# Introduction to LAN/WAN

## Medium Access Sublayer (Part III)

# Now, Where are We?

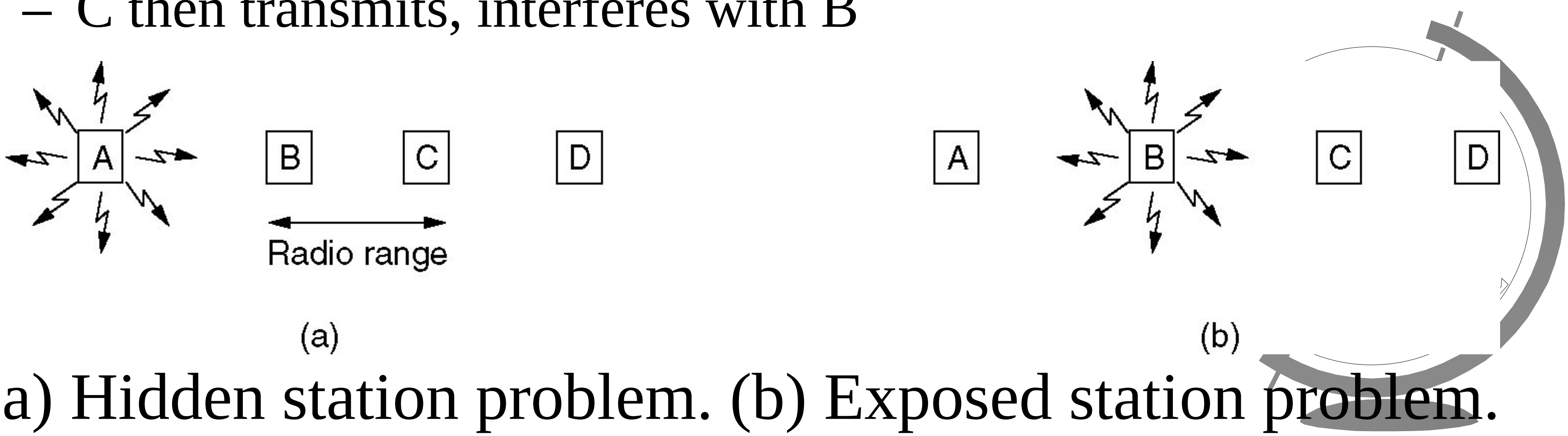
- ☞ Introduction
- ☞ Multiple Access Protocols
  - – contention
  - – collision-free
- ☞ Ethernet
- ☞ Wireless LAN Protocols ←
- ☞ Bridges

# Wireless LAN Protocols

- Proliferation of mobile devices (laptops, PDAs, cell phones, etc)
- Wireless LAN: system of notebooks which communicate by radio
- Typical configuration: office building with base stations (access points) placed around building
- Base stations may be interconnected using wires
- Unlike cellular, all cells can use entire spectrum
- Therefore need a MAC protocol to share broadcast channel

# Hidden Terminal Problem

- Stations have transmission range: *naïve to try pure CSMA*
- Problem: due to ranges, interference at receiver is what matters
- Hidden terminal problem (no CSMA), fig A:
  - A, C want to send to B,
  - A starts transmitting, C cannot hear (out of range)
  - C then transmits, interferes with B




(a) Hidden station problem. (b) Exposed station problem.

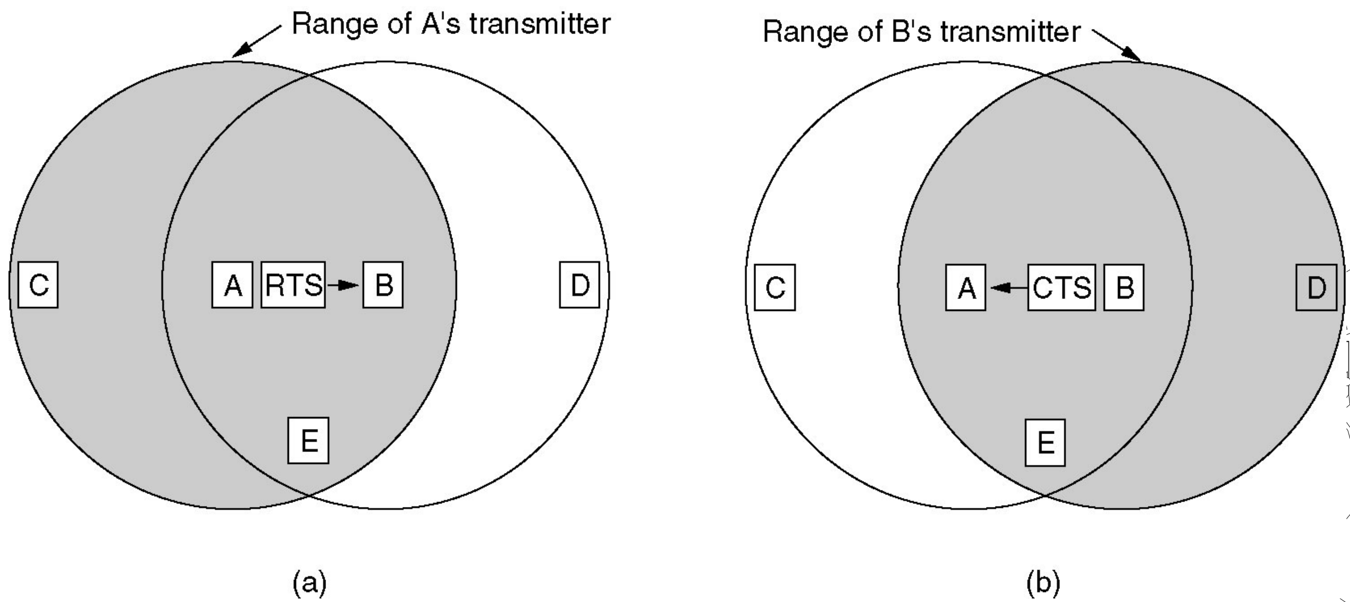
# Exposed Terminal Problem

- Exposed terminal problem (reverse of hidden terminal), fig (b):
  - A wants to transmit to B, C wants to transmit to D
  - Note: both transmissions can happen simultaneously since there will be bad reception only in area between B and C
  - A transmits, C senses channel and falsely thinks it can't transmit, doesn't transmit


(a) Hidden station problem. (b) Exposed station problem.

# Wireless LAN Protocols

- MACA protocol solved hidden, exposed terminal:
  - Send Ready-to-Send (RTS) and Clear-to-Send (CTS) first
  - RTS, CTS helps determine who else is in range or busy (Collision avoidance). Can collision still occur?
- MACAW added ACKs and CSMA (no RTS at same time)



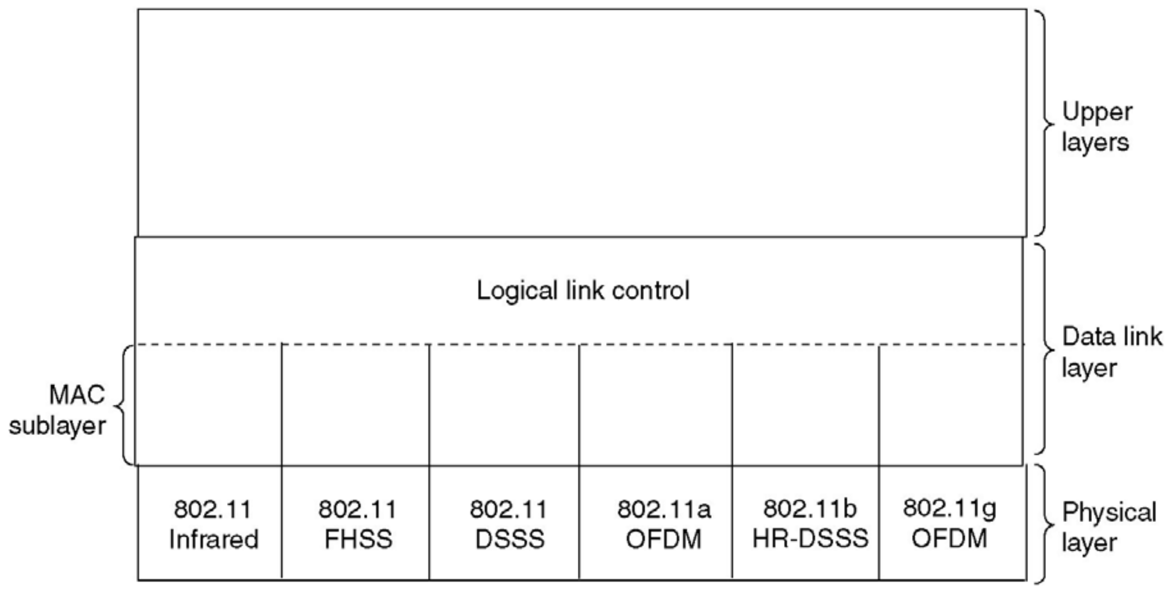

(a) A sending an RTS to B.(b) B responding with a CTS to A.

# IEEE 802.11 WLAN Protocol

- IEEE 802.11: Wireless LAN standard
  - Protocol Stack
  - Physical Layer
  - MAC Sublayer Protocol
  - Frame Structure
  - Services
- Possible configurations: with or without base station
- Operate in free ISM bands (900MHz, 2.4GHz, 5.5GHz)

# The 802.11 Protocol Stack

- Physical layer conforms to OSI (five options)
  - 1997: infrared, FHSS, DHSS
  - 1999: OFDM, HR-DSSS
- Data Link layer split into two: LLC and MAC as before



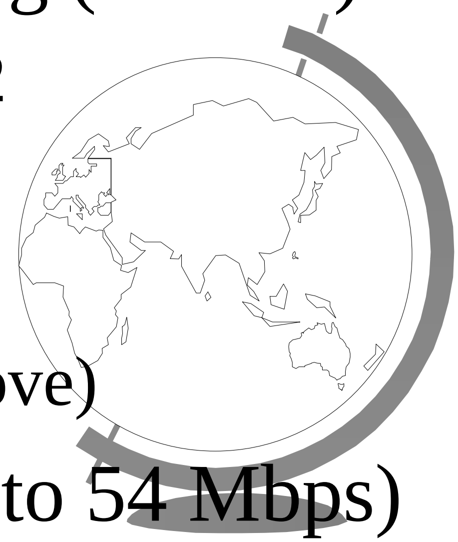

Part of the 802.11 protocol stack.

# The 802.11 Physical Layer

- Infrared
  - Two speeds: 1 Mbps, 2Mbps
  - Cannot penetrate walls (think TV remote control)
  - Low bandwidth makes it non-viable
- Frequency Hopping Spread Spectrum (FHSS)
  - 79 channels, each 1Mhz wide
  - Same pseudo-random number generator by both sender/receiver
  - Dwell time: min. time on channel before hopping (400msec)
- Direct Sequence Spread Spectrum
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA, sec. 2.6.2)
  - Each bit transmitted as 11 chips (Barker seq.), PSK at 1Mbaud
  - Each station assigned unique chip seq.,1-sequence, 0–complim

# The 802.11 Physical Layer

- Previously FCC rule: must use SS in ISM bands
- Dropped rule in 2002: two new high speed standards
- High Rate-DSSS
  - 802.11b
  - Up to 11 Mbps in 2.4GHz band
  - 11 million chips/sec, PSK (simply increase chip rate)
- Orthogonal Frequency Division Multiplexing (OFDM)
  - 802.11a, compatible with European HiperLAN2
  - Up to 54 Mbps in wide 5.5 GHz band
  - 52 channels: 48 for data, 4 for synchronization
  - Complex encoding (PSK to 18 Mbps, QAM above)
- 2001: 802.11g (OFDM in 2.4GHz band, up to 54 Mbps)

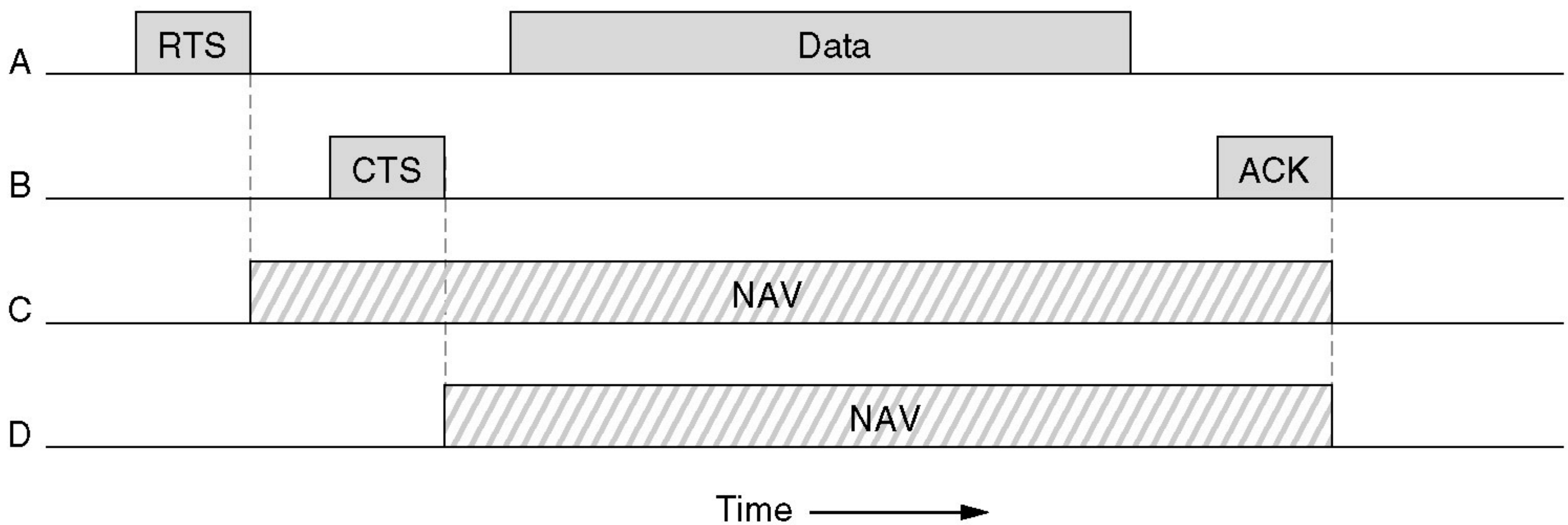


# The 802.11 MAC Protocol

- Two modes:
  - Point Coordination Function (PCF) (with base station)
  - Distributed Coordination Function (DCF) (no BS)
- DCF must be implemented, PCF optional
- Two DCF options:
  - Both use CSMA/CA (physical and virtual carrier sensing)
  - One without RTS-CTS
  - Other with RTS/CTS, (Based on MACAW)
  - Exponential backoff algorithm (like ethernet) if collision (Collision Avoidance)

# The 802.11 MAC Protocol

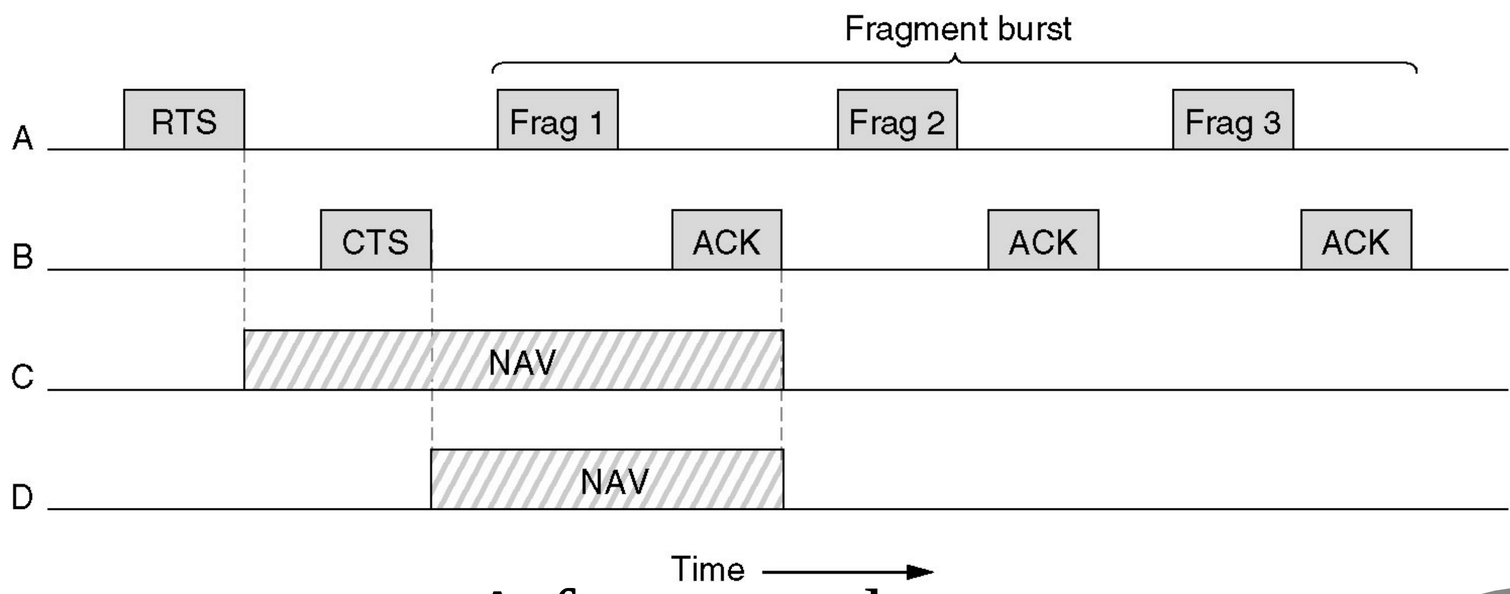
- Network Allocation Vector (NAV)
  - Information in RTS (or CTS) tells how long transmission plus ACK will take (implicit reservation)
  - All stations hearing NAV defer for estimated time (virtual carrier sensing)




The use of virtual channel sensing using CSMA/CA.

# Fragmentation in The 802.11 MAC

- High wireless error rate means very long packets have slim chance of making it through
- Solution: break packets up (fragmentation)
- Fragments individually numbered and ACKed using stop-and-wait (*k* before *k+1*)
- Sequence of fragments: fragment burst



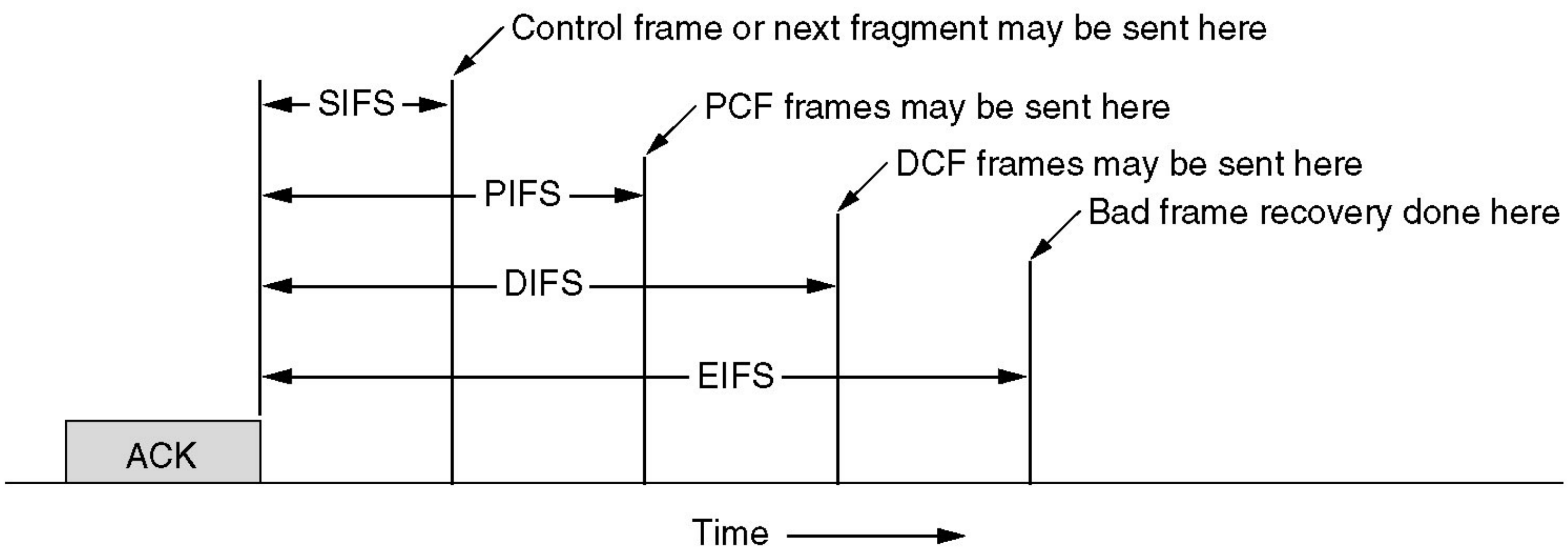

A fragment burst.

# The 802.11 MAC:  PCF

- PCF uses base station
- Base station polls other stations for traffic
- Good for deterministic (real-time, video, audio) traffic
- Beacon sent periodically for synchronization
- Stations can go to sleep to save battery
- Base station stores packets for sleeping station
- PCF and DCF can co-exist by using InterFrame Spacing (IFS)
- IFS: after a frame is sent all stations must wait a certain amount of dead time before transmitting

# The 802.11 MAC: IFS

- Short IFS: time waited between packets in an ongoing dialog (RTS, CTS, data, ACK, next fragment)
- PCF IFS: no SIFS, base station waits PIFS and jumps in (beacon or poll frame)
- DIFS: no PIFS any station can jump in (new dialog)
- EFS: Bad or unknown frame report (low priority)




Interframe spacing in 802.11.

# The 802.11 Frame Structure

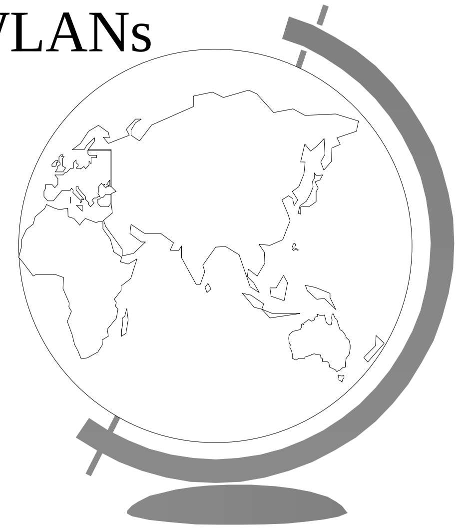
| Bytes | 2 | 2 | 6 | 6 | 6 | 2 | 6 | 0-2312 | 4 |
|---|---|---|---|---|---|---|---|---|---|
| | Frame control | Duration | Address 1 | Address 2 | Address 3 | Seq. | Address 4 | Data | Checksum |

| Bits | 2 | 2 | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Version | Type | Subtype | To DS | From DS | MF | Retry | Pwr | More | W | O | Frame control |

The 802.11 data frame.

# 802.11 Services

- Conformant wireless LANs must provide nine services
  - 5 distribution, 4 station services
- Distribution Services (managing cell membership)
  - Association: connect to base station
  - Disassociation: disconnect from base station
  - Reassociation: handoff, moving from cell to cell
  - Distribution: how base station routes packets (local or backbone)
  - Integration: address translation between different WLANs
- Intracell Services (activity within a cell)
  - Authentication: secure join
  - Deauthentication: secure leave
  - Privacy: encryption (uses RC4, by Ronald Rivest)
  - Data Delivery (heart of 802.11, already discussed)

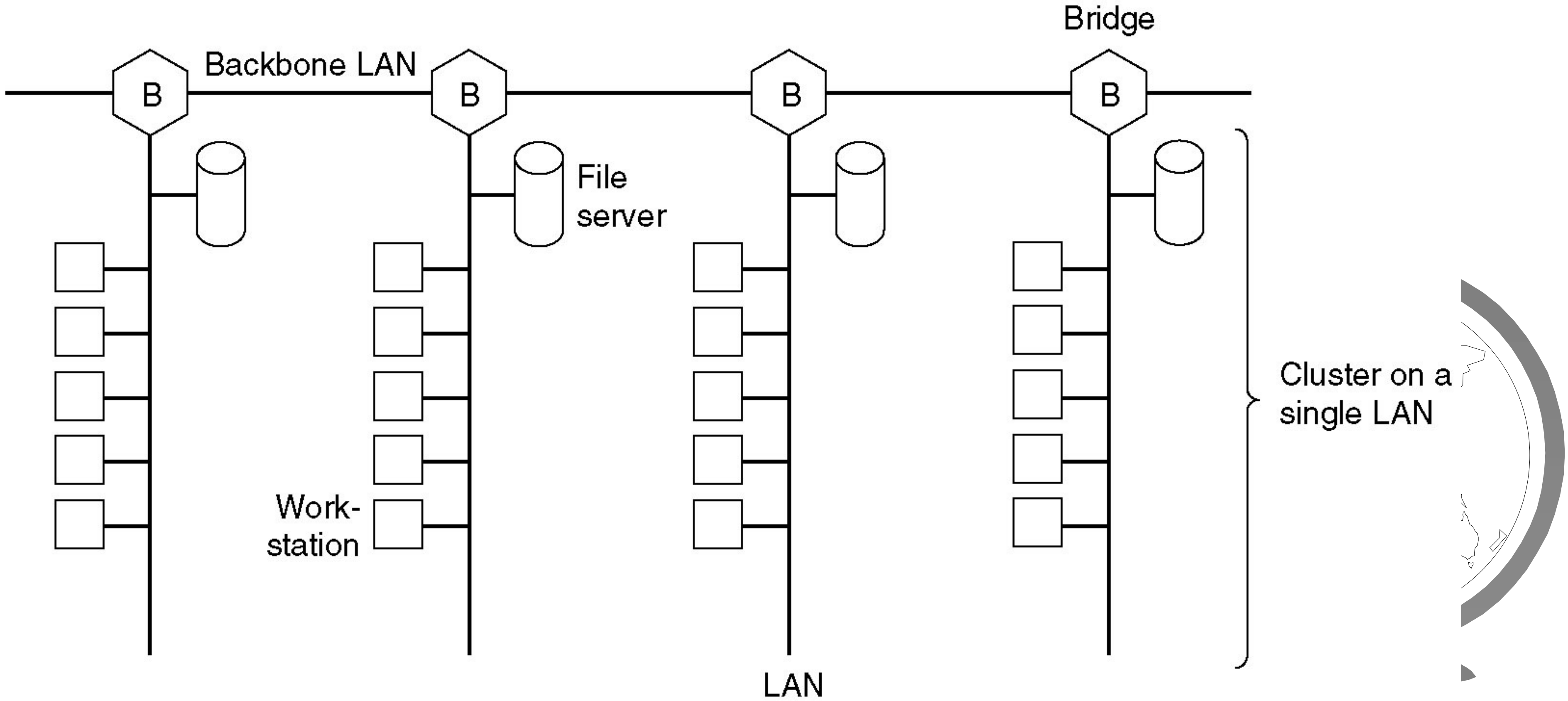


# Now, Where are We?

- ☞ Introduction
- ☞ Multiple Access Protocols
  - – contention
  - – collision-free
- ☞ Ethernet
- ☞ Wireless LAN Protocols
- ☞ Bridges ←

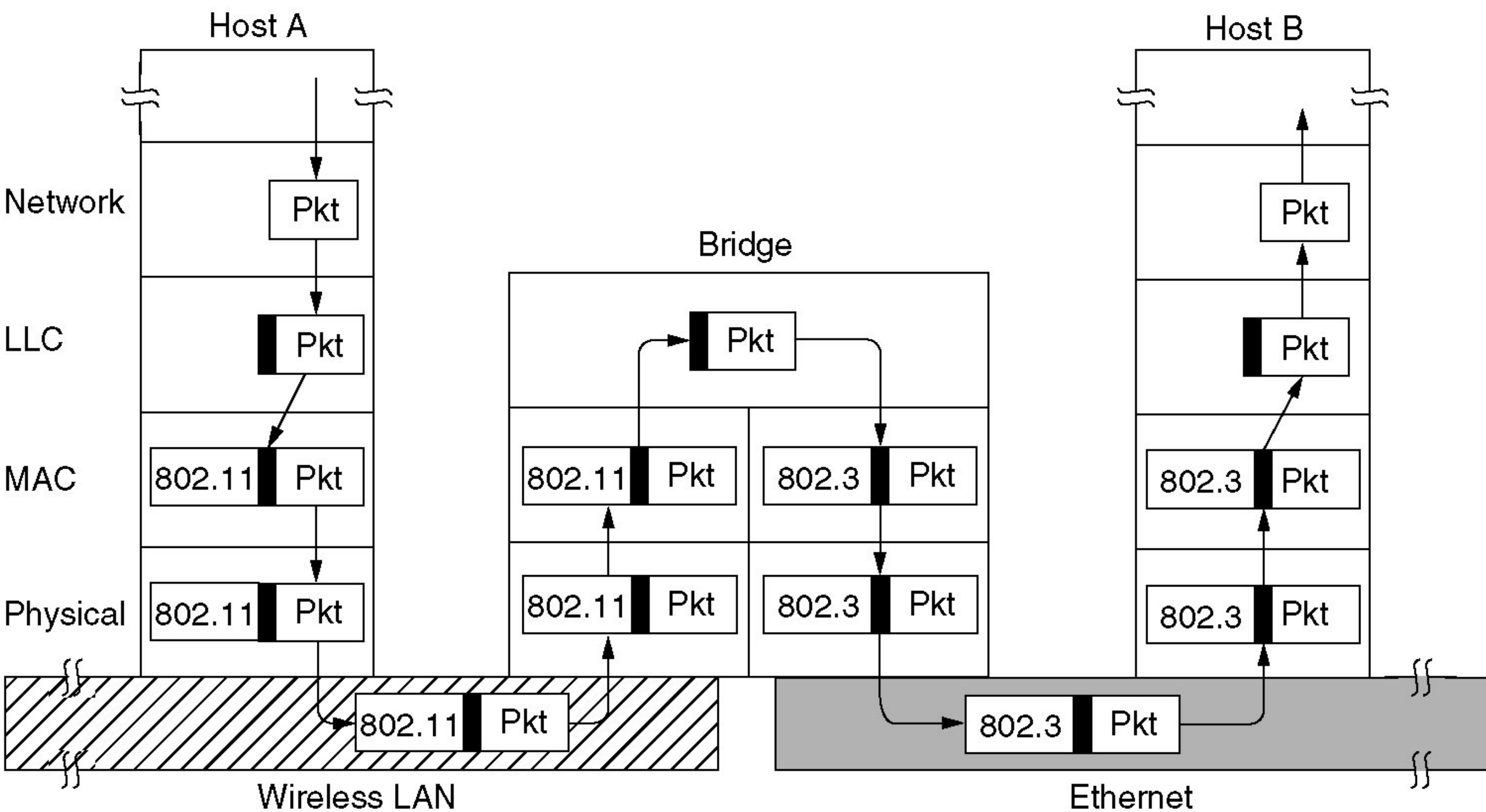
# Bridges

- ☞ Connect different LANs at the *Data Link Layer*
  - – Transparently, so LANs can stay the same
  - – Network layer not looked at
  - – Can transport IPv4, IPv6, IPX, or OSI packets
- ☞ Routers do look at network (IP) header (more later)



# Bridges

- Two different LANs: two different packet formats
- Everyone wants to keep their packet formats
- Bridge reads in packets on does conversion




Operation of a LAN bridge from 802.11 to 802.3.

# What else is the Big Deal?

- Data rate
  - Fast to slow (bridge buffers packets)
- Different frame length
  - Cannot fragment or reassemble here, messes protocols and layering up (no solution, discard large frames)
- Security
  - Some (802.11, 802.16) support encryption, others do not
  - Can force higher layers to do encryption (not transparent!!)
- Quality of Service
  - 802.11 provides for QoS using PCF, ethernet does not

# Where Are We Going?

- Physical Layer
- Data Link Layer
  - Medium Access Sublayer
- Network Layer ←
- Transport Layer
- Katmandu