

# CMPE 150/L : Introduction to Computer Networks

Chen Qian

Computer Engineering  
UCSC Baskin Engineering

Lecture 17

# Course evaluation

- ❑ Bring your mobile devices next Tuesday
- ❑ I will finish the lecture 15 mins earlier and you may use the time for course evaluation.

# CSMA (carrier sense multiple access)

**CSMA:** listen before transmit:

if channel sensed idle: transmit entire frame

❖ if channel sensed busy, defer transmission

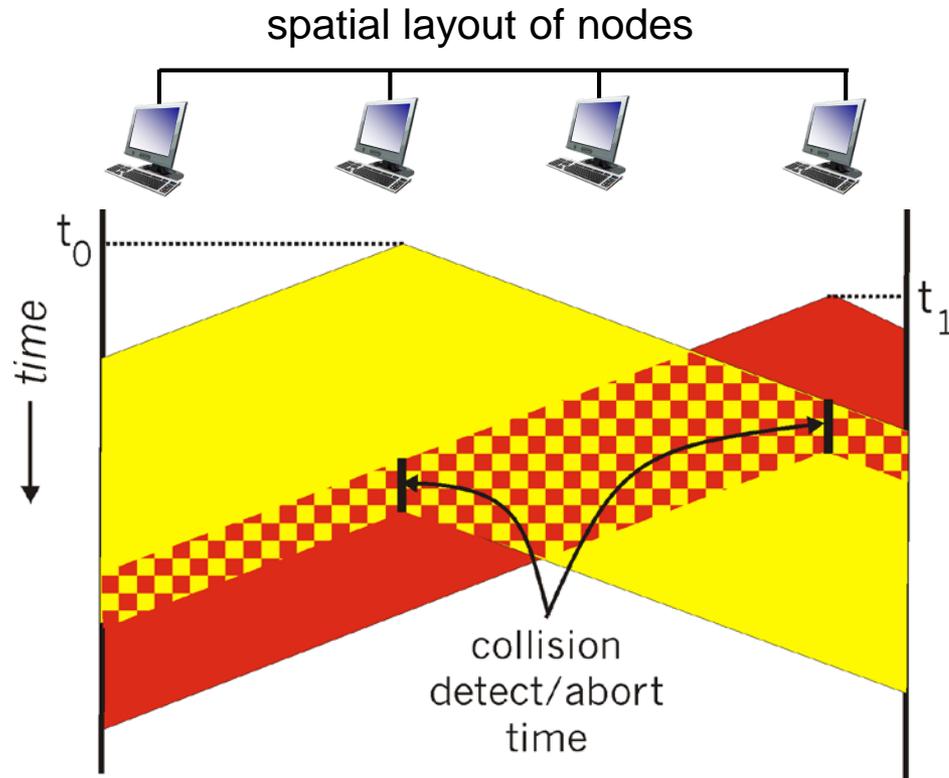
❖ human analogy: don't interrupt others!

# CSMA/CD (collision detection)

**CSMA/CD:** carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- ❖ collision detection:
  - easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - difficult in wireless LANs: received signal strength overwhelmed by local transmission strength
- ❖ human analogy: the polite conversationalist

# CSMA/CD (collision detection)



# Ethernet CSMA/CD algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !
4. If NIC detects another transmission while transmitting, aborts and sends jam signal
5. After aborting, NIC enters *binary (exponential) backoff*:
  - after  $m$ th collision, NIC chooses  $K$  at random from  $\{0, 1, 2, \dots, 2^m - 1\}$ . NIC waits  $K \cdot 512$  bit times, returns to Step 2
  - longer backoff interval with more collisions

# 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

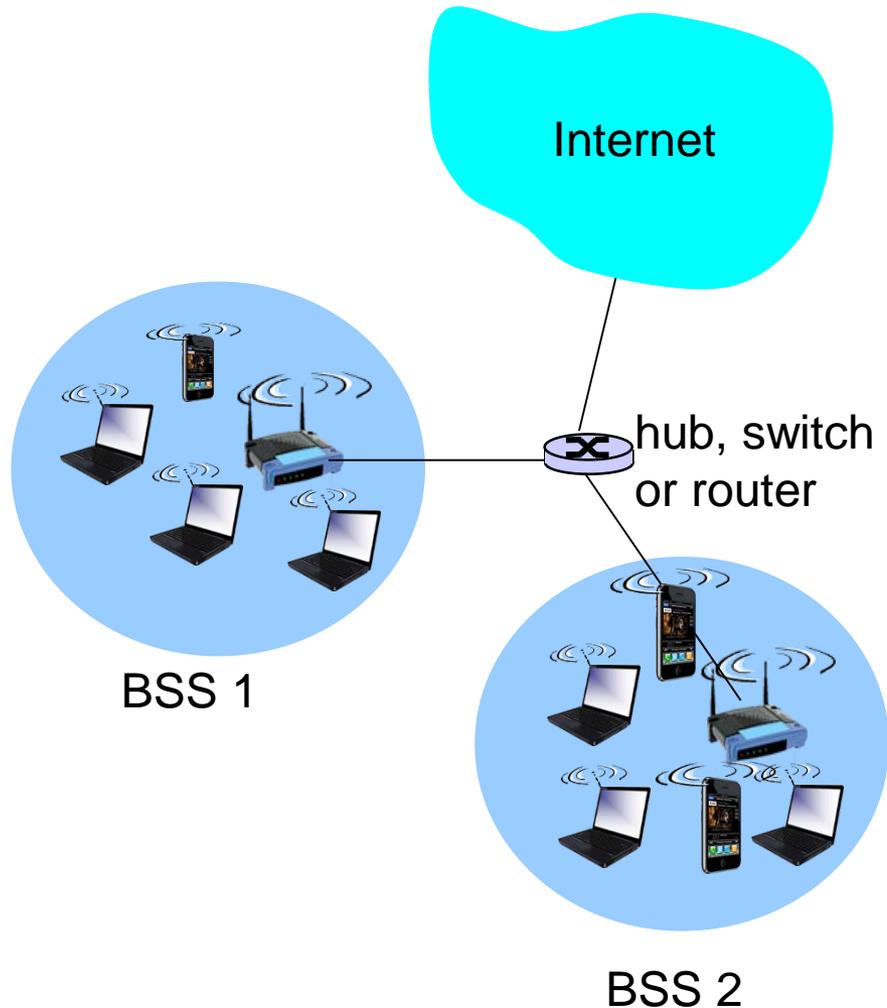
- 2.4-5 GHz range
- up to 54 Mbps

## 802.11n: multiple antennae

- 2.4-5 GHz range
- up to 200 Mbps

- ❖ all use CSMA/CA (collision avoidance) for multiple access
- ❖ all have base-station and ad-hoc network versions

# 802.11 LAN architecture

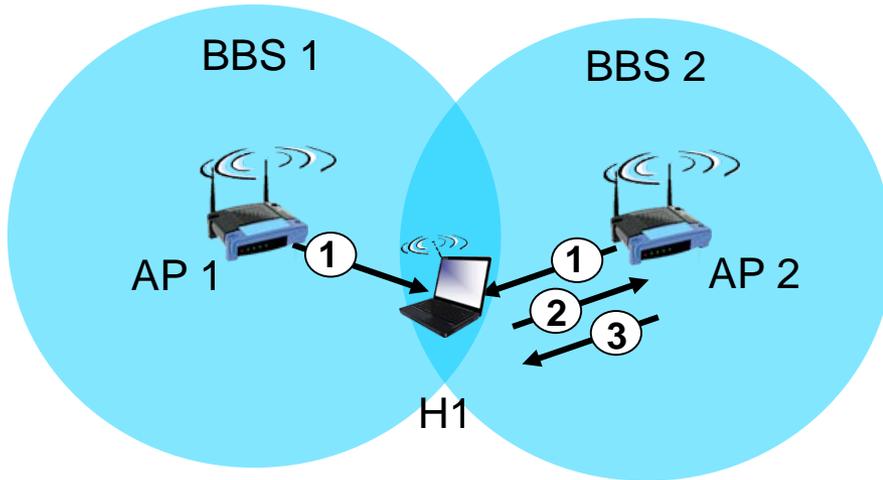


- ❖ wireless host communicates with base station
  - base station = access point (AP)
- ❖ **Basic Service Set (BSS)** (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

# 802.11: Channels, association

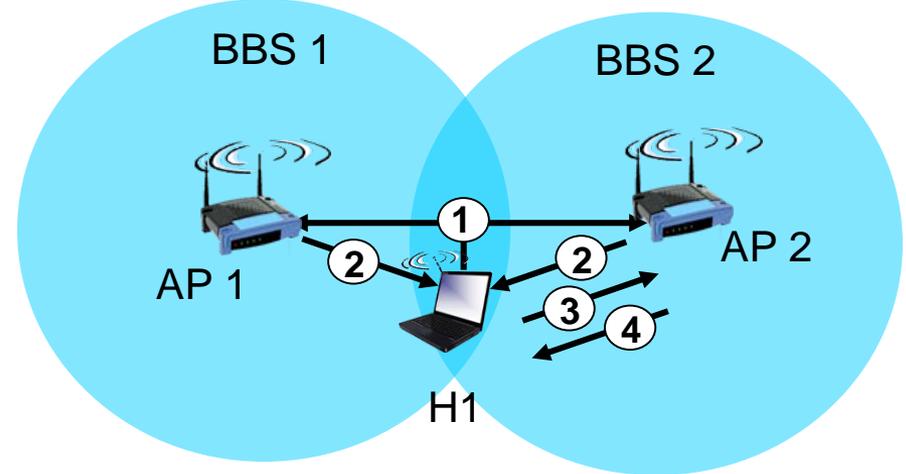
- ❖ 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- ❖ host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing 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

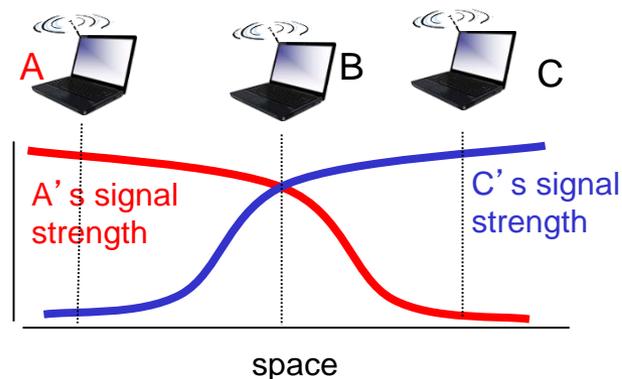
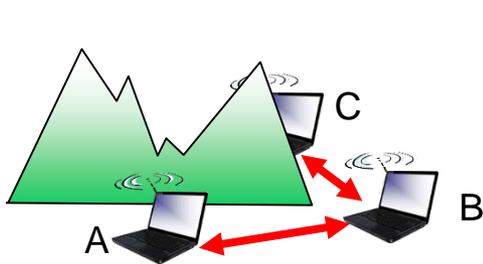


## active scanning:

- (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<sup>+</sup> 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/CA (Collision Avoidance)



# IEEE 802.11 MAC Protocol: CSMA/CA

## 802.11 sender

1 if sense channel idle for **DIFS** then

transmit entire frame (no CD)

DIFS: Distributed coordination function  
Interframe Space

2 if sense channel busy then

start random backoff time

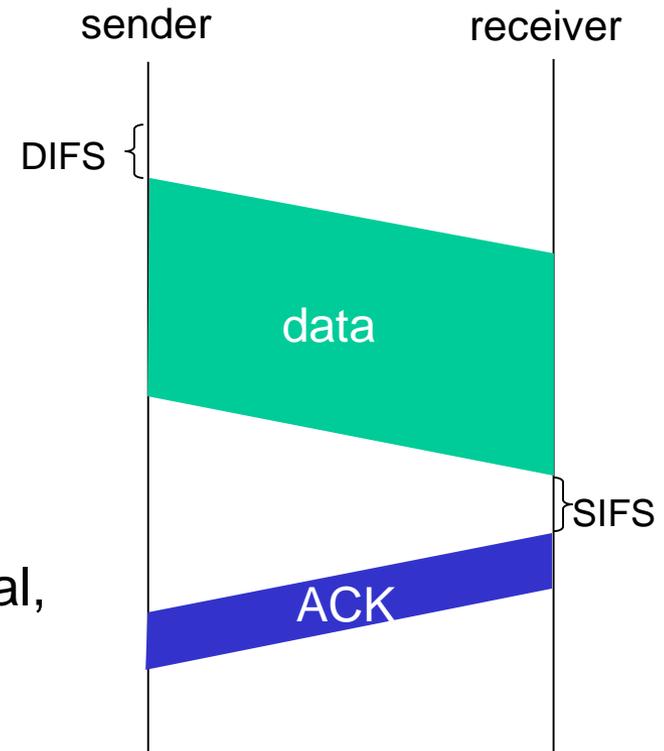
timer counts down while channel idle

transmit when timer expires

if no ACK, increase random backoff interval,  
repeat 2

## 802.11 receiver

- if frame received OK, return ACK after **SIFS**  
(Short Interframe Space), ACK needed due  
to hidden terminal problem

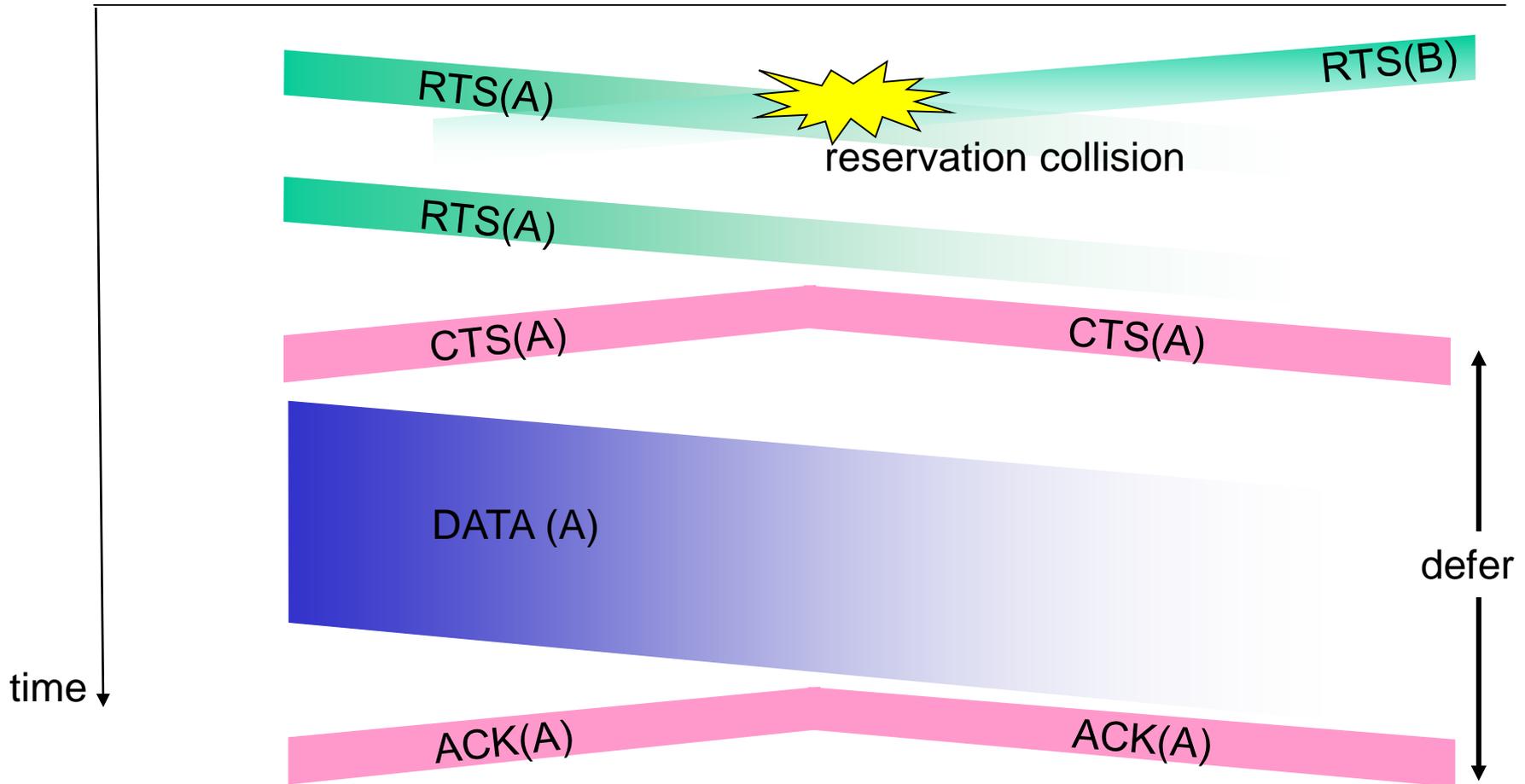


# Avoiding collisions (more)

- 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



# “Taking turns” MAC protocols

## channel partitioning MAC protocols:

- share channel *efficiently* and *fairly* at high load
- inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

## random access MAC protocols

- efficient at low load: single node can fully utilize channel
- high load: collision overhead

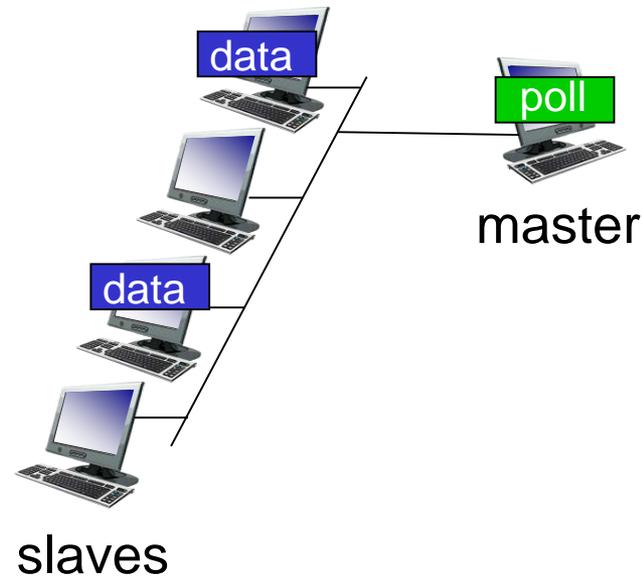
## “taking turns” protocols

look for best of both worlds!

# “Taking turns” MAC protocols

## *polling:*

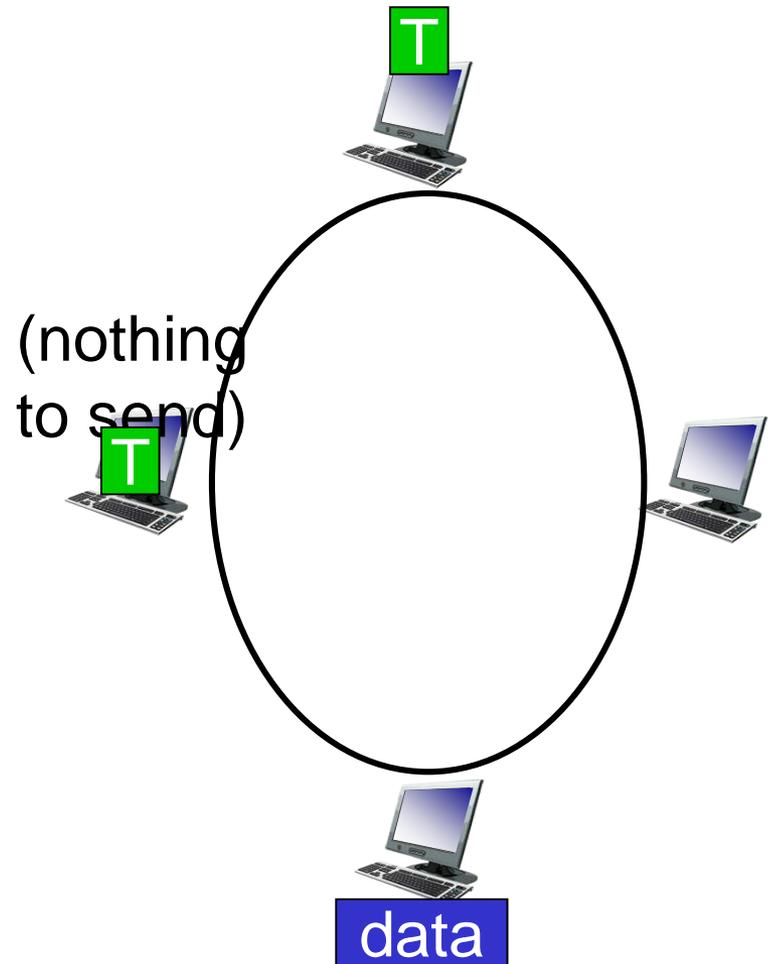
- ❖ master node “invites” slave nodes to transmit in turn
- ❖ typically used with “dumb” slave devices
- ❖ concerns:
  - polling overhead
  - latency
  - single point of failure (master)



# “Taking turns” MAC protocols

## token passing:

- ❖ control **token** passed from one node to next sequentially.
- ❖ token message
- ❖ concerns:
  - token overhead
  - latency
  - single point of failure (token)



# Summary of MAC protocols

- ❖ *channel partitioning*, by time, frequency or code
  - Time Division, Frequency Division
- ❖ *random access* (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11
- ❖ *taking turns*
  - polling from central site, token passing
  - bluetooth

# Summary of MAC protocols

- ❖ *channel partitioning*, by time, frequency or code
  - Time Division, Frequency Division
- ❖ *random access* (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11
- ❖ *taking turns*
  - polling from central site, token passing
  - bluetooth

# Link layer, LANs: outline

5.1 introduction, services

5.2 error detection,  
correction

5.3 multiple access  
protocols

5.4 LANs

- addressing, ARP
- Ethernet
- switches

5.5 data center  
networking

5.6 a day in the life of a  
web request

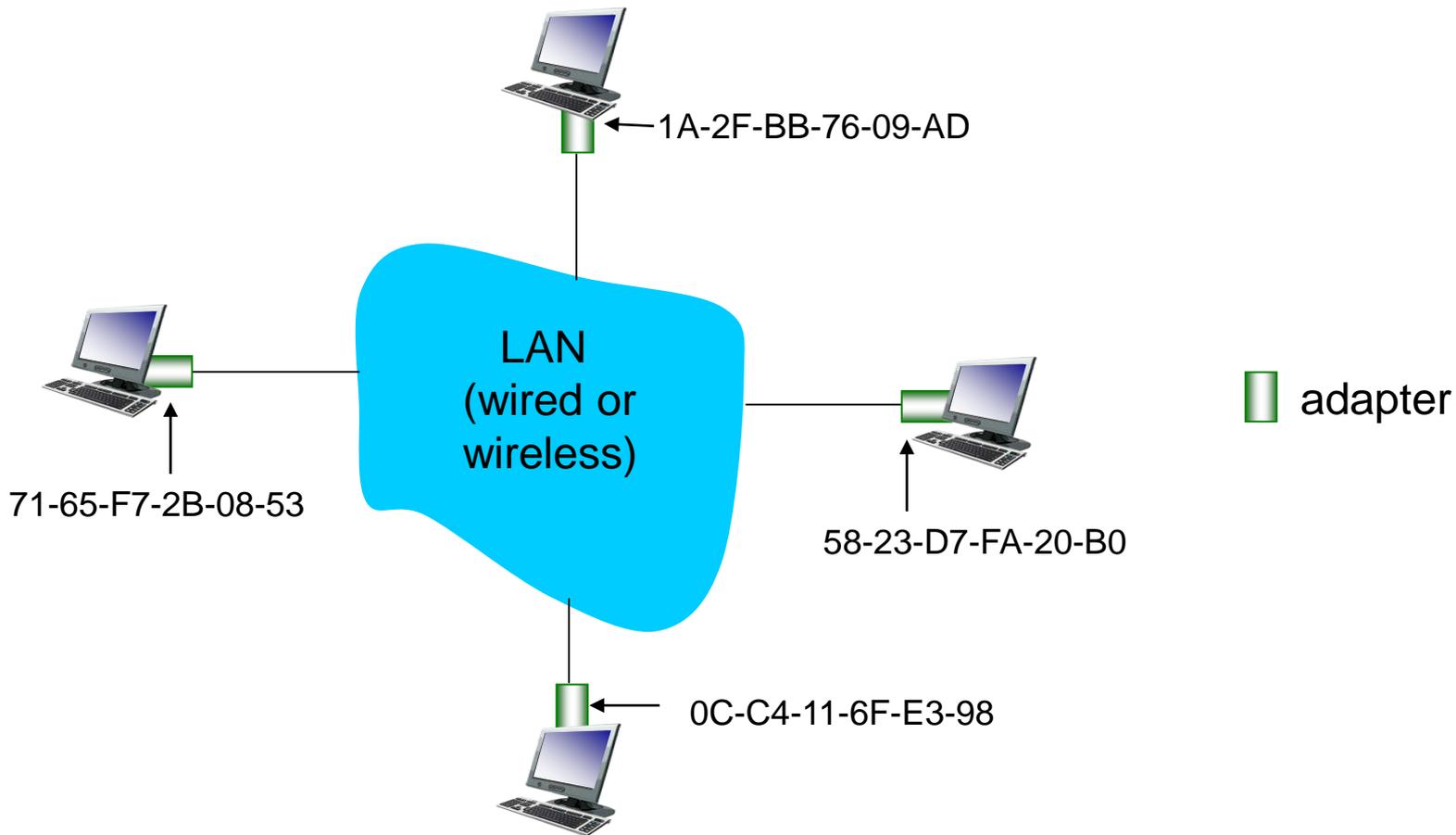
# MAC addresses and ARP

- ❖ 32-bit IP address:
  - *network-layer* address for interface
  - used for layer 3 (network layer) forwarding
- ❖ MAC (or LAN or physical or Ethernet) address:
  - function: *used ‘locally’ to get frame from one interface to another physically-connected interface (same network, in IP-addressing sense)*
  - 48 bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

hexadecimal (base 16) notation  
(each “number” represents 4 bits)

# LAN addresses and ARP

each adapter on LAN has unique *LAN* address

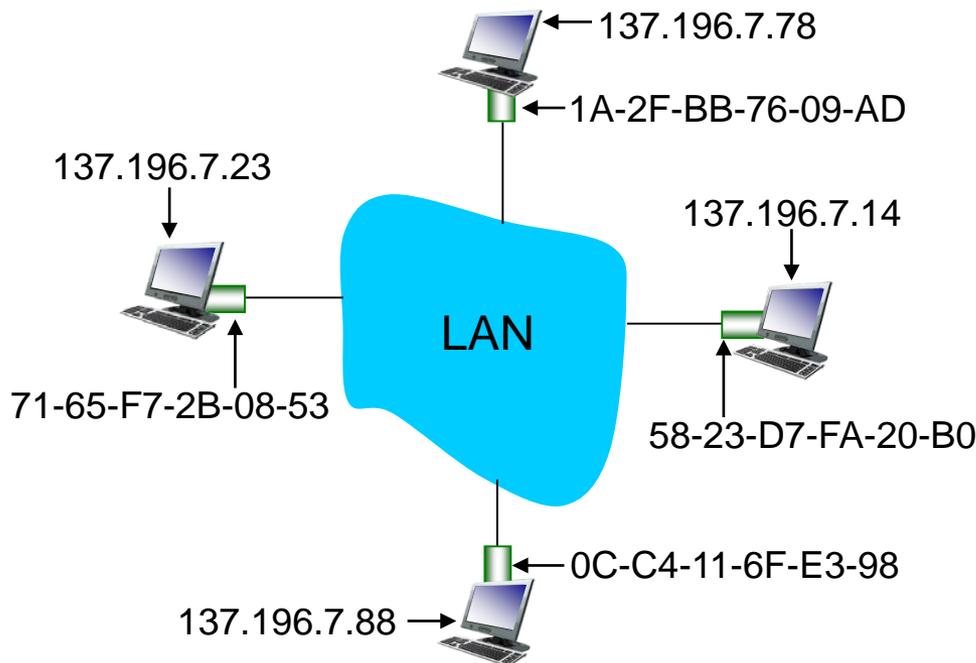


# LAN addresses (more)

- ❖ MAC address allocation administered by IEEE
- ❖ manufacturer buys portion of MAC address space (to assure uniqueness)
- ❖ analogy:
  - MAC address: like Social Security Number
  - IP address: like postal address
- ❖ MAC flat address → portability
  - can move LAN card from one LAN to another
- ❖ IP hierarchical address *not* portable
  - address depends on IP subnet to which node is attached

# ARP: address resolution protocol

**Question:** how to determine interface's MAC address, knowing its IP address?



**ARP table:** each IP node (host, router) on LAN has table

- IP/MAC address mappings for some LAN nodes:  
< IP address; MAC address; TTL >
- TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

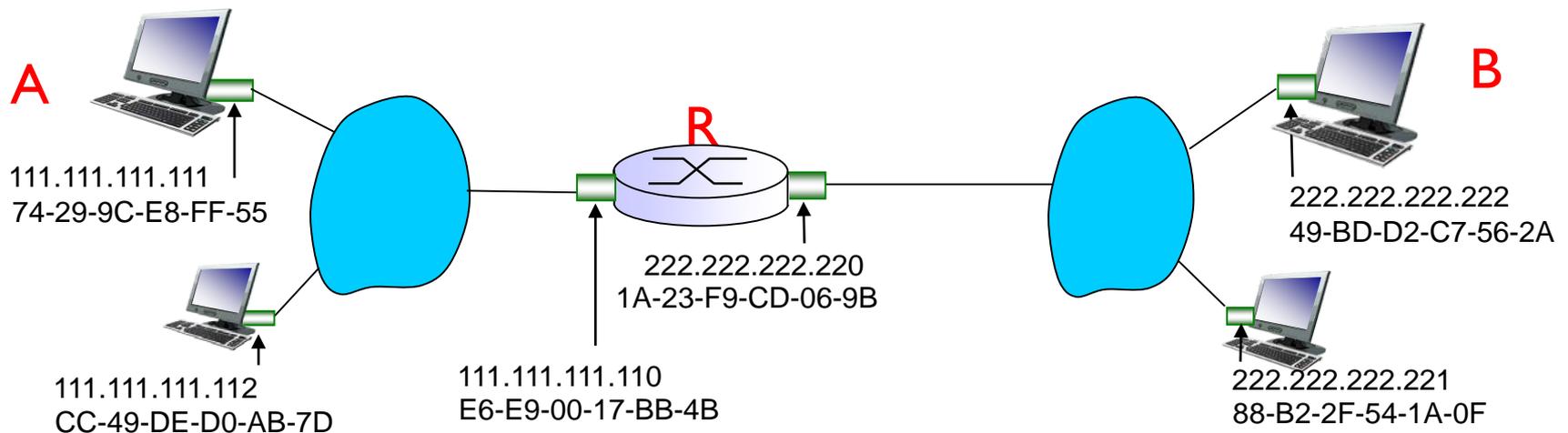
# ARP protocol: same LAN

- ❖ A wants to send datagram to B
  - B's MAC address not in A's ARP table.
- ❖ A **broadcasts** ARP query packet, containing B's IP address
  - dest MAC address = FF-FF-FF-FF-FF-FF
  - all nodes on LAN receive ARP query
- ❖ B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (unicast)
- ❖ A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  - soft state: information that times out (goes away) unless refreshed

# Addressing: routing to another LAN

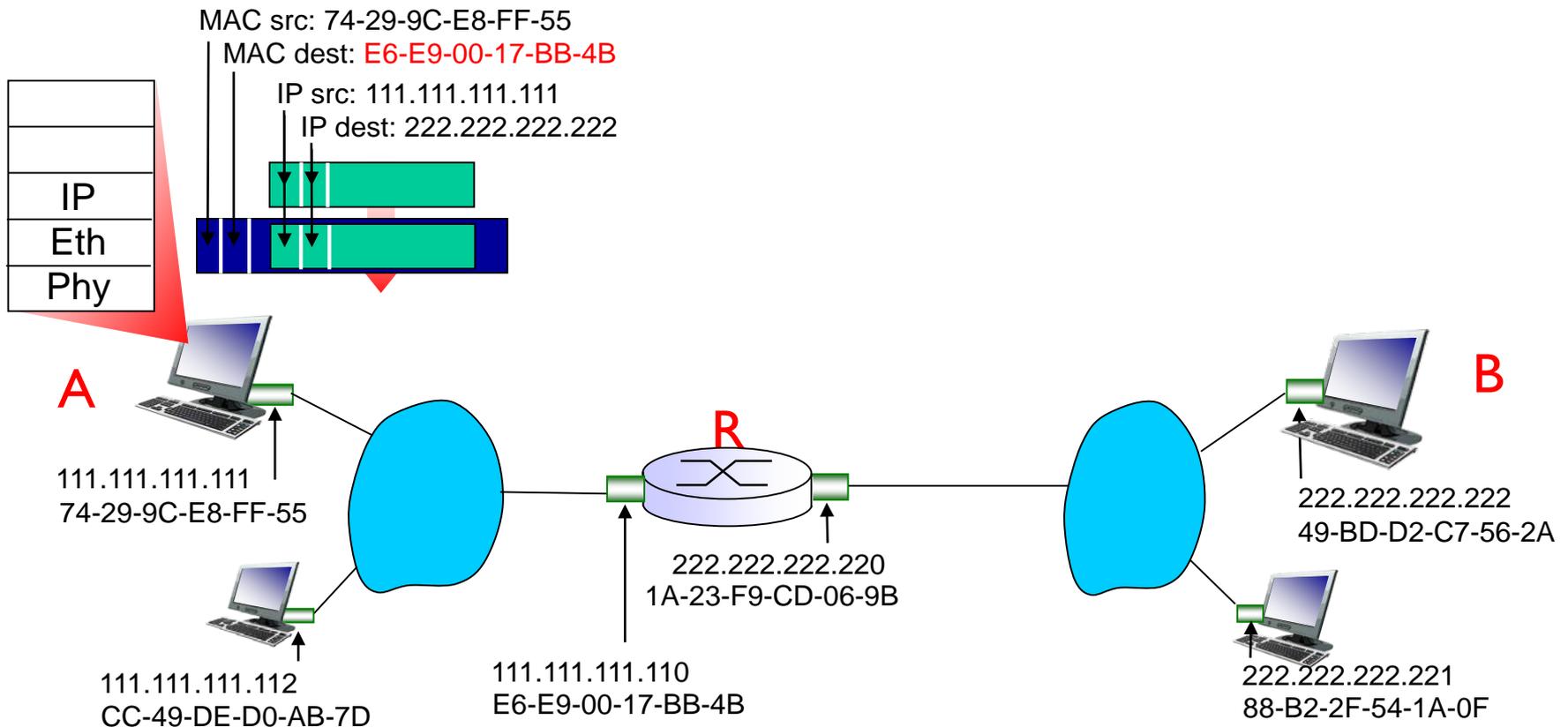
walkthrough: **send datagram from A to B via R**

- focus on addressing – at IP (datagram) and MAC layer (frame)
- assume A knows B's IP address
- assume A knows IP address of first hop router, R (how?)
  - DHCP
- assume A knows R's MAC address (how?)
  - ARP



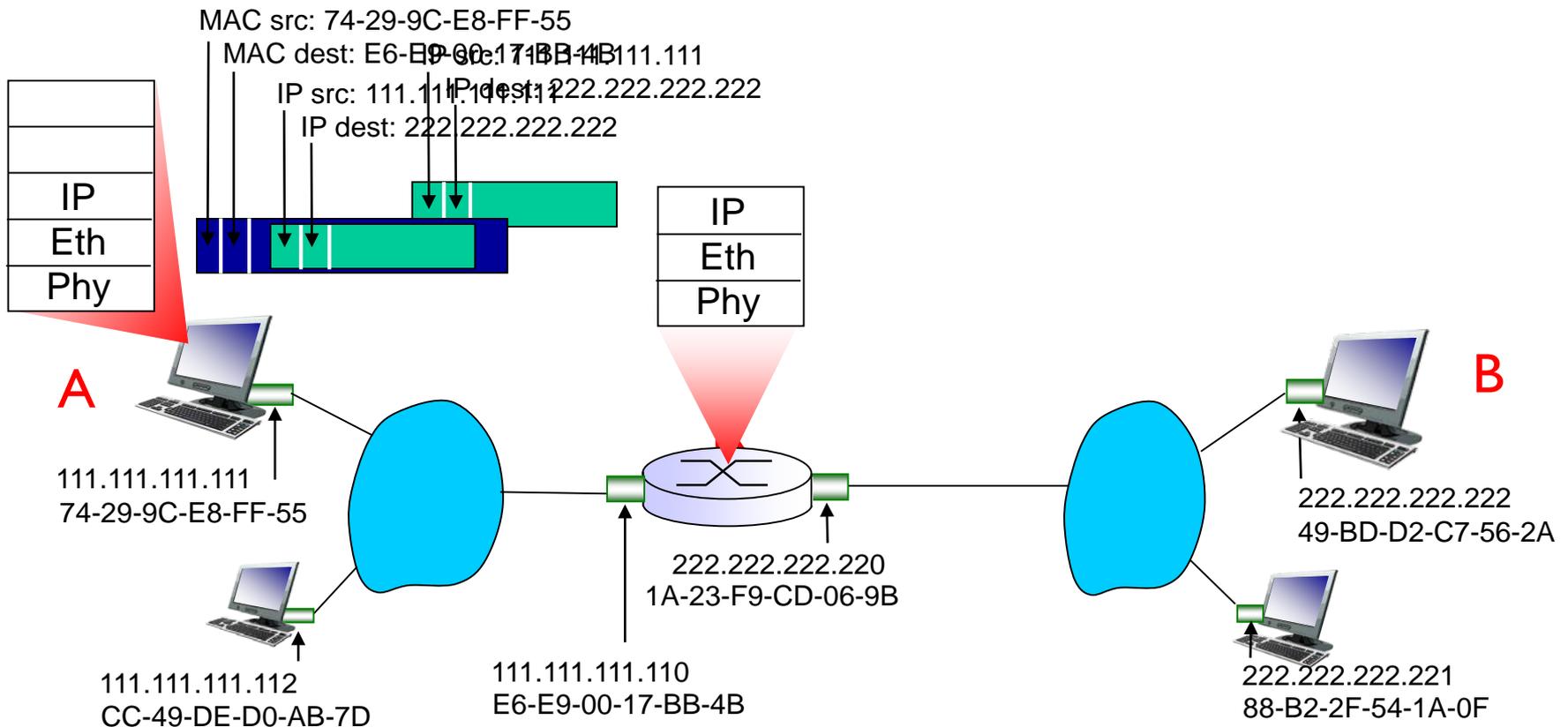
# Addressing: routing to another LAN

- ❖ A creates IP datagram with IP source A, destination B
- ❖ A creates link-layer frame with R's MAC address as dest, frame contains A-to-B IP datagram



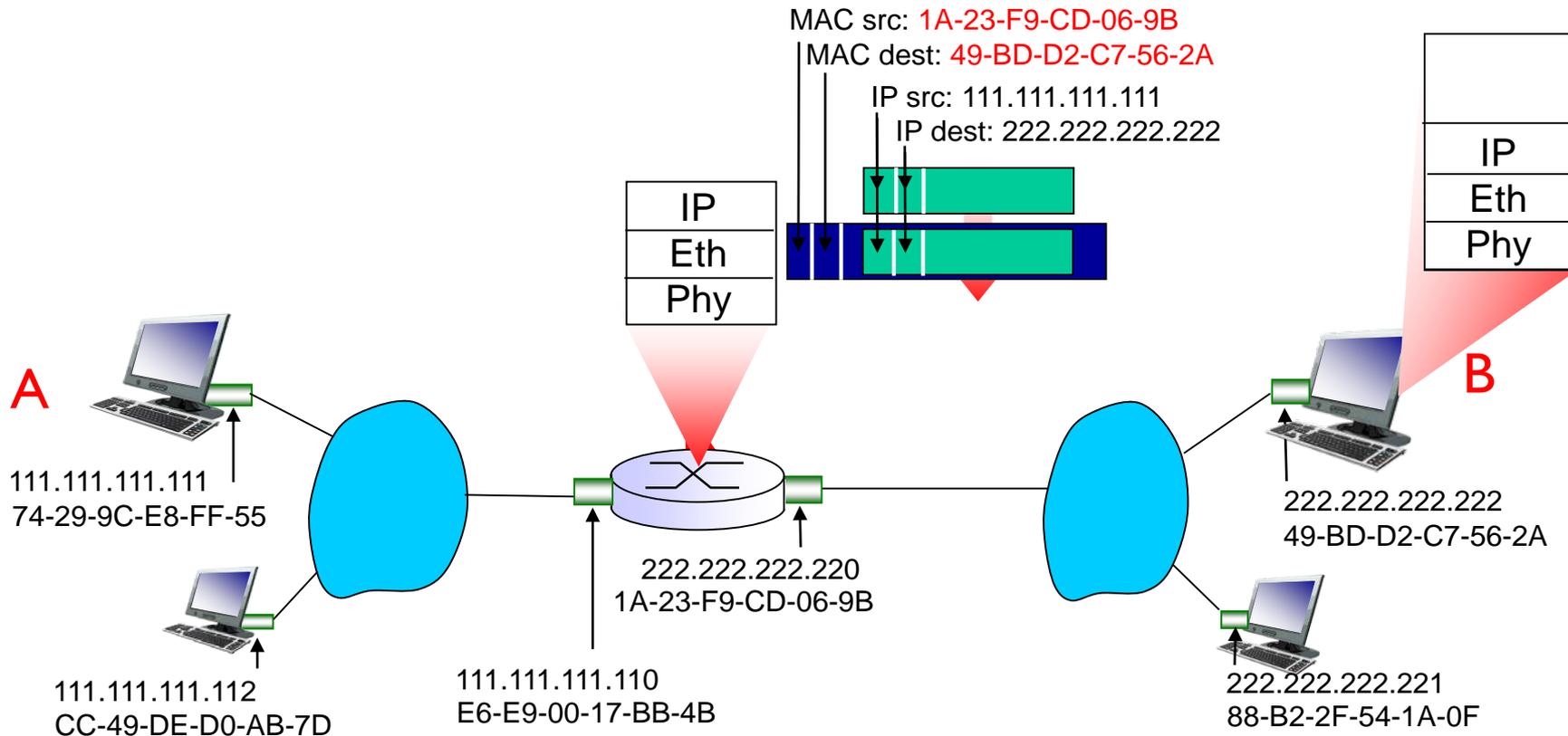
# Addressing: routing to another LAN

- ❖ frame sent from A to R
- ❖ frame received at R, datagram removed, passed up to IP



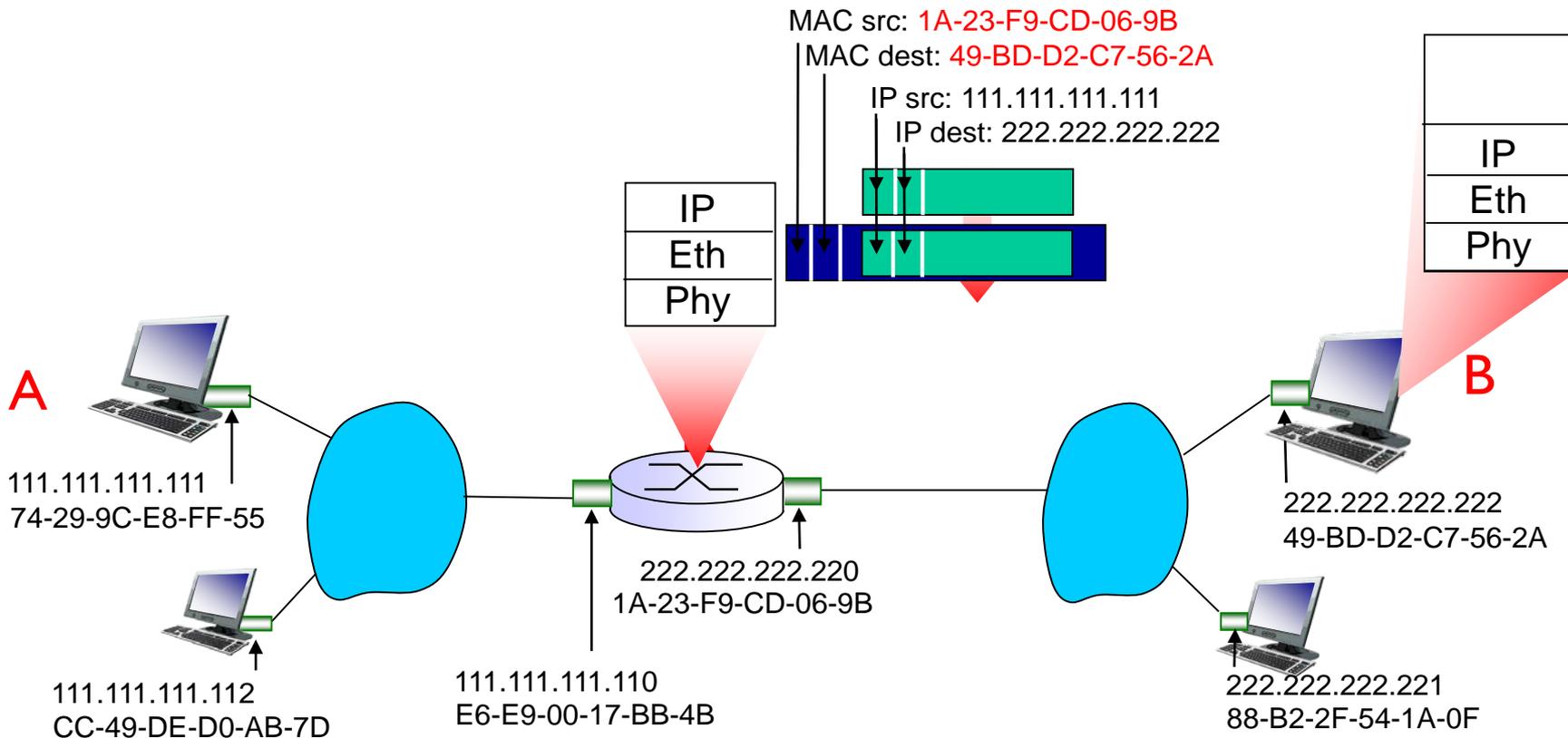
# Addressing: routing to another LAN

- ❖ R forwards datagram with IP source A, destination B
- ❖ R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram



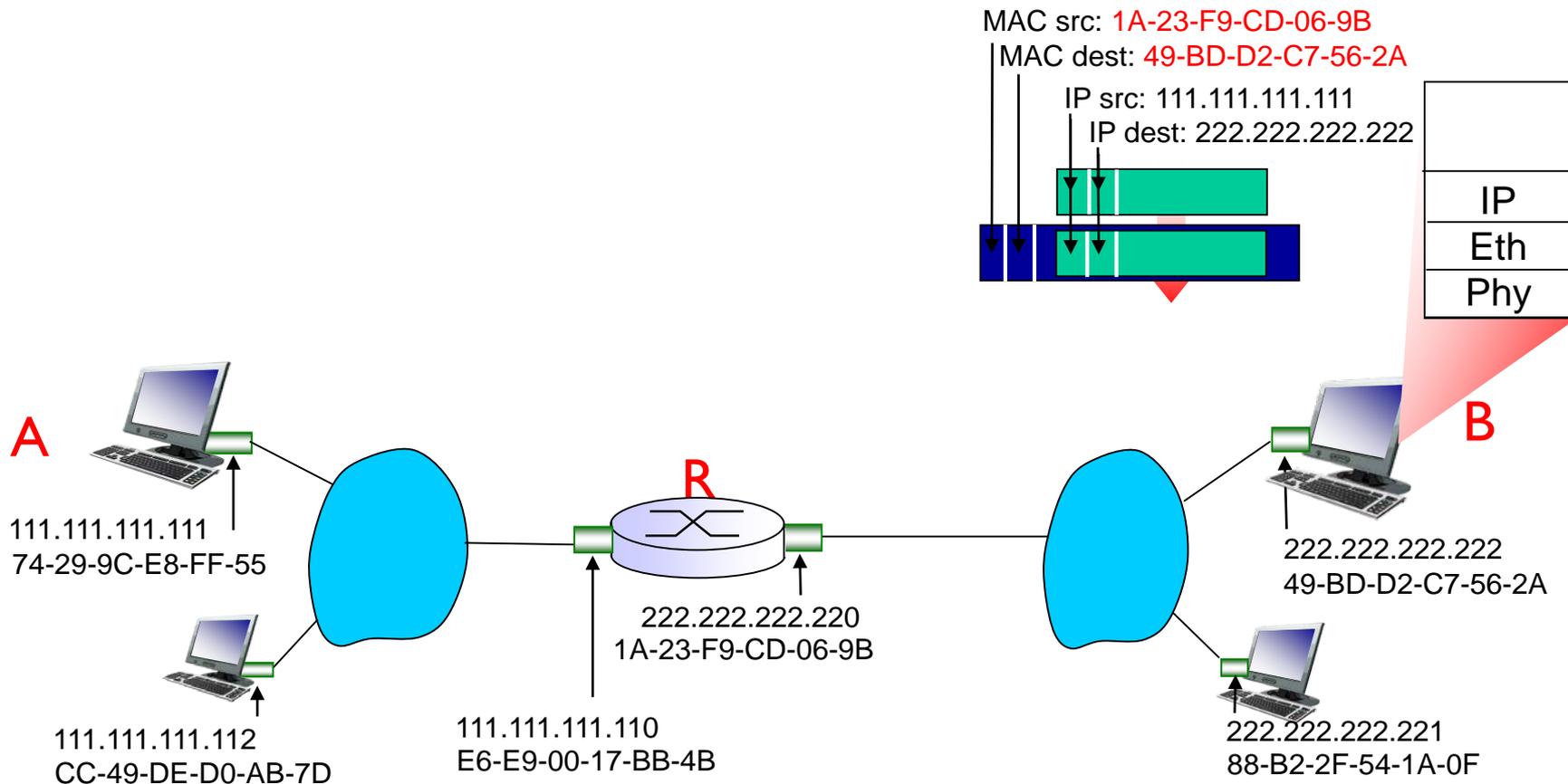
# Addressing: routing to another LAN

- ❖ R forwards datagram with IP source A, destination B
- ❖ R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram



# Addressing: routing to another LAN

- ❖ R forwards datagram with IP source A, destination B
- ❖ R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram



# Link layer, LANs: outline

5.1 introduction, services

5.2 error detection,  
correction

5.3 multiple access  
protocols

## 5.4 LANs

- addressing, ARP
- Ethernet
- switches

5.5 data center  
networking

5.6 a day in the life of a  
web request

# Next class

---

Finish Chapter 5