

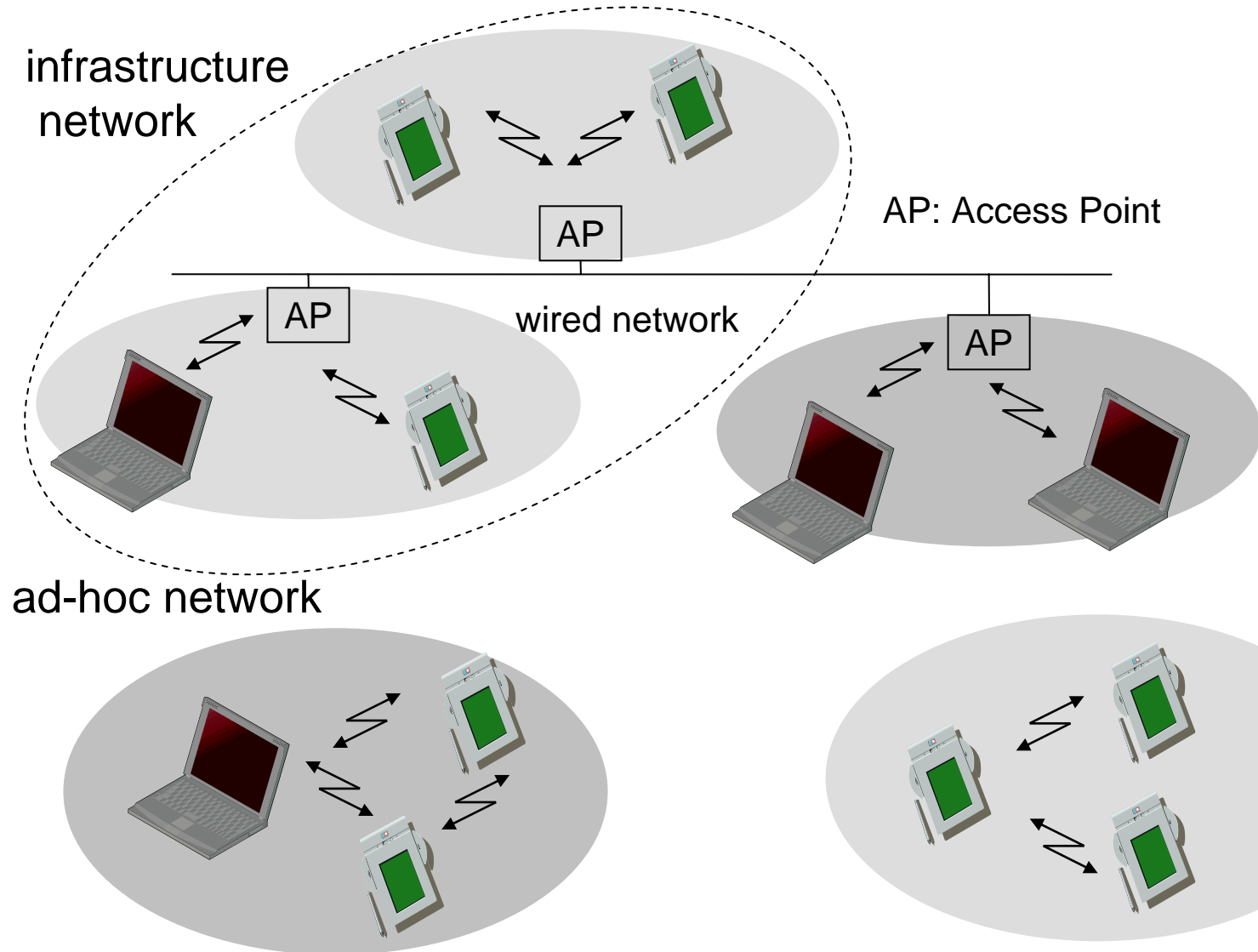
IEEE 802.11 WLANs (WiFi)
Part II/III – System Overview and MAC Layer

Design goals for wireless LANs (WLANs)

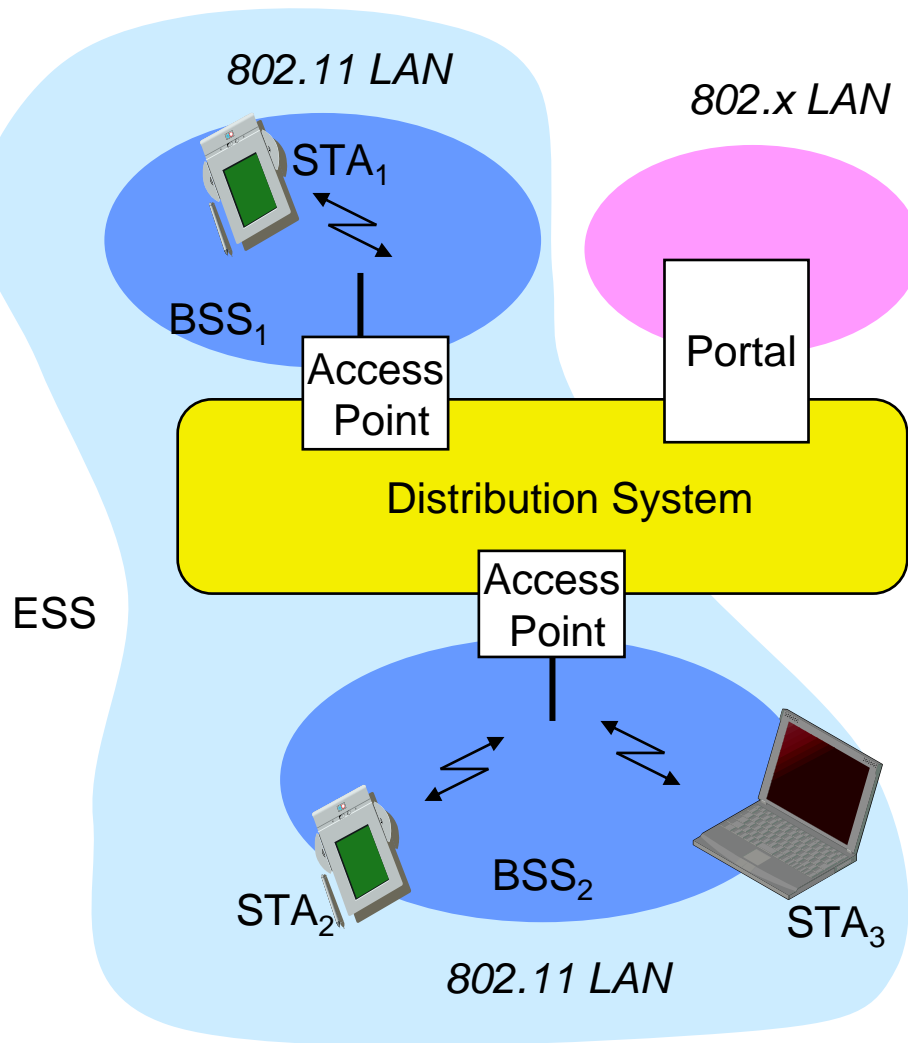
- ◆ Global, seamless operation
- ◆ Low power for battery use
- ◆ No special permissions or licenses needed to use the spectrum for building WLAN (vs. Billions of dollars spent for 3G networks spectrum worldwide)
- ◆ Robust transmission technology
- ◆ Easy to use for everyone, simple management
 - ☞ e.g. Simplified spontaneous cooperation at meetings
- ◆ Protection of investment in wired networks, e.g. compatible with Ethernet
- ◆ Security
 - ☞ no one should be able to read my data,
 - ☞ no one should be able to collect user profiles
- ◆ Safety (low radiation)
- ◆ Transparency concerning applications and higher layer protocols

Part II – WiFi System Overview

Comparison: Infrastructure vs. Ad-hoc networks

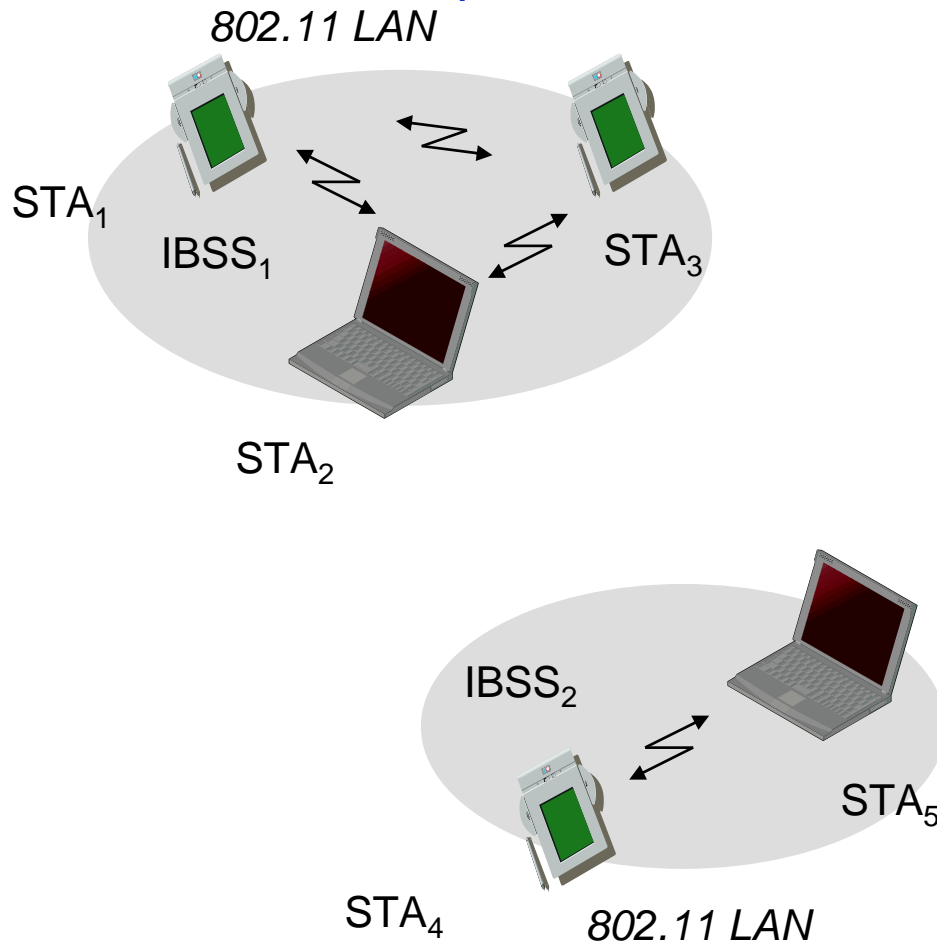


802.11 - Architecture of an Infrastructure network and terminology



- **Station (STA)**
 - ◆ terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Access Point (or Base Station)**
 - ◆ station integrated into the wireless LAN and the distribution system
- **Basic Service Set (BSS)**
 - ◆ group of stations using the same radio frequency (channel)
- **Distribution System**
 - ◆ interconnection network for multiple BSSes to form one logical network, the so-called
- **Extended Service Set (ESS)**
- **Portal**
 - ◆ Bridge/Gateway to other (wired) networks

802.11 - Architecture of an ad-hoc (infrastructureless) network



- Station (STA): terminal with access mechanisms to the wireless medium
- **Independent** Basic Service Set (**IBSS**): group of stations using the same radio frequency
- No Access Points, every STA is equal
- Direct (single-hop) communication within a limited range ; i.e. no multi-hop routing

WLAN: IEEE 802.11b

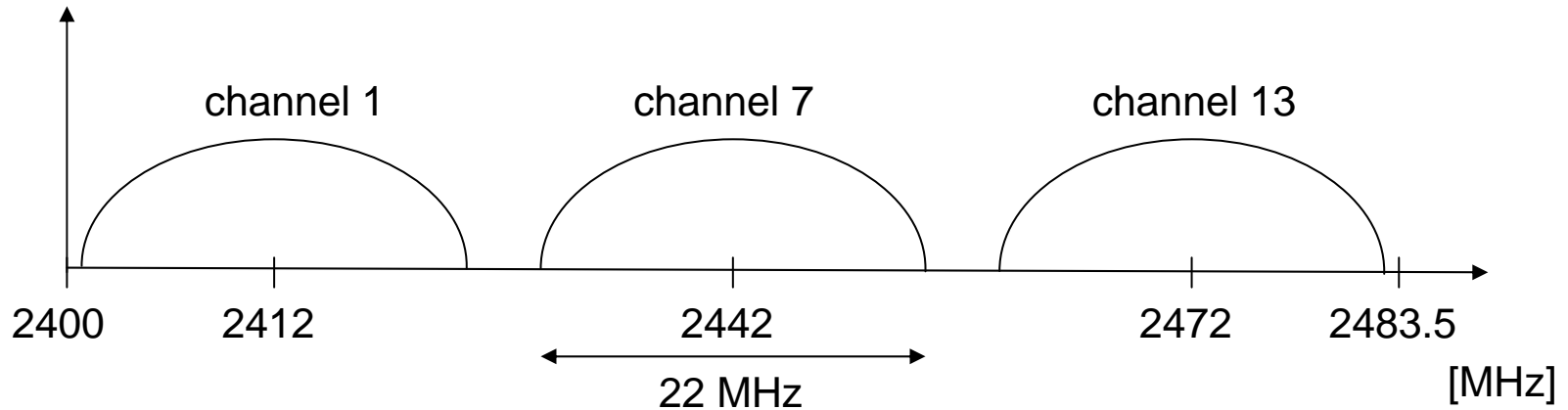
- Data rate
 - ◆ 1, 2, 5.5, 11 Mbit/s, depending on SNR
 - ◆ User data rate max. approx. 6 Mbit/s
 - ◆ direct sequence spread spectrum (DSSS) in physical layer
- Transmission range
 - ◆ 300m outdoor, 30m indoor
 - ◆ Max. data rate ~10m indoor
- Frequency
 - ◆ Free 2.4 GHz ISM (**Unlicensed**)-frequency band
- Security standards
 - ◆ WEP insecure, WPA, WPA2, 802.11i, SSID
- Cost
 - ◆ Adapter/ Access Point price keep dropping
- Availability
 - ◆ Many products, many vendors
- Quality of Service
 - ◆ Best effort, no guarantees (unless polling is used, limited support in real products)
- Manageability
 - ◆ Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
 - ◆ Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
 - ◆ Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

802.11: Channels, association

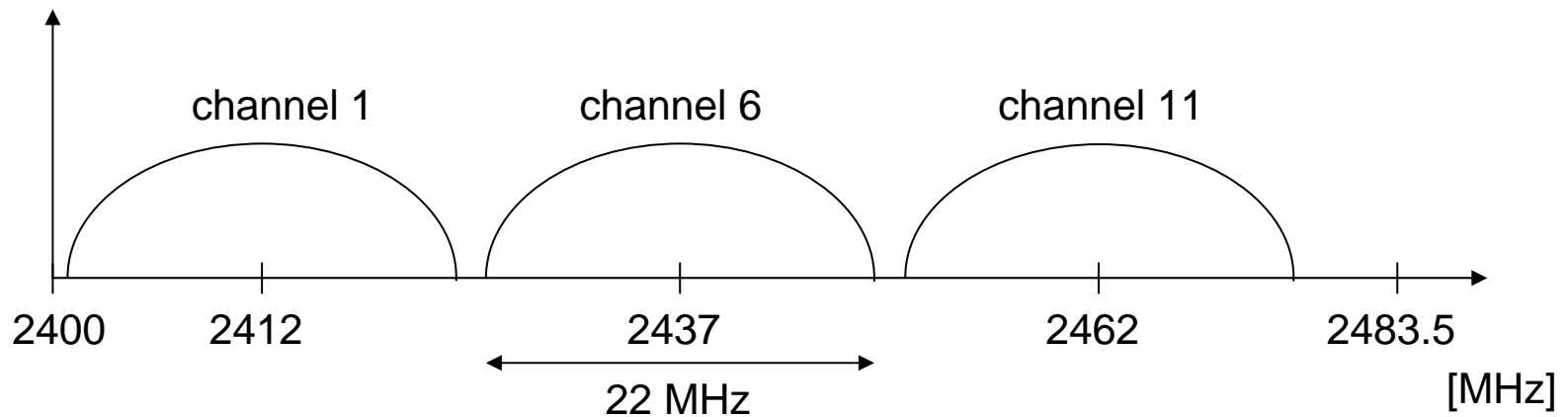
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies ;
 - ◆ Actually quite few of the 11 channels are totally non-overlapped
 - ◆ Network administrator chooses frequency for each AP
 - ◆ Interference possible: channel can be same as that chosen by neighboring AP!
 - ☞ Better to have frequency assignment planning
- Station STA (or host): must first *authenticate* and then *associate* with an AP before it can start transmitting data
- How a STA get started ?
 - ◆ The STA scans channels, listening for *beacon frames* containing the ESS's name (SSID) and the MAC address of the AP (BSSID)
 - ◆ selects AP to associate with
 - ◆ may perform authentication before association
 - ◆ After association is done, STA will typically run DHCP to get IP address in AP's IP subnet (if STA does not have an IP addr already, or if it has moved to a new IP subnet)

Channel selection for 802.11b (non-overlapping)

Europe (ETSI)



US (FCC)/Canada (IC)



Other IEEE 802.11 Wireless LAN Standards

■ 802.11a

- ◆ 5-6 GHz range
 - ◆ up to 54 Mbps
 - ◆ Disadvantages:
 - ☞ stronger shading due to higher frequency
 - ☞ Using different frequency ranges than 802.11b => extra hardware to support dual mode of 802.11a or 802.11b
- => Bad for backward compatibility

■ 802.11g

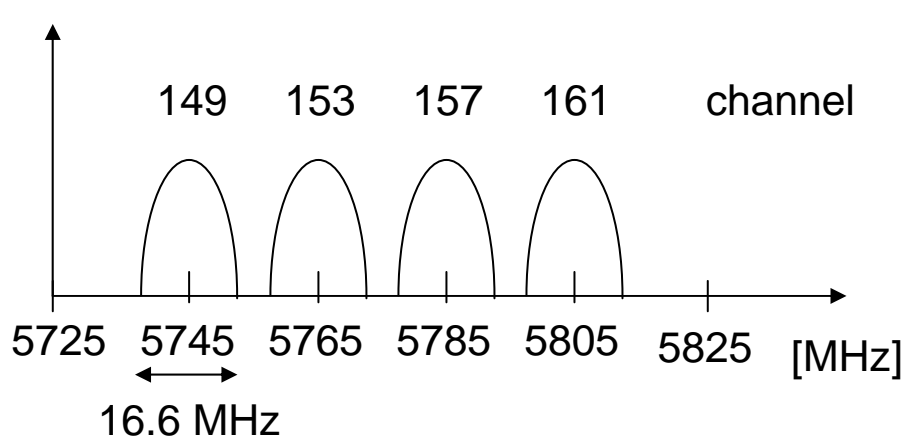
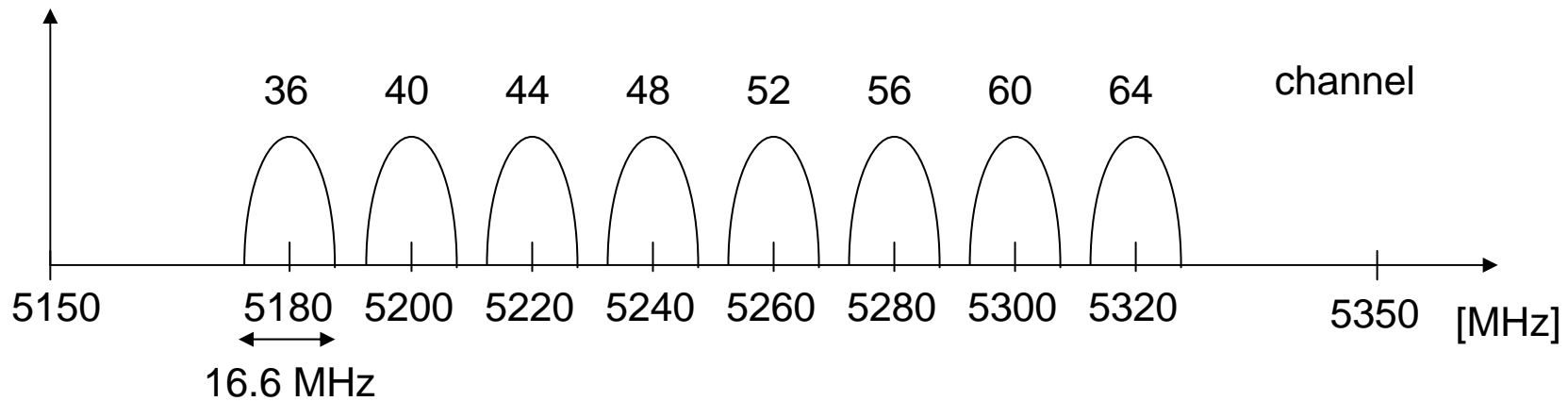
- ◆ 2.4-5 GHz range
 - ☞ Backward compatible with 802.11b
- ◆ up to 54 Mbps

■ 802.11a and 802.11g use OFDM in physical layer

■ All use CSMA/CA for multiple access

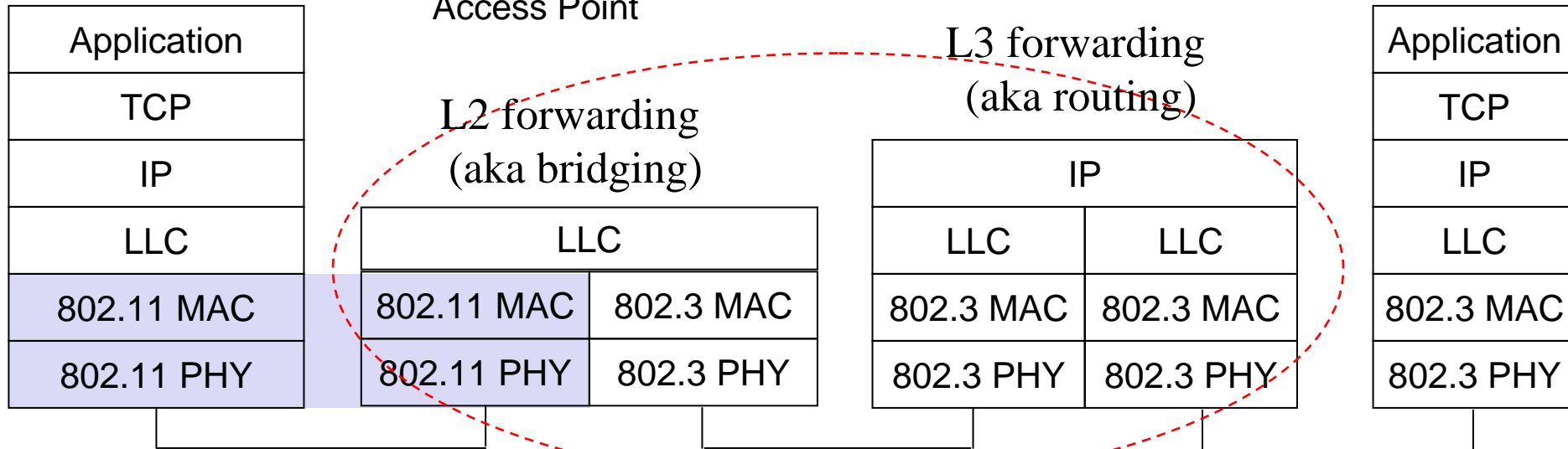
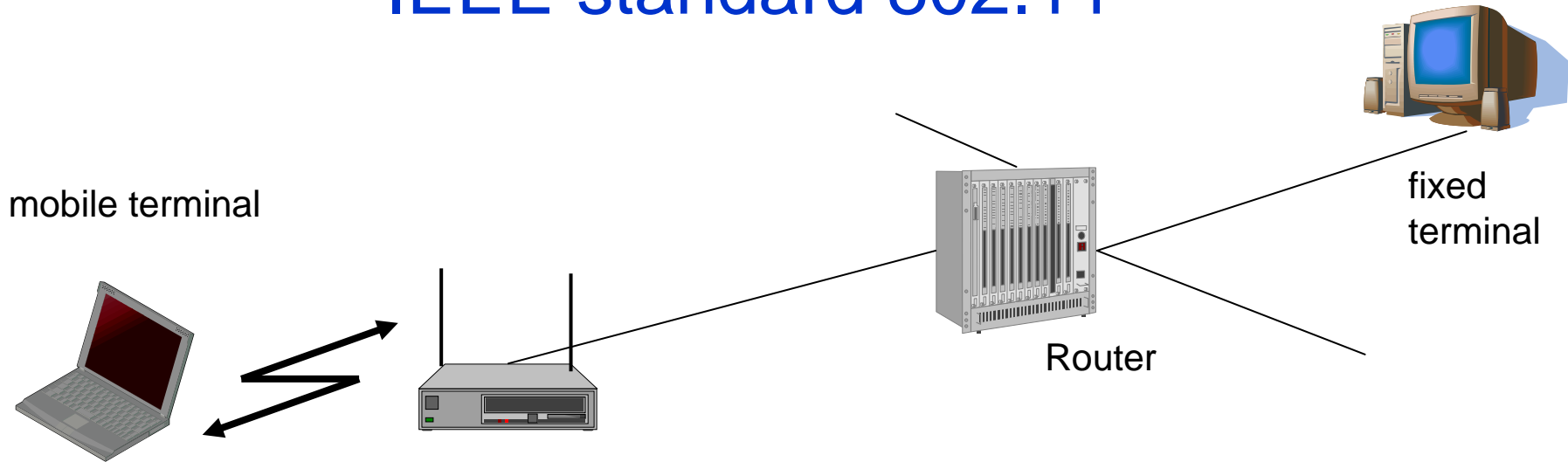
■ All support AP (base-station), (infrastructure) and ad-hoc network modes

Operating channels for 802.11a / US



center frequency =
 $5000 + 5 \times \text{channel number}$ [MHz]

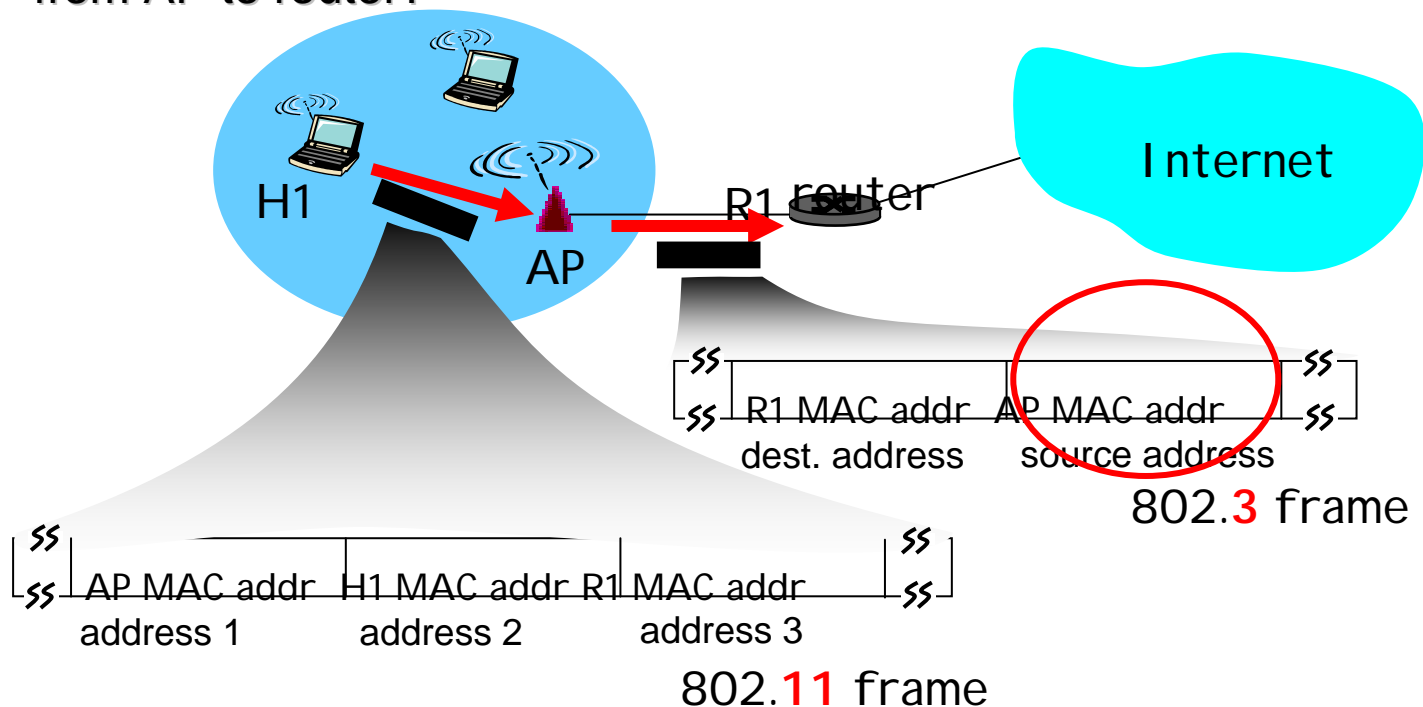
IEEE standard 802.11



Most consumer-focused home wireless routers
merge the functions of the AP and Router

IEEE 802.11 Operations

- Question 1) In the protocol stack of the Wi-Fi client, there are two layers which has packet retransmission function (MAC layer and TCP layer). Why we need two layers at the Wi-Fi client doing the same retransmission function?
- Question 2) What should be the source address of the Ethernet packet from AP to router?

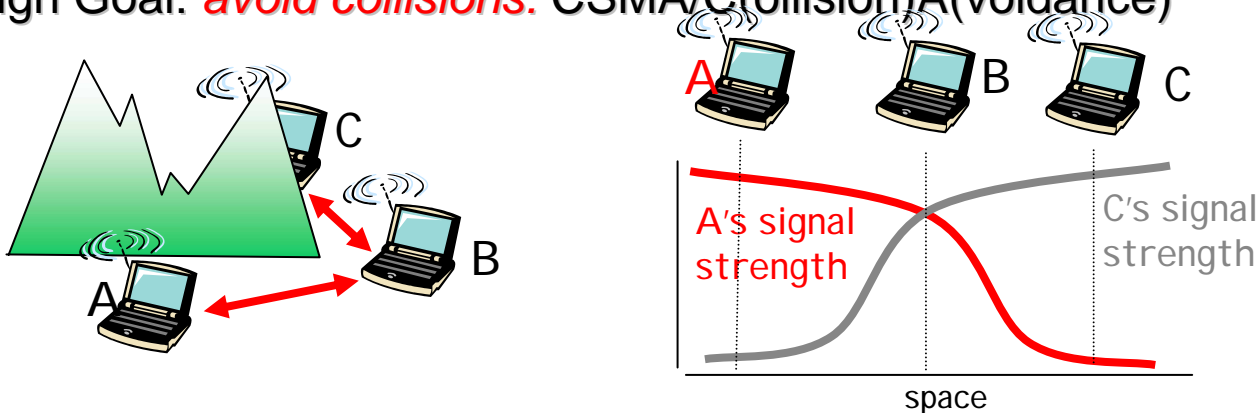


Part III – MAC Layer Overview

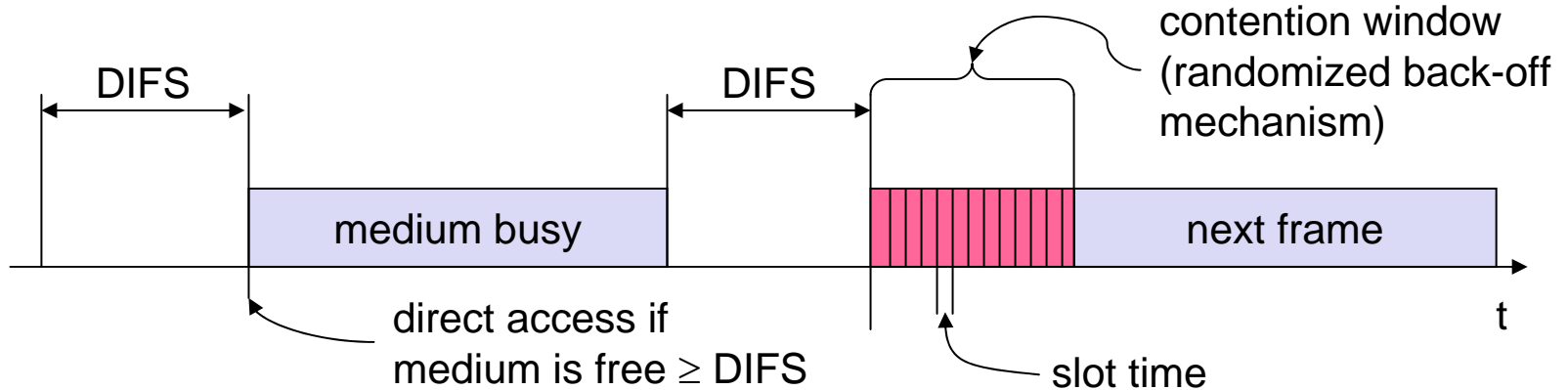
IEEE 802.11 Multiple Access Control (MAC)

- 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) and transmitting at the same time because (TDD operation)
 - ☞ transmission and reception are at the same frequency
 - => the station's receiver's will be overwhelming by it's own transmitting signals and thus can't hear the relatively "weak" signals sent by the others
- ◆ In general can't sense all collisions anyway, e.g. **The Hidden terminal problem**

=> Design Goal: **avoid collisions**: CSMA/C(ollision)A(avoidance)



802.11 MAC CSMA/CA access method

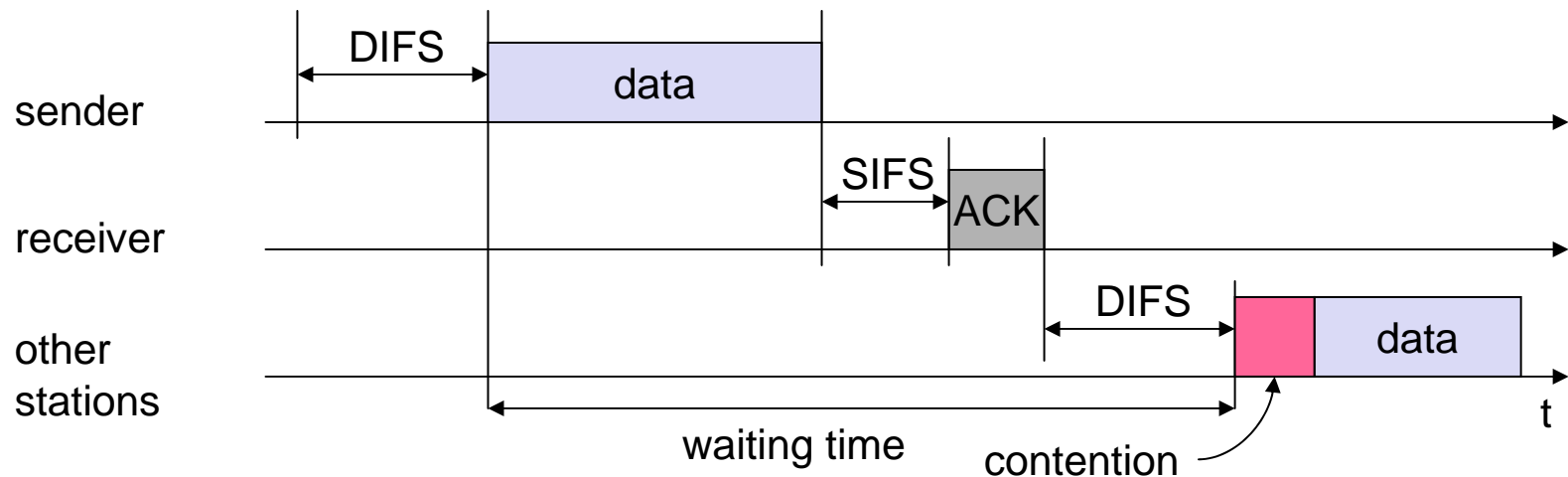


- ◆ station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- ◆ if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- ◆ if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- ◆ if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

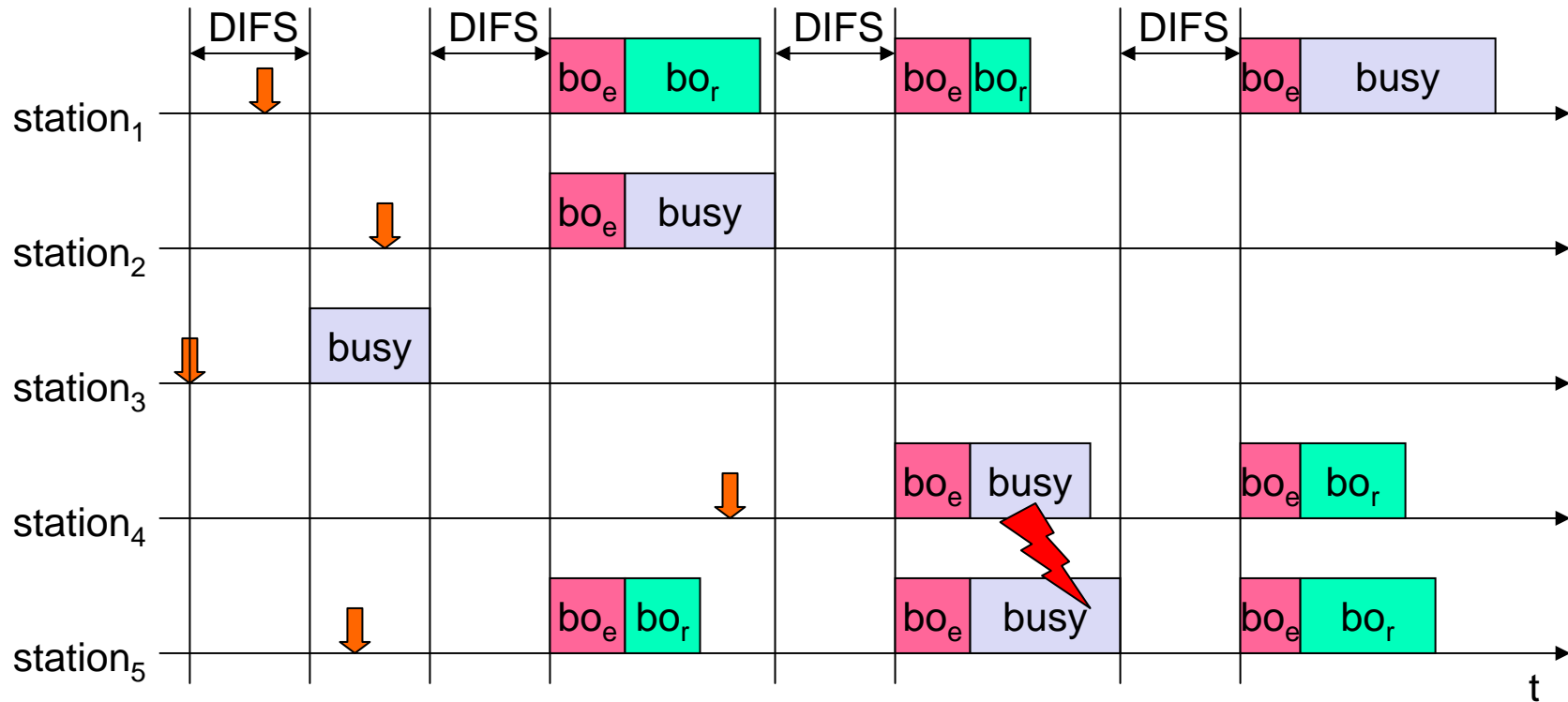
802.11 MAC CSMA/CA access method (cont'd)

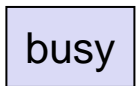
■ Sending unicast packets


- ◆ station has to wait for DIFS before sending data
- ◆ receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- ◆ automatic retransmission of data packets in case of transmission errors





802.11 - competing stations - simple version



 busy medium not idle (frame, ack etc.)

 packet arrival at MAC

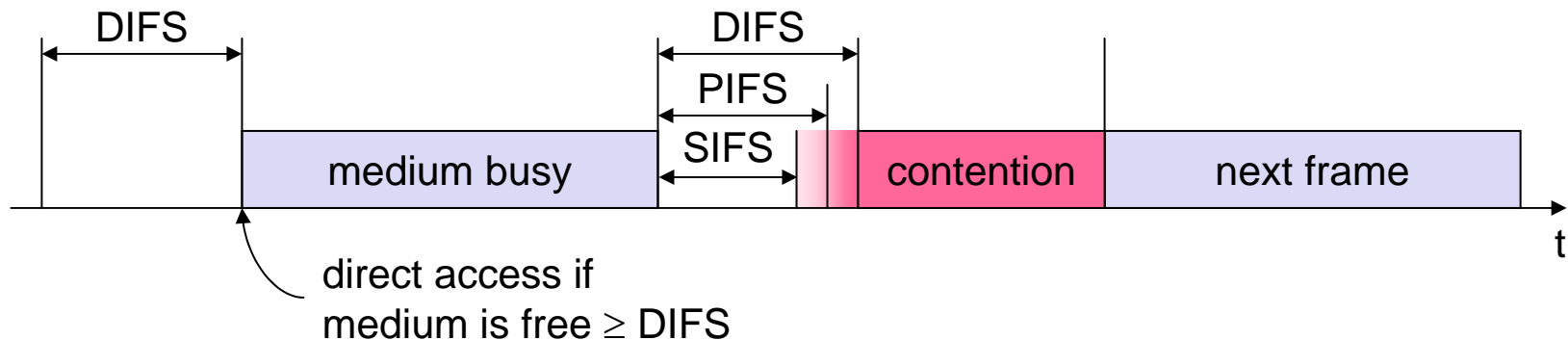
 bo_e elapsed backoff time

 bo_r residual backoff time

802.11 - MAC layer (cont'd)

■ Priorities

- ◆ defined through different inter frame spaces (IFS)
- ◆ no guaranteed, hard priorities
- ◆ SIFS (Short Inter Frame Spacing)
 - ☞ highest priority, for ACK, CTS, polling response
- ◆ PIFS (PCF IFS)
 - ☞ medium priority, for time-bounded service using PCF
- ◆ DIFS (DCF, Distributed Coordination Function IFS)
 - ☞ lowest priority, for asynchronous data service



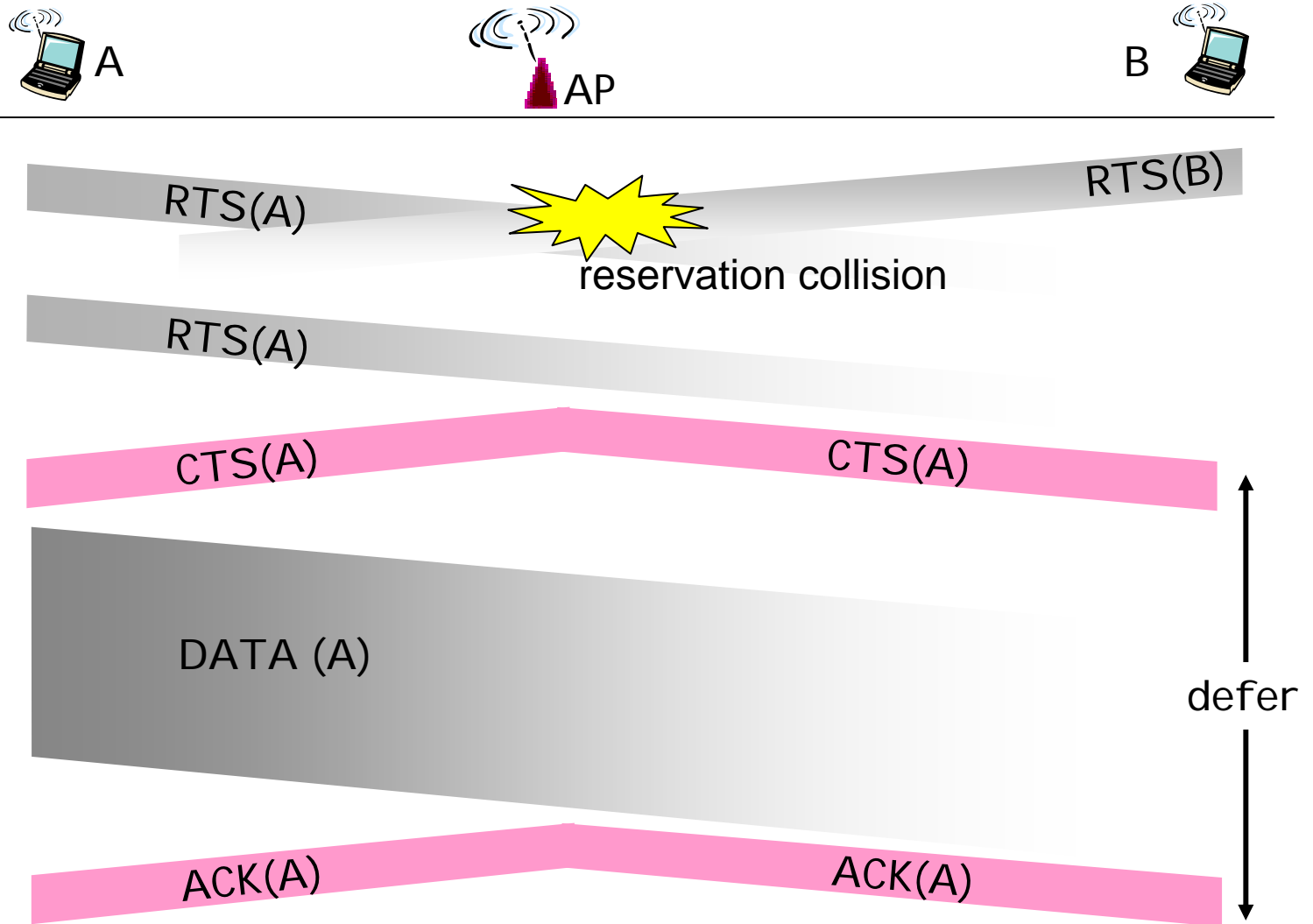
To Further Avoiding collisions

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
- RTS 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



More Details on 802.11 MAC, aka DFWMAC (Distributed Foundation Wireless MAC)

Traffic services

- Asynchronous Data Service (**mandatory**)
 - ◆ exchange of data packets based on “best-effort”
 - ◆ support of broadcast and multicast
- Time-Bounded Service (**optional, seldom implemented by real products**)
 - ◆ implemented using PCF (Point Coordination Function)

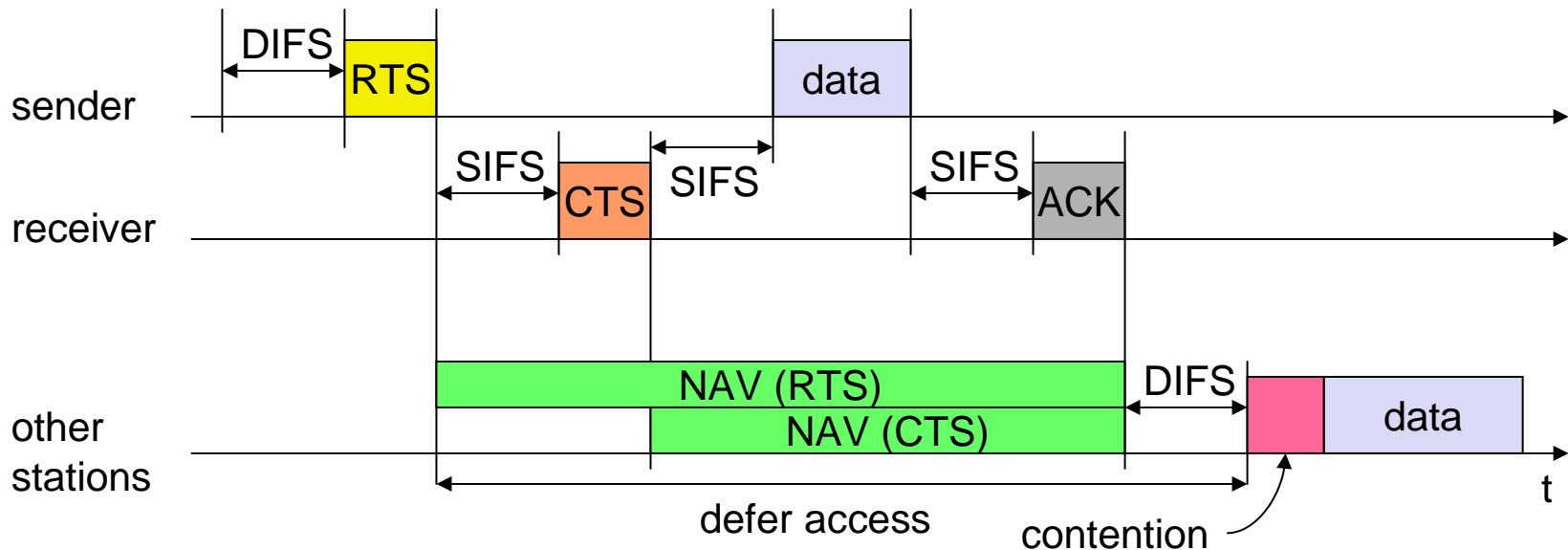
Access methods

- DFWMAC-DCF CSMA/CA (**mandatory**)
 - ◆ Basic collision avoidance via randomized “back-off” mechanism
 - ◆ minimum distance between consecutive packets
 - ◆ ACK packet for acknowledgements (**NO ACK for broad/multicasts**)
- DFWMAC-DCF with RTS/CTS (**optional**)
 - ◆ Distributed Foundation Wireless MAC
 - ◆ avoids hidden terminal problem
- DFWMAC- PCF (**optional, seldom implemented by products**)
 - ◆ access point polls terminals according to a list

802.11 – DFWMAC RTS/CTS

Sending unicast packets

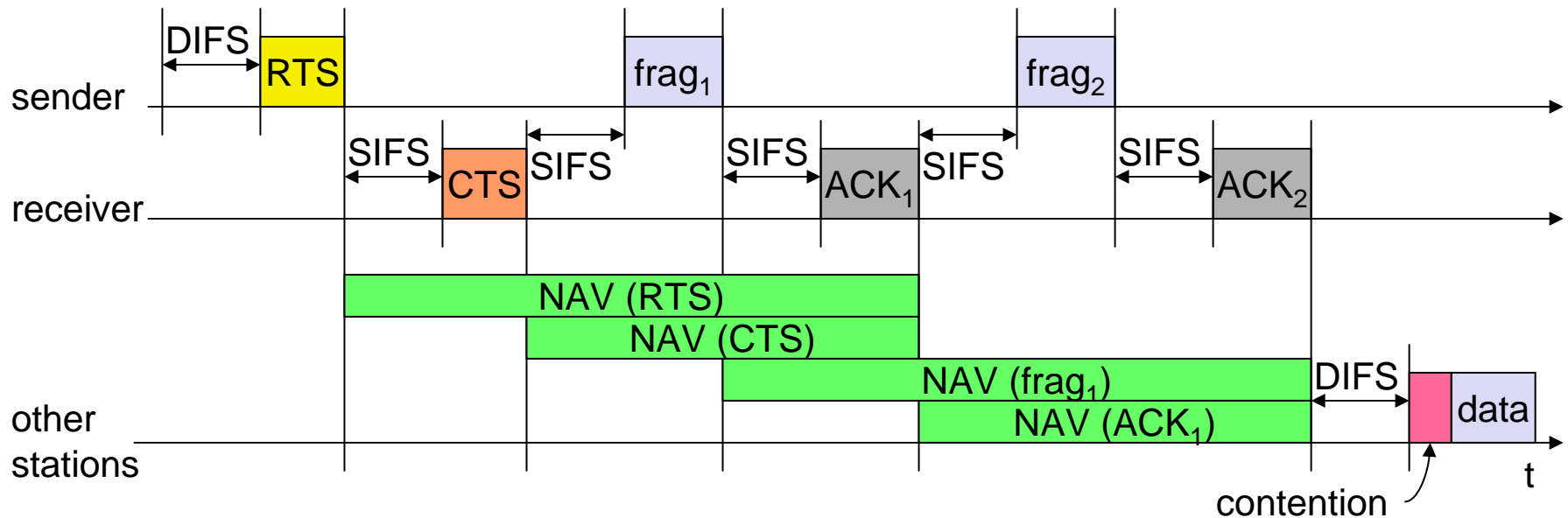
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data after SIFS, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



NAV = Network Allocation Vector ; to enable “**Virtual Carrier Sensing**”

Virtual Carrier Sensing: the sender tells others how long it will be using the channel by setting the value of NAV => others don't need to keep on sensing till then

Fragmentation: to send a Big data frame in multiple pieces

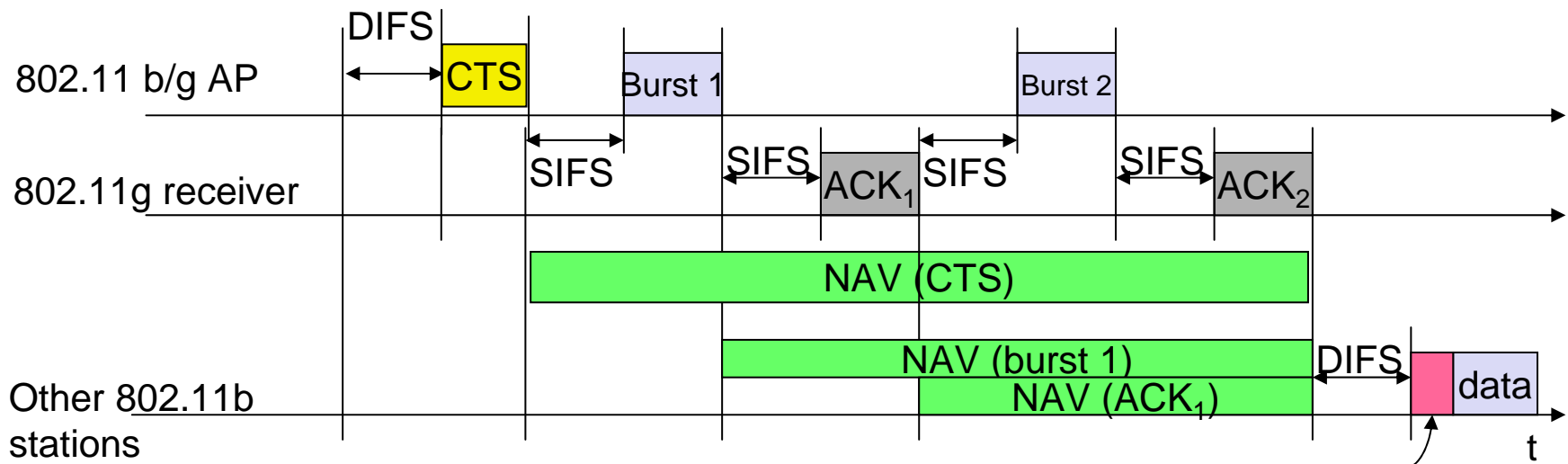


Why Fragmentation ?

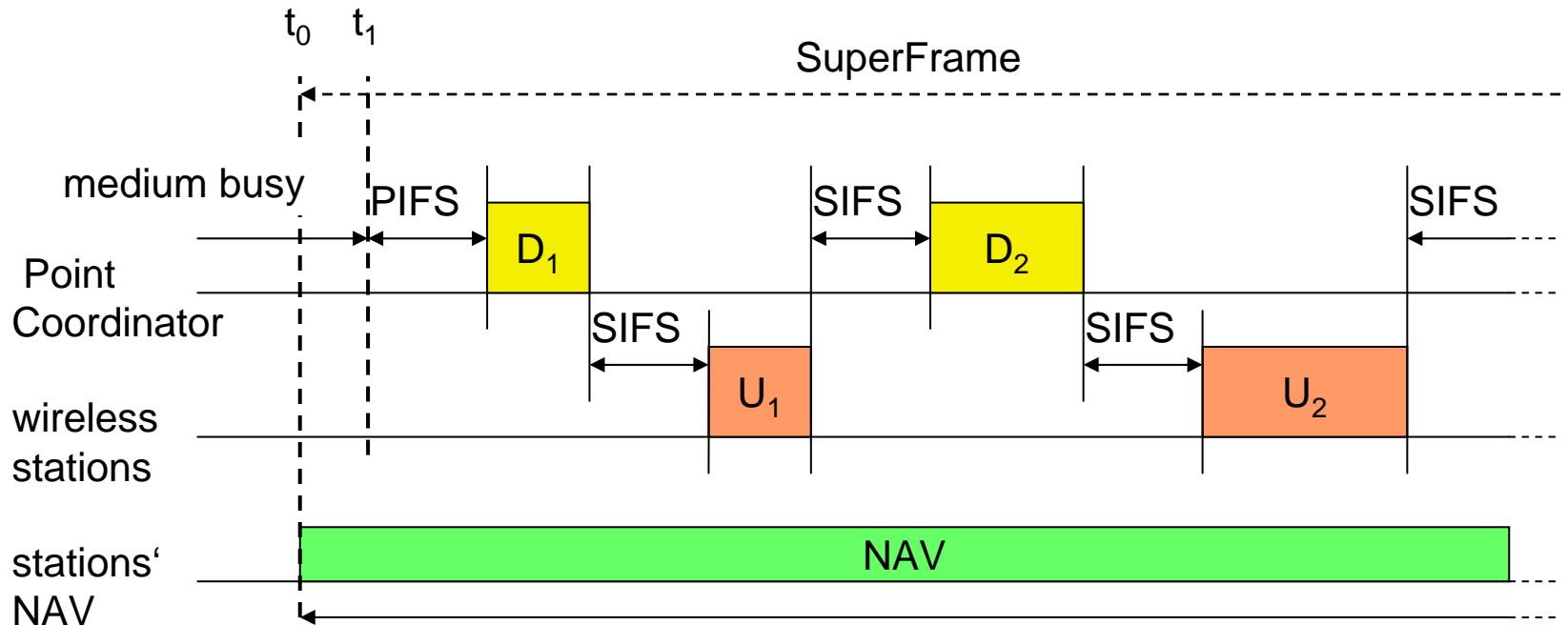
- May be due to L2 limit on maximum frame-size of data sent each time ;
- The bigger a frame, the more vulnerable it is in getting a bit transmission error ; A single error-bit can ruin the whole frame and require re-transmission of the whole frame => better off to send/retransmit small fragments instead

Burst Mode for mixing .11g/.11g clients

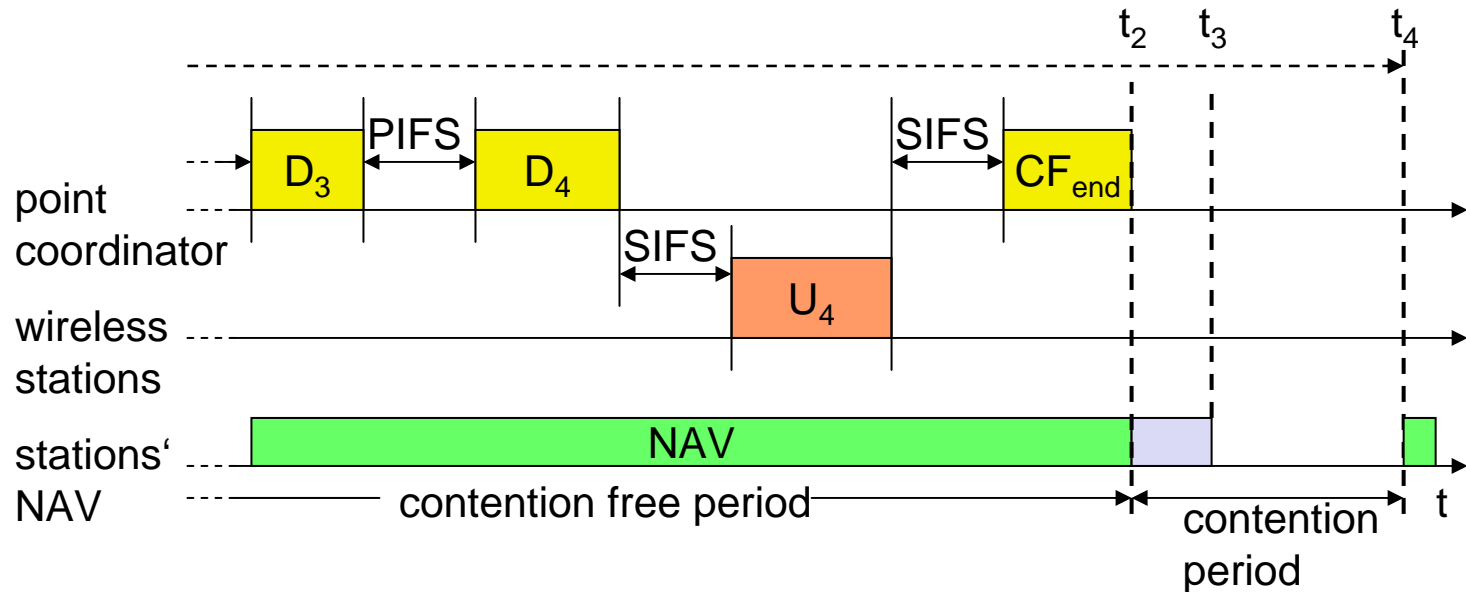
- For backward compatibility, the 802.11g packets have a mode that support 802.11b preamble. This is needed to allow other 802.11b clients to carrier sense channel busy while 802.11g clients are transmitting.
- However, this makes the actual throughput of 802.11g clients pretty low (despite 54Mbps physical transmission rate for payload) because of huge overhead involved in the 802.11b preamble (56us / 128us).
- To allow more efficient mixing of 802.11b/g clients, a b/g compatible AP can use the RTS/CTS for bursting traffic to g clients.
 - ◆ b/g AP sends CTS with NAV → trying to reserve the media for a specified period of time. → all devices (b/g) observe the NAV and remains silence.
 - ◆ b/g AP then sends the 11g packets (with g-preamble) to the intended g clients one by one. → the g-packet transmission has less overhead due to much shorter preamble.



DFWMAC-Point Coordination Function (PCF)



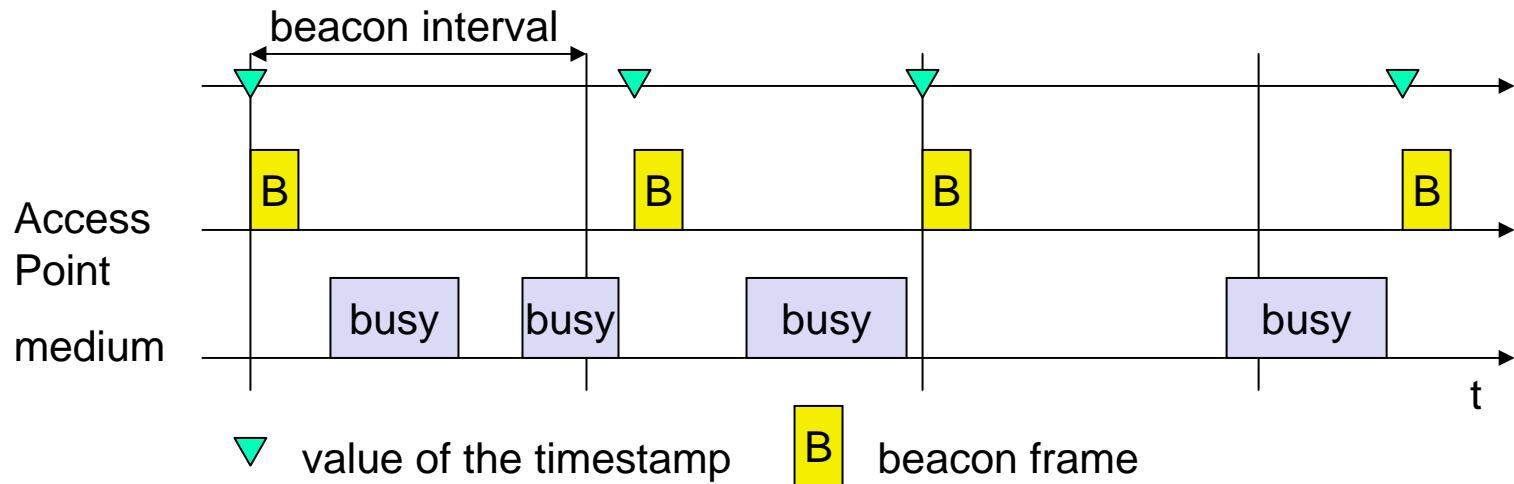
DFWMAC-PCF (cont'd)



Note:

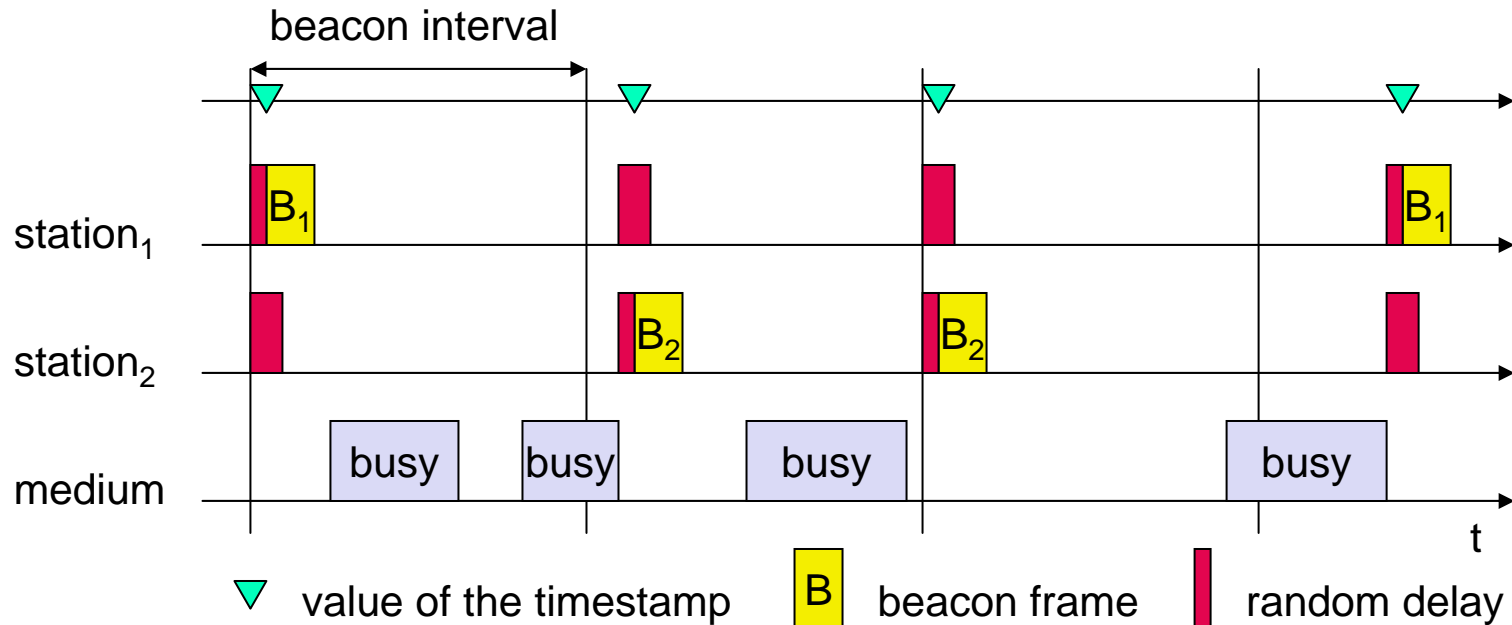
Since $SIFS < PIFS$, if User 3 has something to send, it would have done so before the Point coordinator's waiting period of PIFS is over ; not hearing from user 3 by then means the Point coordinator can safely proceed to User 4

Synchronization using a Beacon (infrastructure)



- The AP broadcasts a “Beacon” message periodically which contains the reference time-stamp value ;
- Each station adjusts/tunes its local clock using the value of the time-stamp in the Beacon as the reference.

Synchronization using a Beacon in an Ad-hoc Network (i.e. No AP)



For each station:

(1) Set a random delay timer ;

(2) If a Beacon from another station is received before timer expires
Adjust local clock using time-stamp in the received Beacon as reference

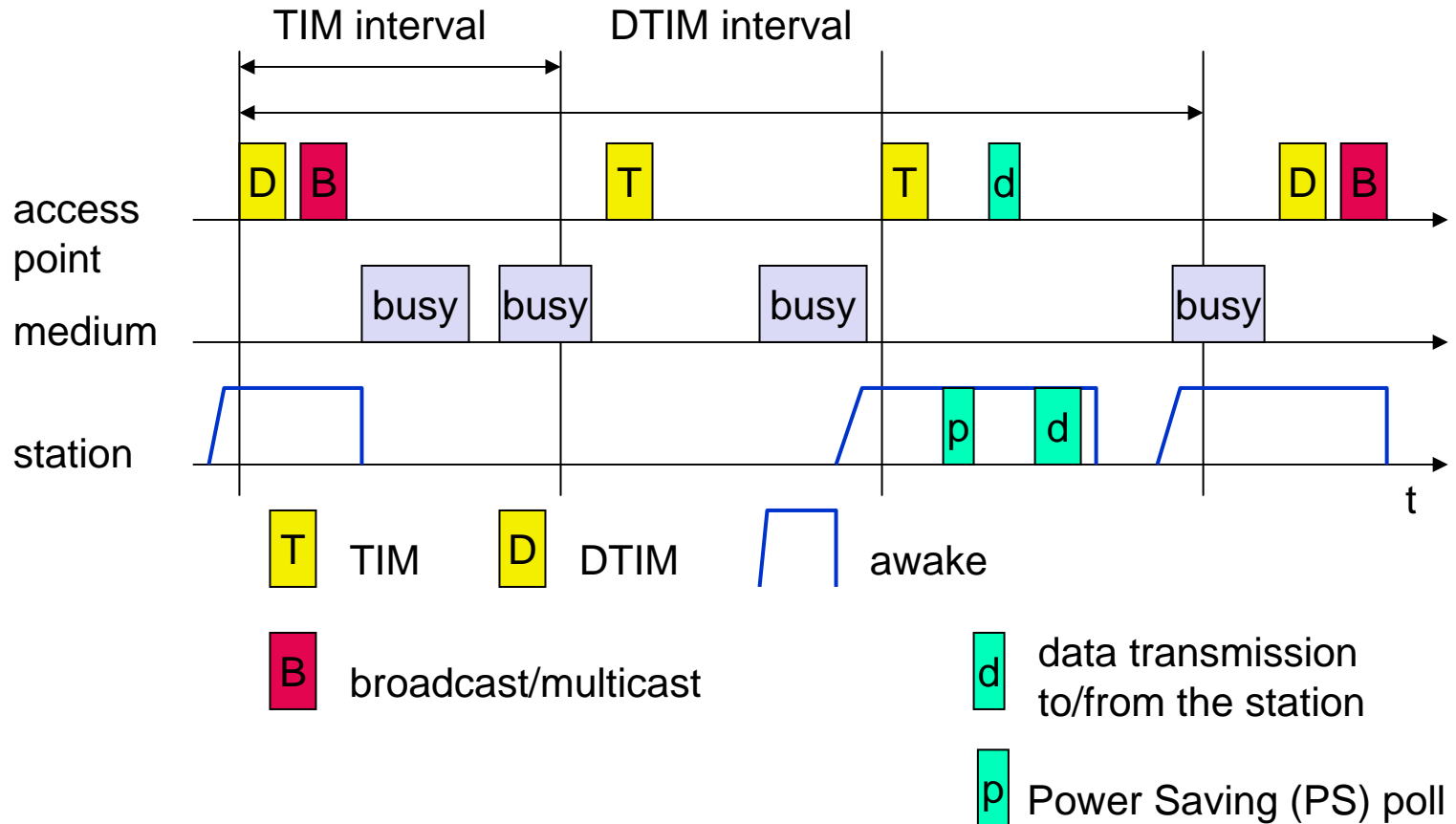
else (i.e. no Beacon from others heard before timer expires)

Upon timer expires, broadcast a Beacon using local clock to generate the time-stamp ; (to be used by all other stations as time reference)

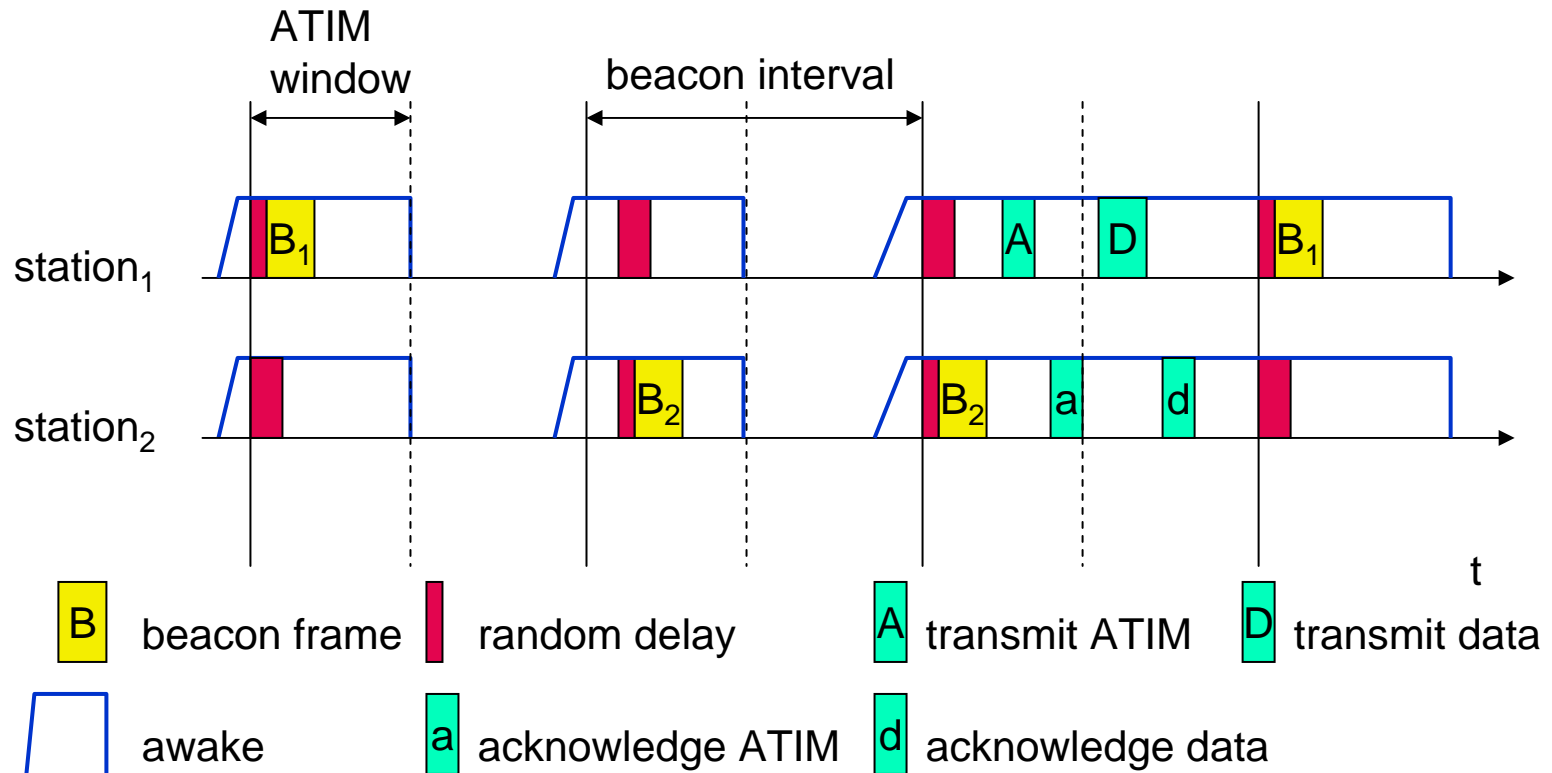
Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF) (see previous 2 pages)
 - ◆ stations wake up at the same time
- Infrastructure
 - ◆ Traffic Indication Map (TIM)
 - ☞ list of unicast receivers transmitted by AP
 - ☞ When unicast receiver wakes up and hear it has incoming frames buffered by the AP, it sends PS-poll to AP to ask for delivery
 - ◆ Delivery Traffic Indication Map (DTIM)
 - ☞ list of broadcast/multicast receivers transmitted by AP
 - ☞ Unicast Polling mechanism does not work for Multicast/Broadcast from AP ; instead, it's each STA's responsibility to wait up every "DTIM-interval" to check for Multicast/Broadcast from AP
- Ad-hoc
 - ◆ Ad-hoc Traffic Indication Map (ATIM)
 - ☞ announcement of receivers by stations buffering frames
 - ☞ more complicated - no central AP
 - ☞ collision of ATIMs possible (scalability?)

Power saving with wake-up patterns (infrastructure)



Power saving with wake-up patterns (ad-hoc)



802.11 - Frame format

Types

- ◆ control frames (e.g. RTS, CTS, ACK, PS-poll), management frames (ATIM, association, authentication, etc), data frames

Sequence numbers

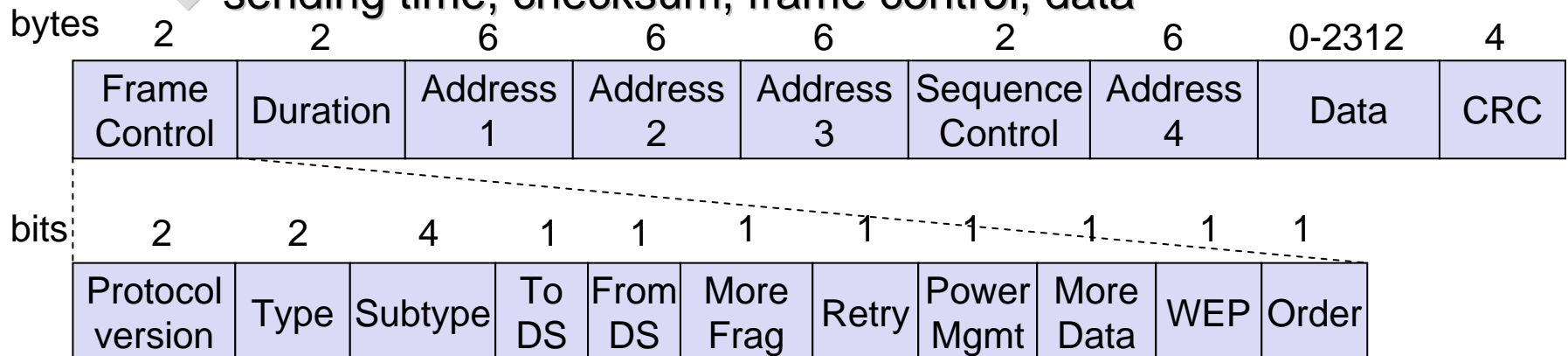
- ◆ important against duplicated frames due to lost ACKs

Addresses

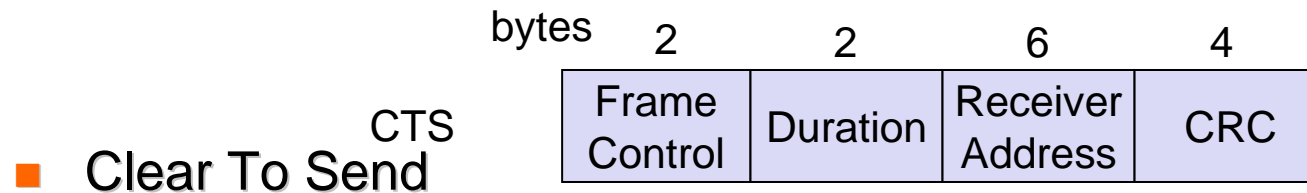
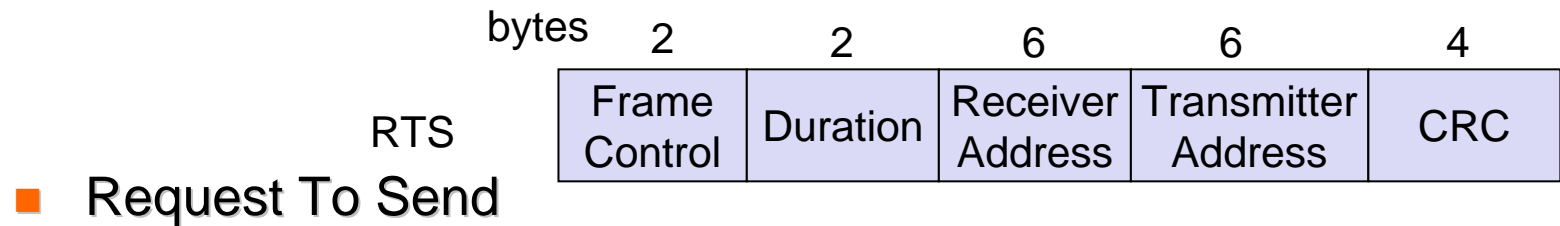
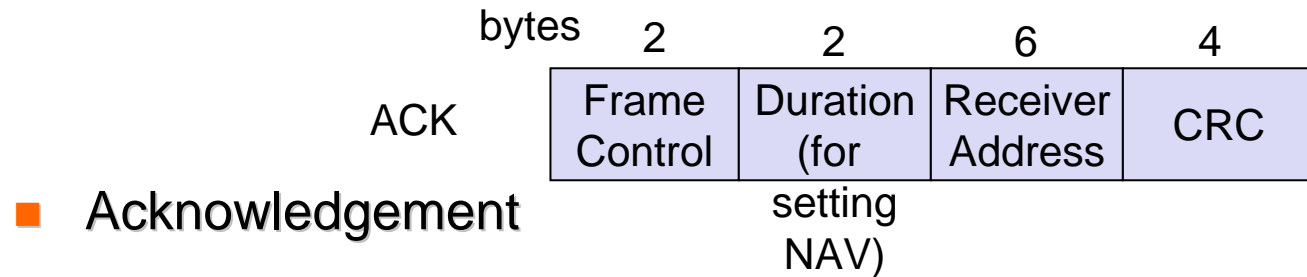
- ◆ receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous

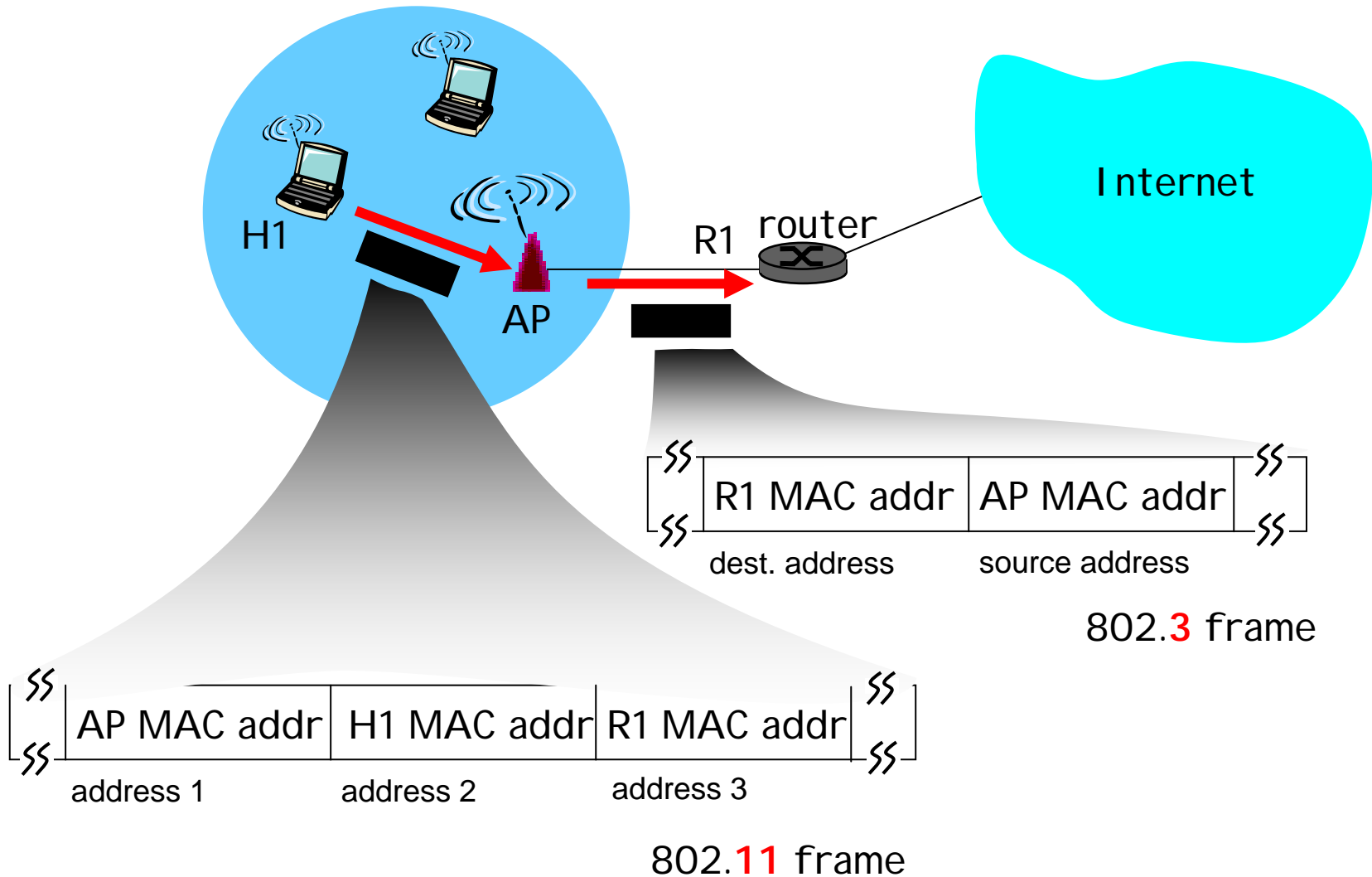
- ◆ sending time, checksum, frame control, data



Special Frames: ACK, RTS, CTS



802.11 frame: addressing



Why can't 802.11 WLAN just use 2 addresses per frame like wired Ethernet ?

MAC address format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System

AP: Access Point

DA: Destination Address

SA: Source Address

BSSID: Basic Service Set Identifier (= MAC address of the AP)

RA: Receiver Address

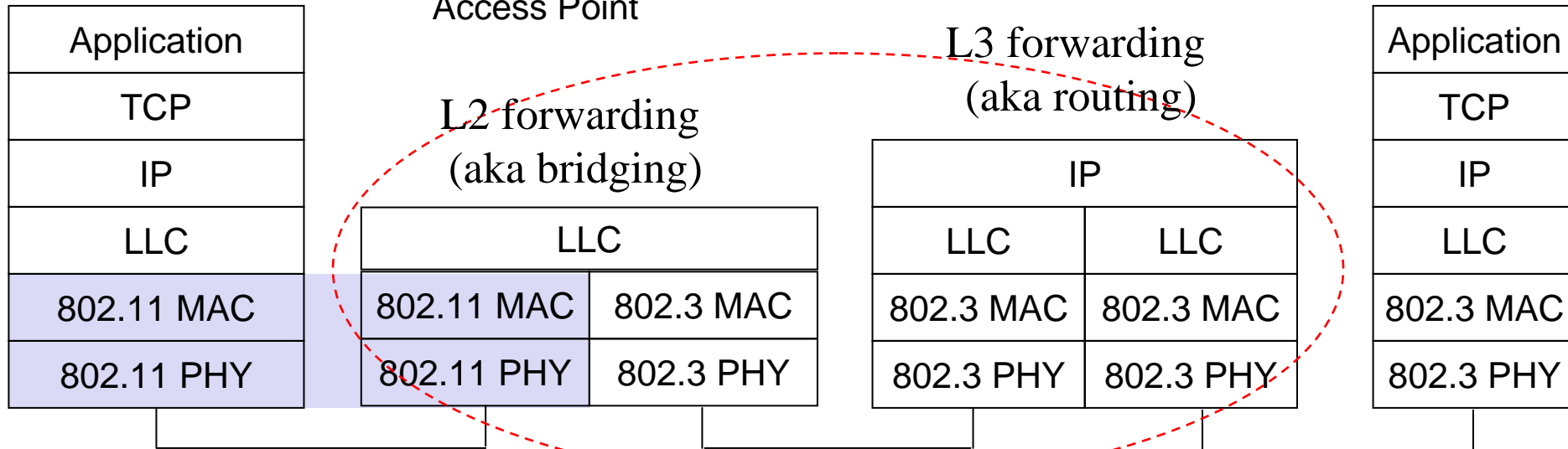
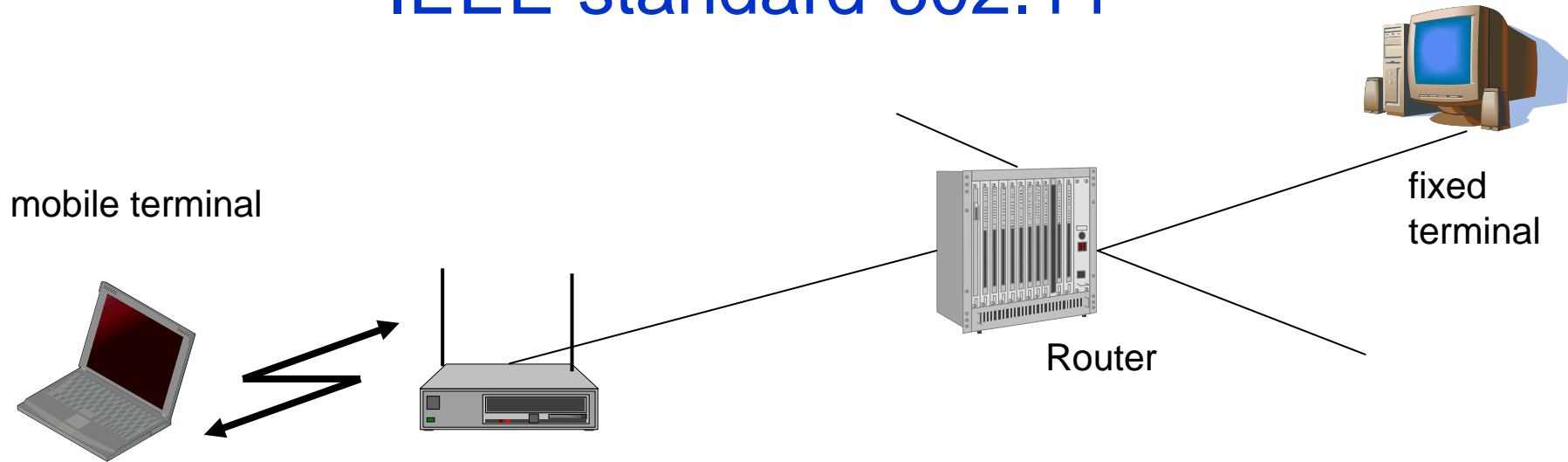
TA: Transmitter Address

Digression to IP addressing
and L3 vs L2 forwarding

Review on Naming and Addressing and Translation Mechanisms

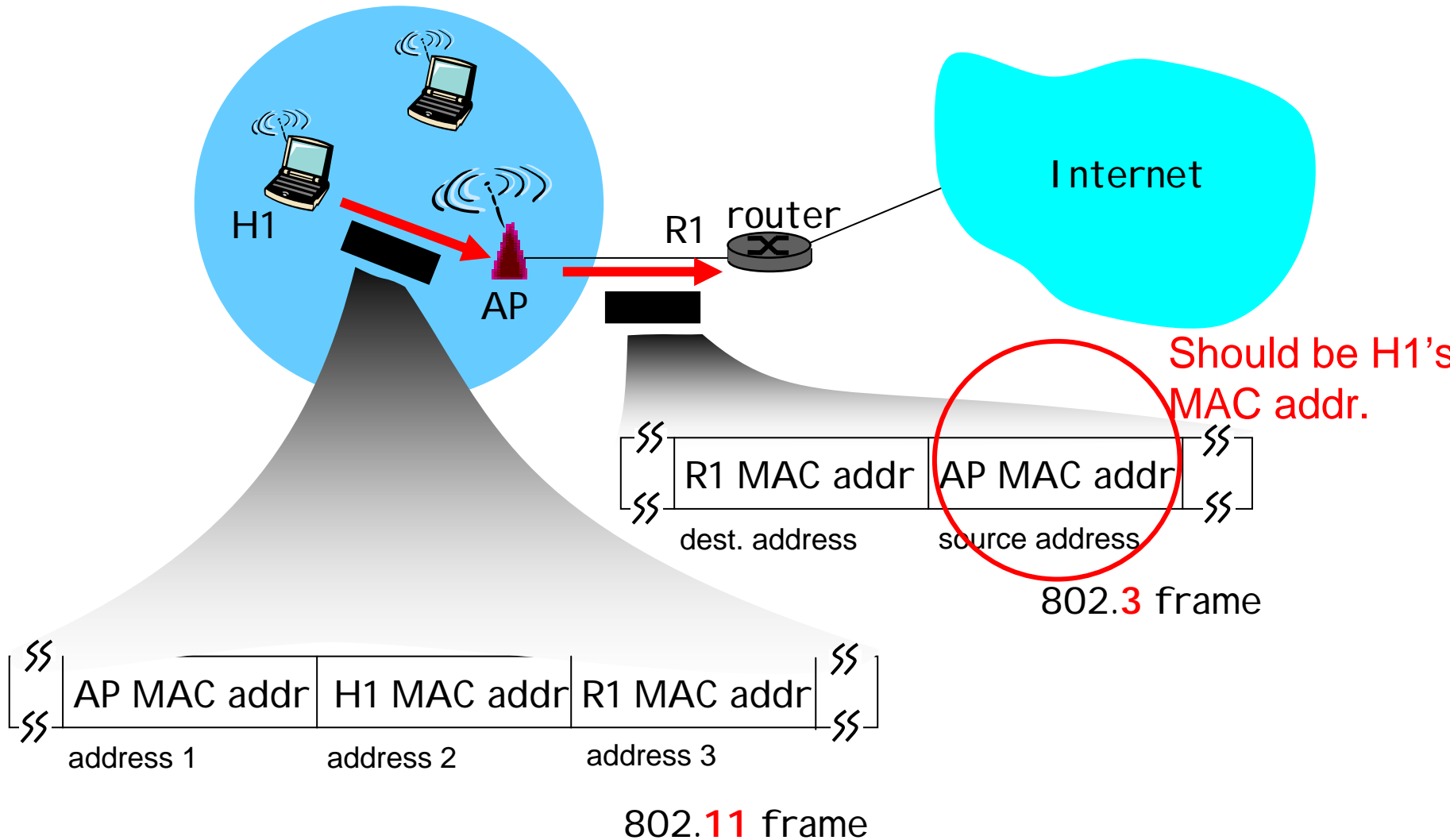
- Given the **Domain-name** of the destination host, e.g. www.ee.ust.hk, the end-host ask an Domain Name System (DNS) server to translate it to an **IP address**, e.g. 128.83.50.156
- This **IP address** is put into the destination IP address field of the packets sent to the destination host ; this destination IP address is used for routing table lookup along the path
- When the packet arrives at the “destination network” (the destination IP subnet), e.g. the LAN segment connected to the destination host, the last-hop router use the **Address Request Protocol (ARP)** to translate the **destination IP address** to the **MAC address** of the ethernet network interface card (NIC) on the destination host
- This MAC address is used as the destination address to deliver the Ethernet frame to the destination host **via L2 forwarding**

IEEE standard 802.11



Most consumer-focused home wireless routers
merge the functions of the AP and Router

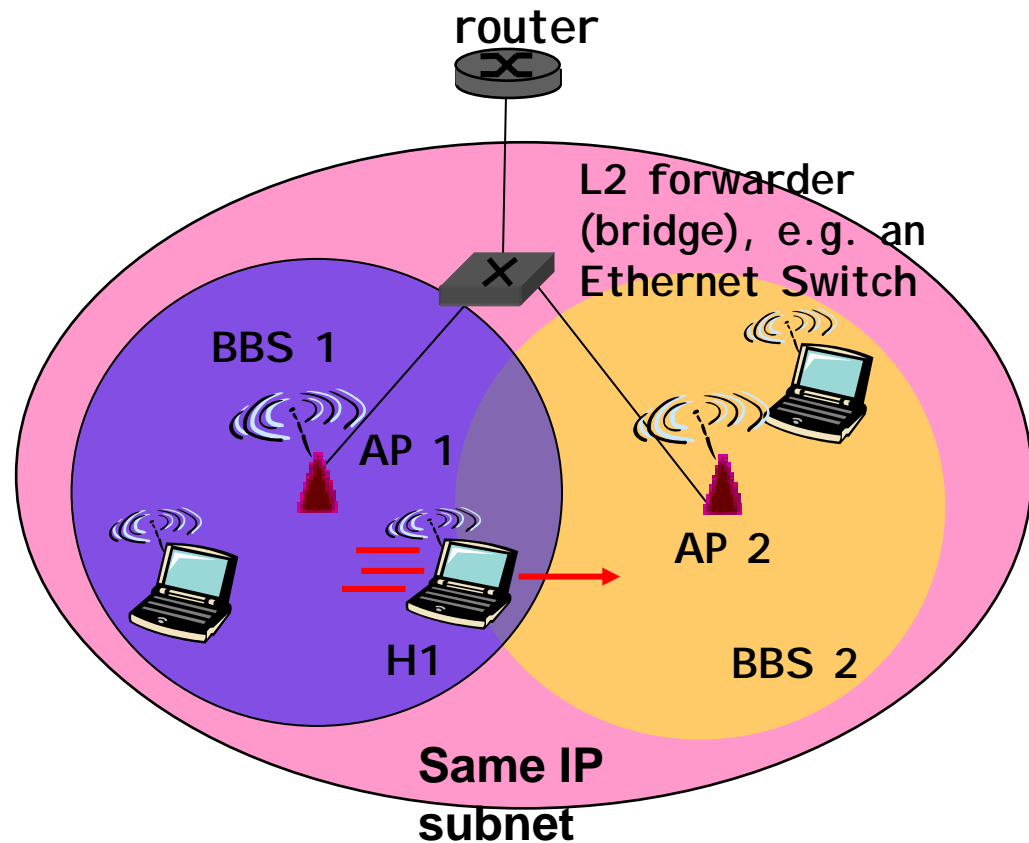
802.11 frame: addressing



Why can't 802.11 WLAN just use 2 addresses per frame like wired Ethernet ?

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: switch will see frame from H1 and “remember” which switch port can be used to reach H1
 - ◆ But what if there are more than one switch in the IP subnet ?



802.11 - Roaming

When STA experienced No or bad connection (e.g. poor SNR) perform:

- Scanning
 - ◆ scan the environment,
 - ☞ Either passively listen into the medium for beacon signals or
 - ☞ Actively send probes into the medium and wait for an AP to answer
- Reassociation Request
 - ◆ station sends a request to one or several AP(s)
- Reassociation Response
 - ◆ success: AP has answered, station can now participate
 - ◆ failure: continue scanning
- AP accepts Reassociation Request
 - ◆ signal the new station to the distribution system
 - ◆ the distribution system updates its data base (i.e., location information)
 - ◆ typically, the distribution system now informs the old AP so it can release resources using yet-to-be standardized Inter Access Point Protocol (IAPP)

802.11 - MAC management Task Summary

- Synchronization
 - ◆ try to find a LAN, try to stay within a LAN
 - ◆ timer etc.
- Power management
 - ◆ sleep-mode without missing a message
 - ◆ periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
 - ◆ STA becomes a member of a WLAN/LAN
 - ◆ Roaming, i.e. change networks by changing access points
 - ◆ Scanning, i.e. active search for a network
- Maintenance operations for AP, e.g.
 - ◆ System parameters, e.g. Channel #, configuration ;
 - ◆ Accounting
 - ◆ Activity logging

Some current IEEE 802.11

Standardization activities

- 802.11e: MAC Enhancements – QoS – almost done
 - ◆ Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.
- 802.11f: Inter-Access Point Protocol (IAPP)– experimental best current practice (not a binding standard) is available
 - ◆ Establish an Inter-Access Point Protocol for data exchange via the distribution system.
- 802.11i: Enhanced Security Mechanisms – completed recently
 - ◆ Enhance the current 802.11 MAC to provide improvements in security.
- 802.11n: High Throughput (100Mbps+) – ongoing
- 802.11r: Fast (Seamless) Handover support - ongoing
- 802.11u: Interworking between 802.11 and non-802.11 Wireless networks
- 802.11s: Mesh Networking – ongoing
 - ◆ Using a self-configurable wireless infrastructure within an ESS

IEEE 802.11s – Mesh Network of APs

