFS: Short Inter-Frame Spacing
ack: Acknowledgement

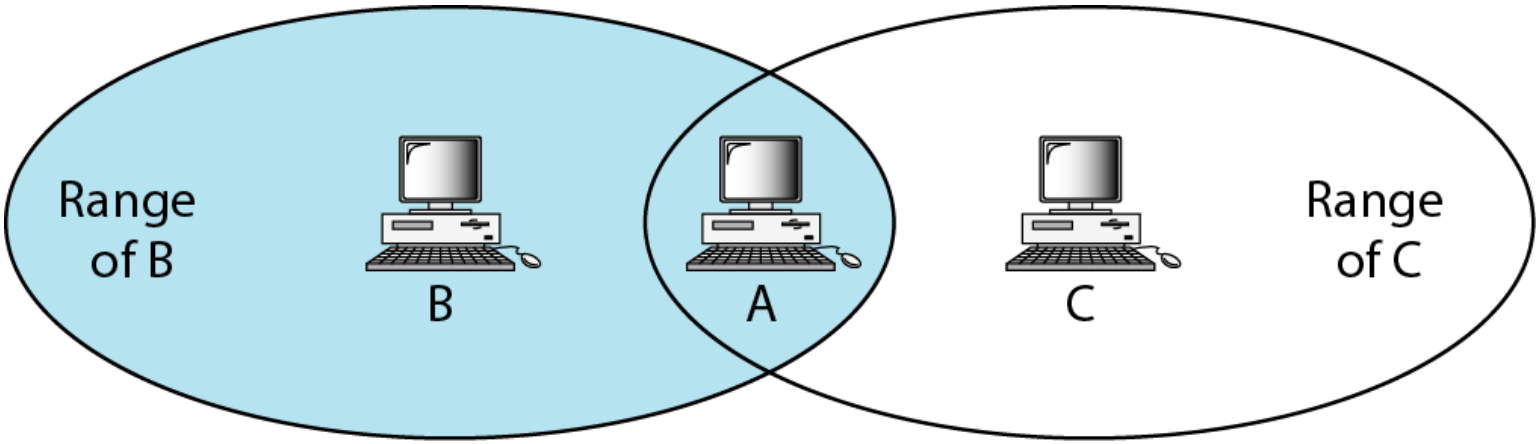
CSMA/CA flowchart



CSMA/CA and NAV



Hidden station problem

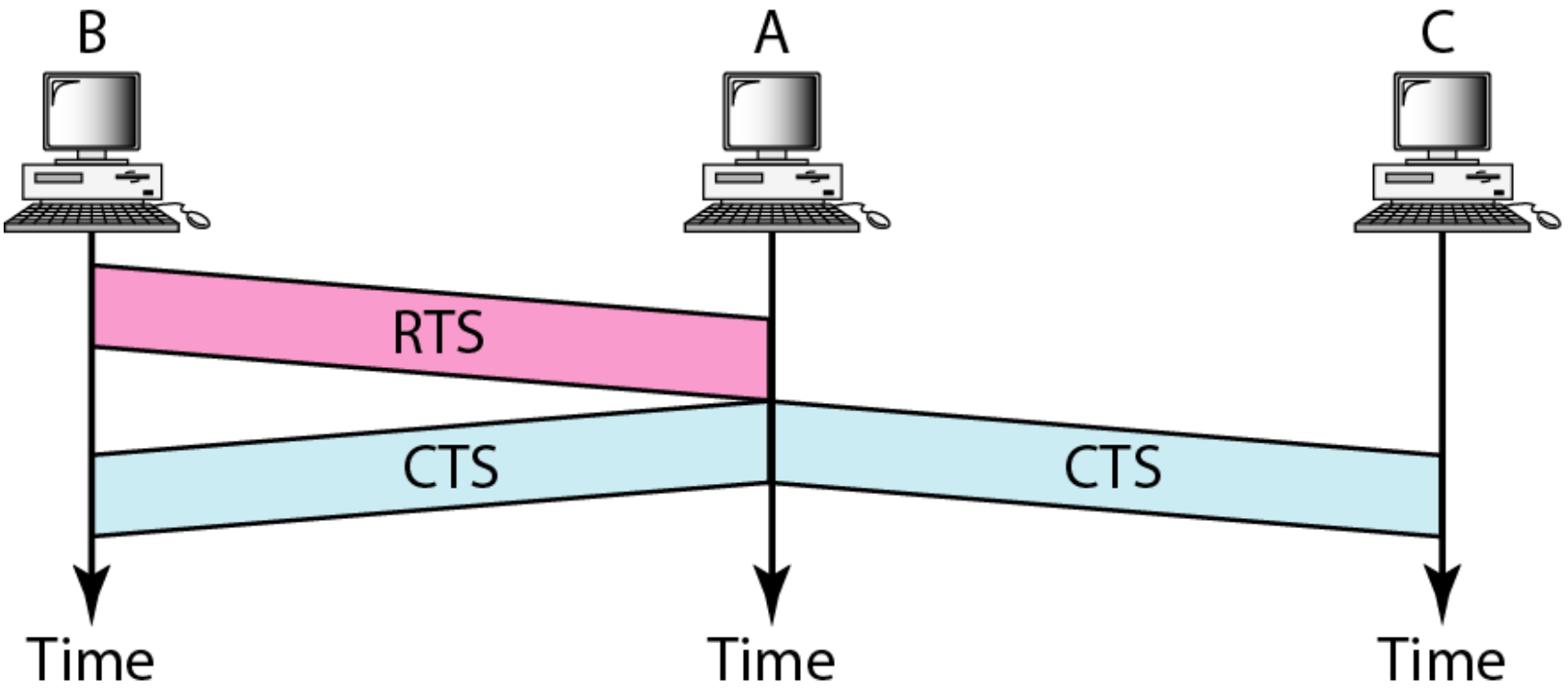


B and C are hidden from each other with respect to A.

Note

The CTS frame in CSMA/CA handshake can prevent collision from
a hidden station.

Use of handshaking to prevent hidden station problem



Exposed station problem

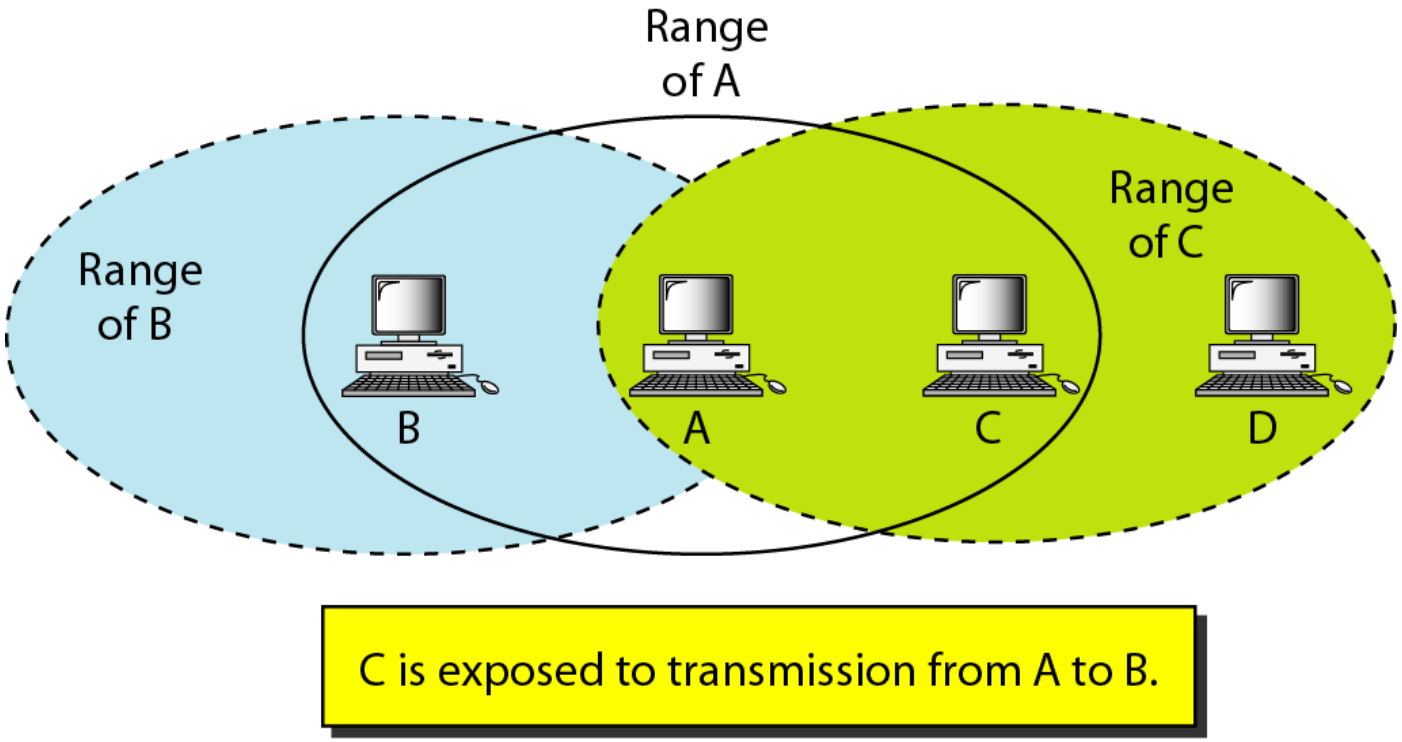
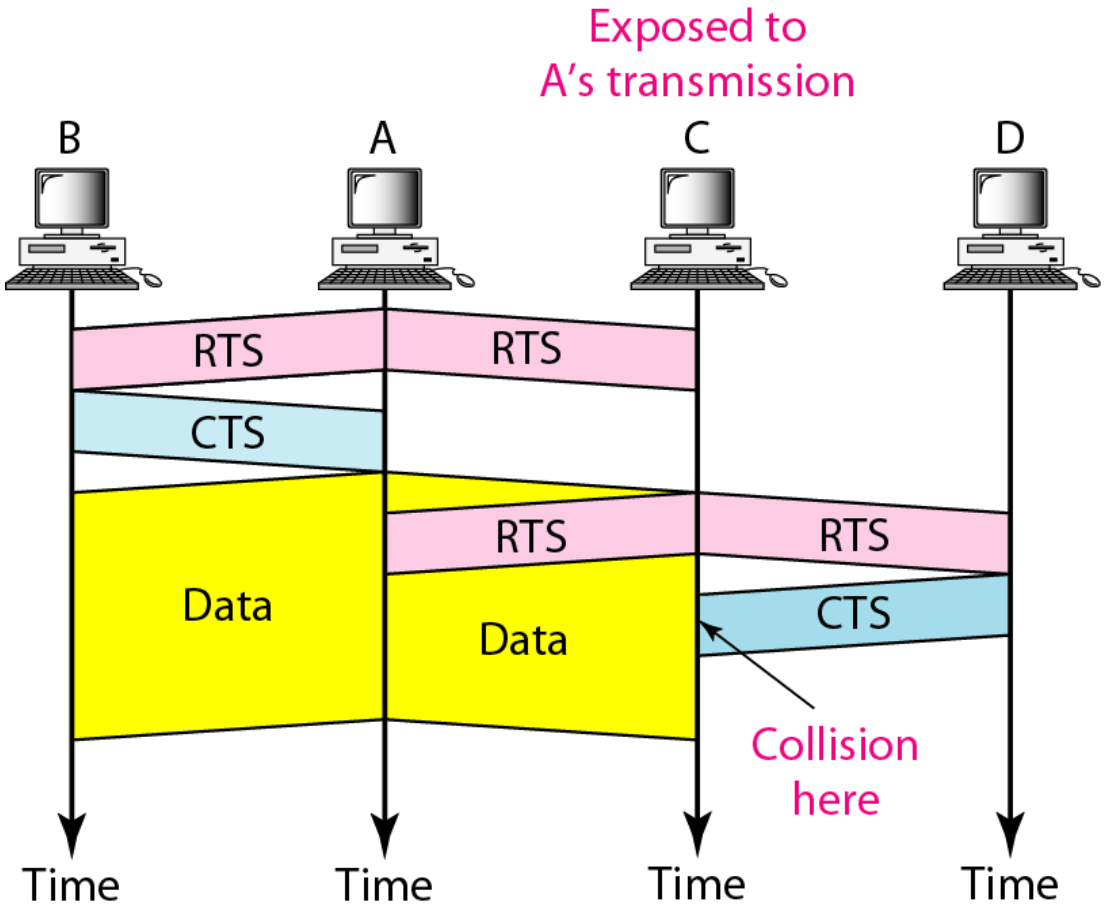
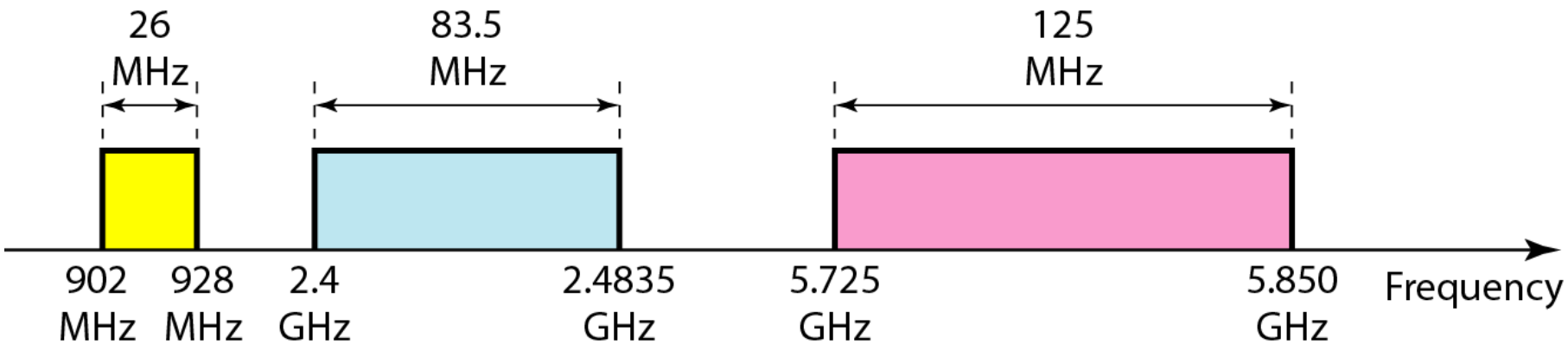


Figure 14.13 *Use of handshaking in exposed station problem*



Industrial, scientific, and medical (ISM) band



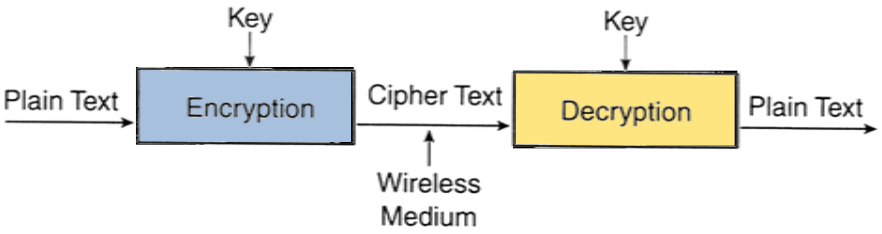
Security

- In theory, spread spectrum radio signals are inherently difficult to decipher without knowing the exact hopping sequences or direct sequence codes used

- The IEEE 802.11 standard specifies optional security called "**W**ired **E**quivalent **P**rivacy" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. The standard also specifies optional authentication measures.

Authentication and privacy

- Goal: to prevent unauthorized access & eavesdropping
- Realized by authentication service prior access
- Open system authentication
  - station wanting to authenticate sends **authentication management frame** - receiving station sends back frame for successful authentication
- Shared key authentication (included in WEP*)
  - **Secret, shared key** received by all stations by a separate, 802.11 independent channel
  - Stations authenticate by a shared knowledge of the key properties
- WEP's privacy (blocking out eavesdropping) is based on ciphering:



**WEP: Wired Equivalent Privacy*

802.11b Security Features

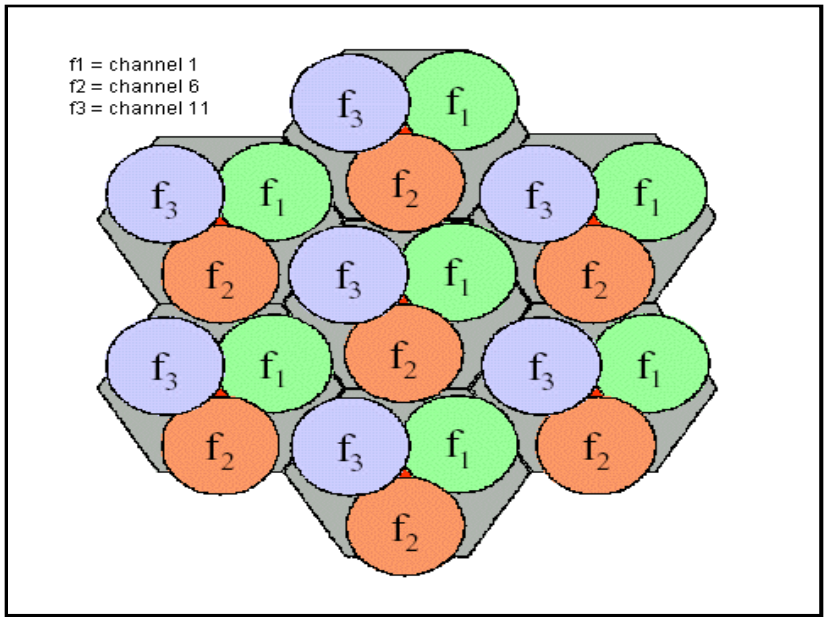
- Wired Equivalent Privacy (**WEP**) – A protocol to protect link-level data during wireless transmission between clients and access points.
- Services:
  - **Authentication**: provides access control to the network by denying access to client stations that fail to authenticate properly.
  - **Confidentiality**: intends to prevent information compromise from casual eavesdropping
  - **Integrity**: prevents messages from being modified while in transit between the wireless client and the access point.

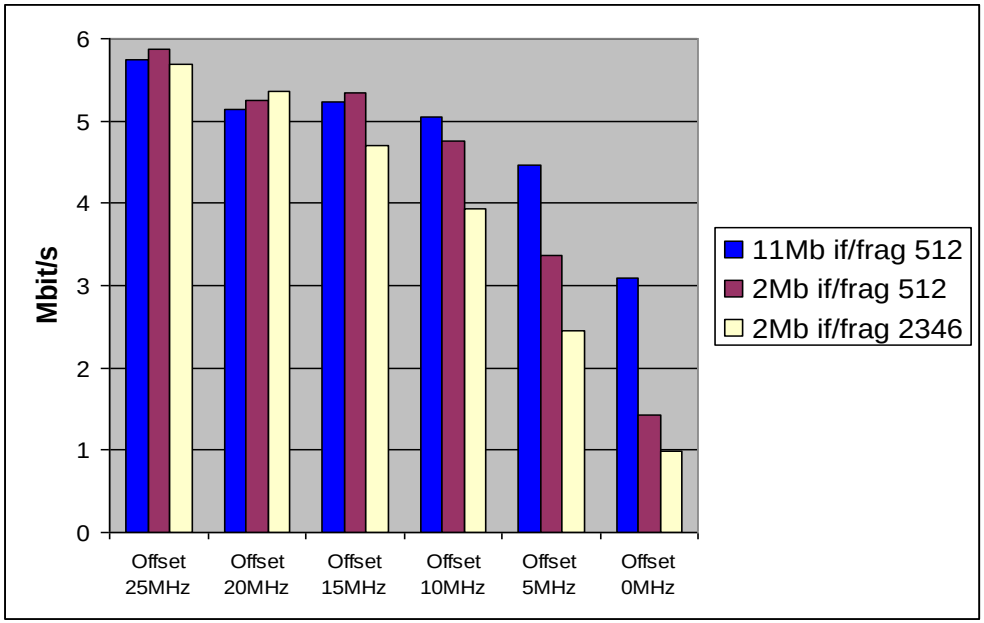
Data Integrity

- Data integrity is ensured by a simple encrypted version of CRC (Cyclic Redundant Check)
- Also vulnerable to some attacks

Frequency planning

- Interference from other WLAN systems or cells
- IEEE 802.11 operates at uncontrolled ISM band
- 14 channels of 802.11 are overlapping, only 3 channels are disjointed. For example Ch1, 6, 11
- Throughput decreases with less channel spacing
- A example of frequency allocation in multi-cell network





WLAN benefits

- Mobility
  - increases working efficiency and productivity
  - extends the On-line period
- Installation on difficult-to-wire areas
  - inside buildings
  - road crossings
- Increased reliability
  - Note: Pay attention to security!
- Reduced installation time
  - cabling time and convenient to users and difficult-to-wire cases

WLAN benefits (cont.)

- Broadband
  - 11 Mbps for 802.11b
  - 54 Mbps for 802.11a/g (GSM:9.6Kbps, HCSCD:~40Kbps, GPRS:~160Kbps, WCDMA:up to 2Mbps)
- Long-term cost savings
  - O & M cheaper that for wired nets
  - Comes from easy maintenance, cabling cost, working efficiency and accuracy
  - Network can be established in a new location just by moving the PCs!

WLAN technology problems

- Date Speed
  - IEEE 802.11b support up to 11 MBps, sometimes this is not enough - far lower than 100 Mbps fast Ethernet
- Interference
  - Works in ISM band, share same frequency with microwave oven, Bluetooth, and others
- Security
  - Current WEP algorithm is weak - usually not ON!
- Roaming
  - No industry standard is available and propriety solution are not interoperable - especially with GSM
- Inter-operability
  - Only few basic functionality are interoperable, other vendor's features can't be used in a mixed network

WLAN implementation problems

- Lack of wireless networking experience for most IT engineer
- No well-recognized operation process on network implementation
- Selecting access points with ‘Best Guess’ method
- Unaware of interference from/to other networks
- Weak security policy
- As a result, your WLAN may have
  - Poor performance (coverage, throughput, capacity, security)
  - Unstable service
  - Customer dissatisfaction