# Link layer, LANs: roadmap

- introduction
- error detection
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs

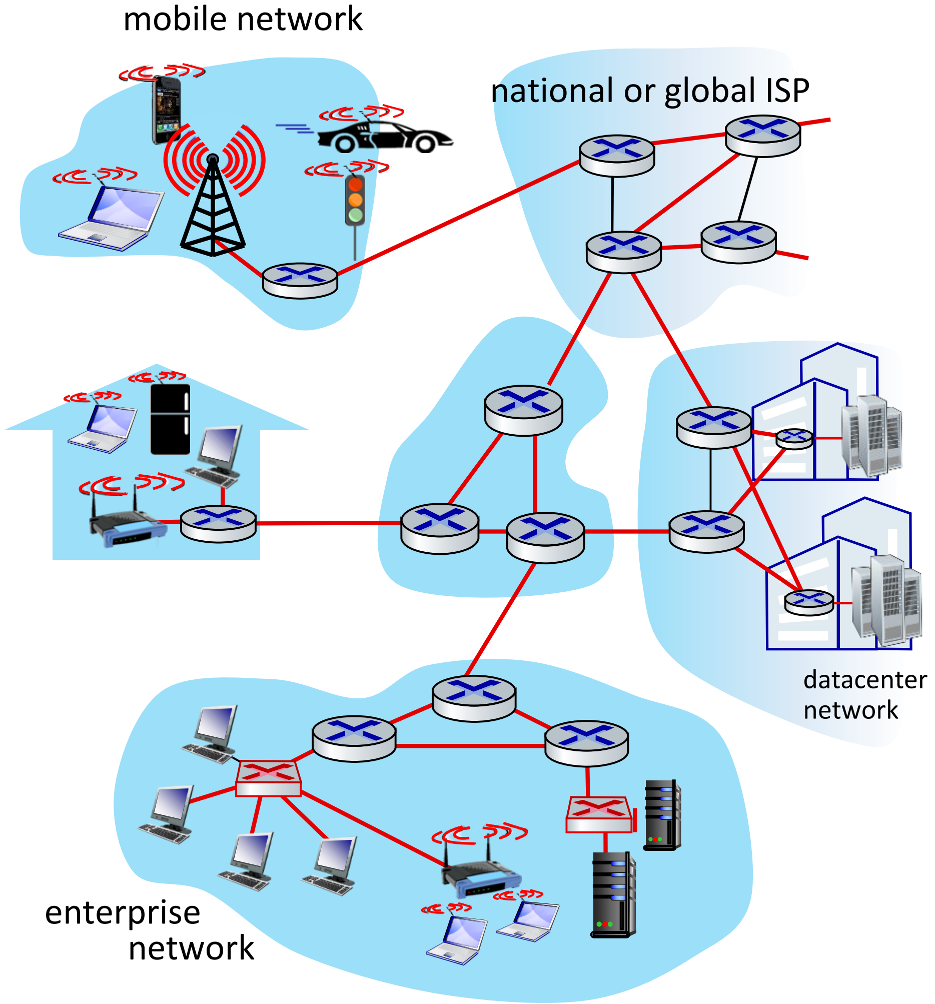
The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Link layer: introduction

terminology:

- hosts and routers: nodes
- communication channels that connect adjacent nodes along communication path: links
  - wired
  - wireless
  - LANs
- layer-2 packet: *frame*, encapsulates datagram

> *link layer has responsibility of transferring datagram from one node to physically adjacent node over a link*



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

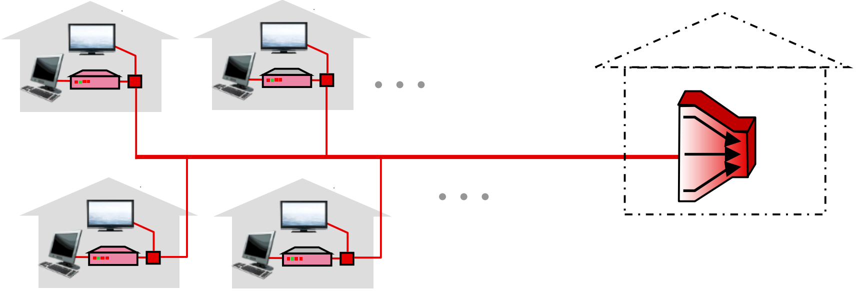
# Link layer: context

- datagram transferred by different link protocols over different links:
  - e.g., WiFi on first link, Ethernet on next link
- each link protocol provides different services
  - e.g., may or may not provide reliable data transfer over link

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Link layer: services

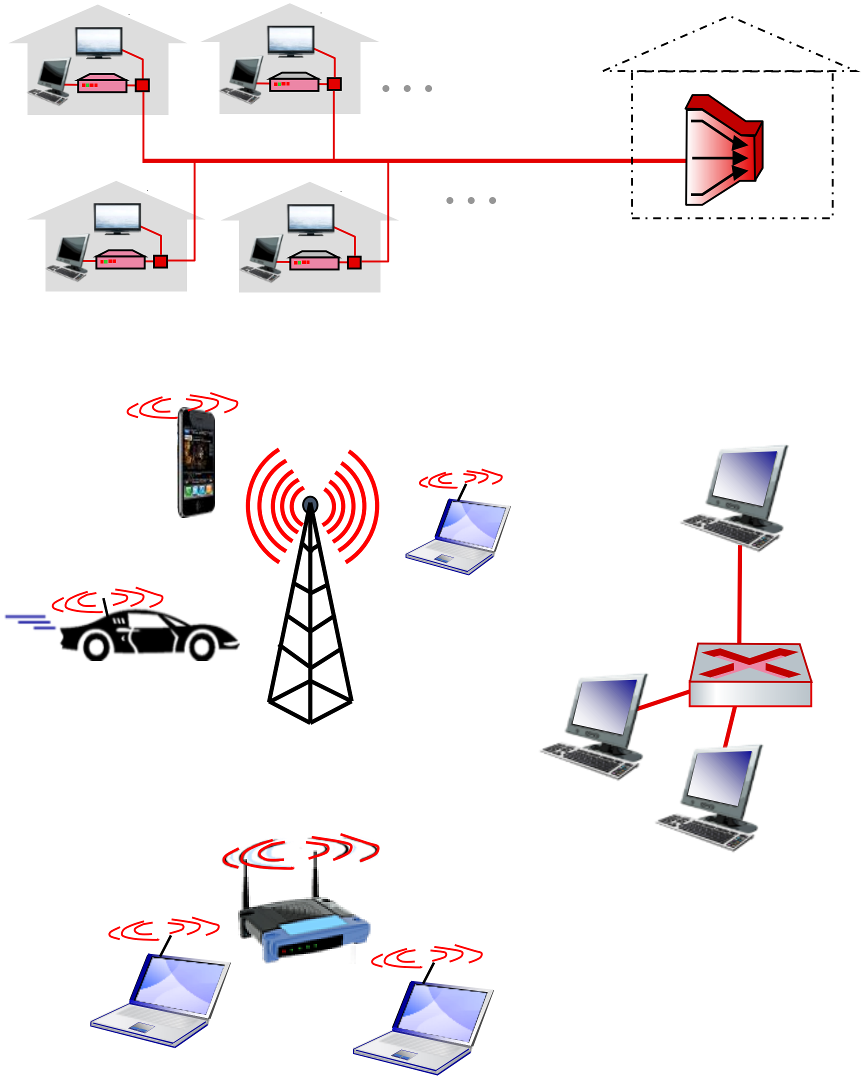
- framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - channel access
  - “Medium Access Control-MAC” addresses in frame headers identify source, destination
- reliable delivery between adjacent nodes
  - seldom used on low bit-error links (fiber, coax, and twisted-pair copper links)
  - often used for wireless links: high error rates
    - *Q:* why both link-level and end-end reliability?
    - correcting an error locally, on the link where the error occurs, rather than forcing an end-to-end retransmission of the data by a transport or application-layer protocol



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Link layer: services (more)

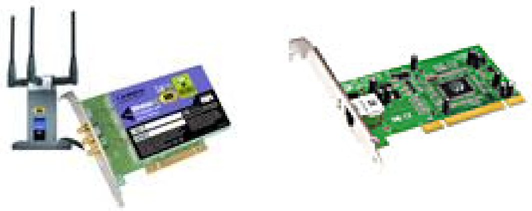
- flow control:
  - pacing between adjacent sending and receiving nodes
- error detection:
  - errors caused by signal attenuation, noise (bit errors, 0 instead of 1 or vice versa)
- error correction:
  - receiver identifies *and corrects* bit error(s) without retransmission
- half-duplex and full-duplex:
  - with half duplex, nodes at both ends of link can transmit, but not at same time

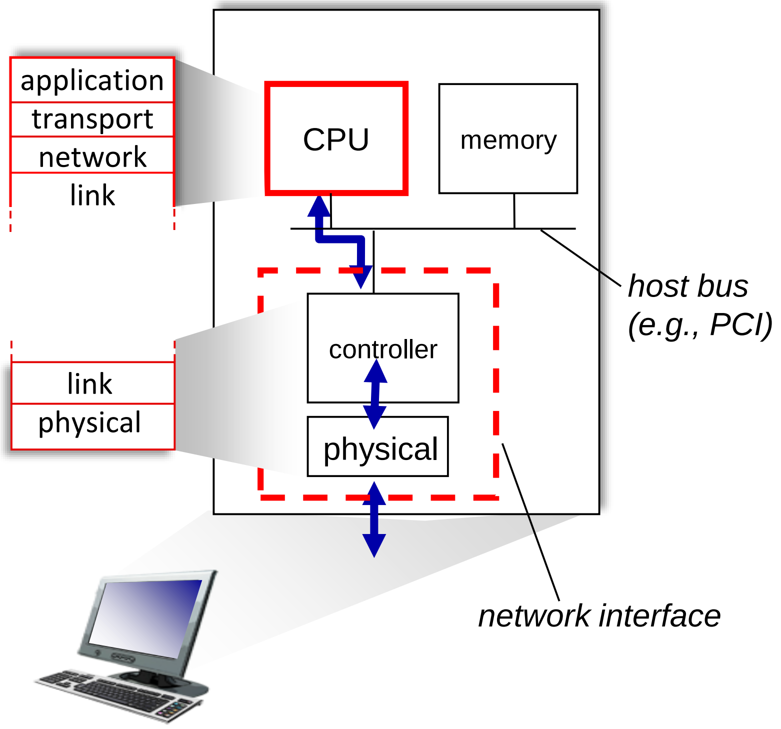


The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Where is the link layer implemented?

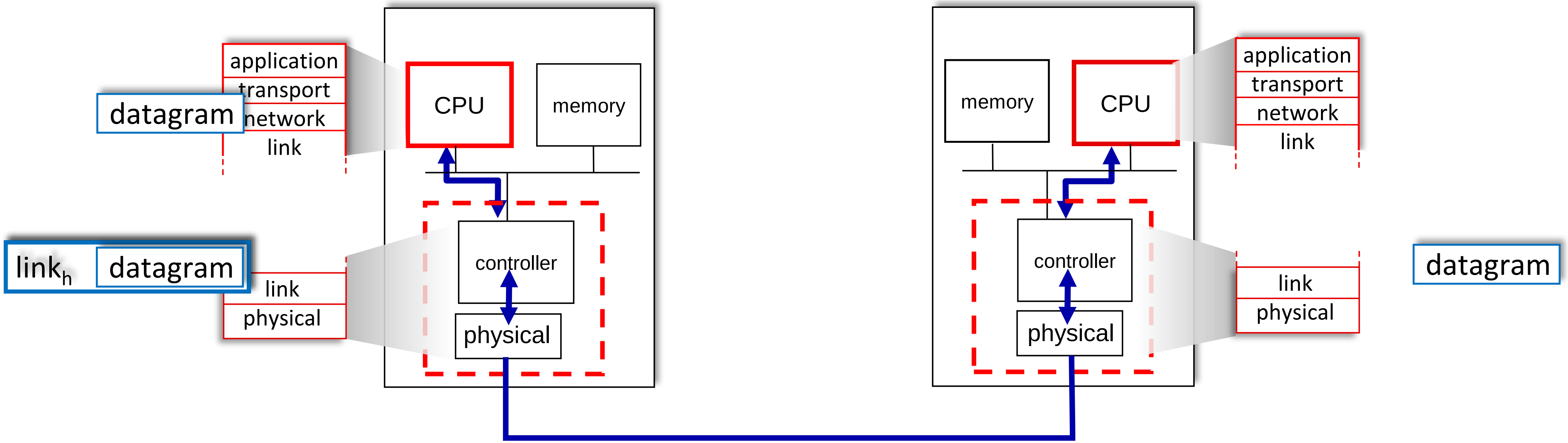
- in each-and-every host
- link layer implemented in *network (adapter) or interface card* (NIC) or on a chip (hardware)
  - Ethernet, WiFi card or chip
- attaches into host's system buses
- combination of hardware, software, firmware





The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Interfaces communicating



sending side:

- encapsulates datagram in frame
- adds error checking bits, reliable data transfer, flow control, etc.

receiving side:

- looks for errors, reliable data transfer, flow control, etc.
- extracts datagram, passes to upper layer at receiving side

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Link layer, LANs: roadmap

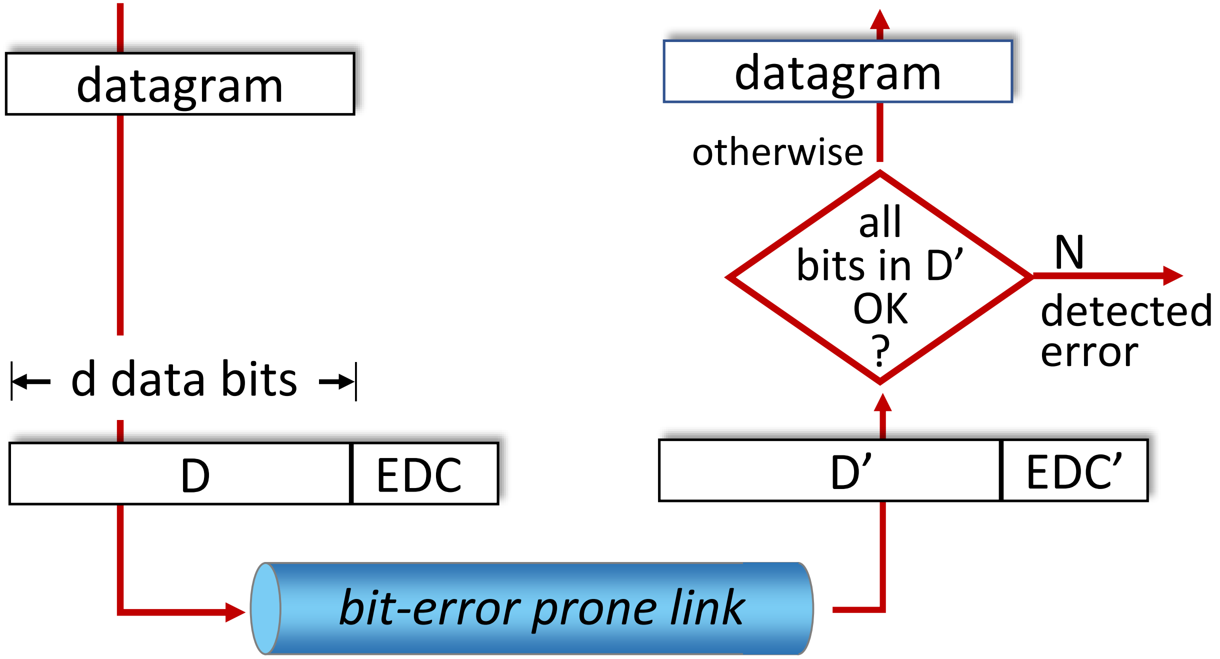
- introduction
- error detection
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Error detection

EDC: error detection and correction bits (e.g., redundancy)

D:  data protected by error checking, may include header fields



Error detection not 100% reliable!

- protocol may miss some errors, but rarely
- larger EDC field yields better detection and correction

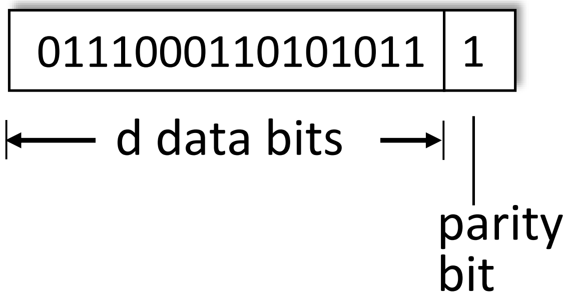
The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Parity checking

the simplest form of error detection

## single bit parity:

- detect single bit errors



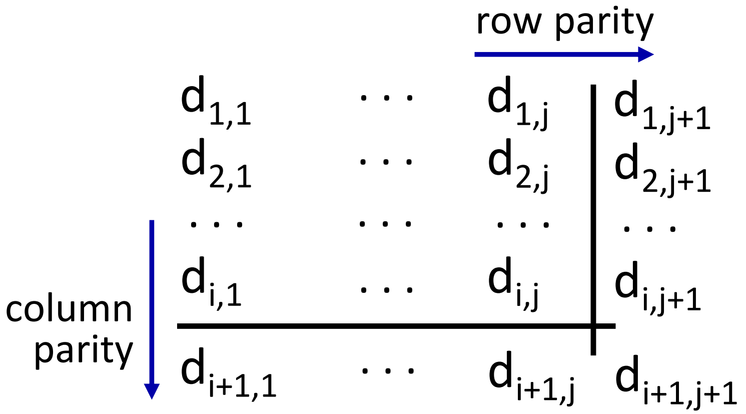
Even parity: set parity bit so there is an even number of 1’s (in d+1 bits)

total number of ones is counted, if it is not even, an error is likely to have occurred

only detects a single error, if two bits are flipped, it won’t catch it

## two-dimensional bit parity:

- detect *and correct* single bit errors



$$\begin{array}{cccc|c} d_{1,1} & \cdots & d_{1,j} & & d_{1,j+1} \\ d_{2,1} & \cdots & d_{2,j} & & d_{2,j+1} \\ \cdots & \cdots & \cdots & & \cdots \\ d_{i,1} & \cdots & d_{i,j} & & d_{i,j+1} \\ \hline d_{i+1,1} & \cdots & d_{i+1,j} & & d_{i+1,j+1} \end{array}$$

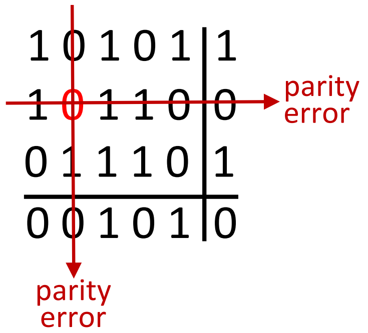
d bits are divided into i rows and j columns

a parity value is computed for each row and for each column

no errors:

$$\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 \end{array}$$

detected and correctable single-bit error:



$$\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 \end{array}$$

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Internet checksum

*Goal:* detect errors (*i.e.,* flipped bits) in transmitted segment

sender:

- treat contents of UDP segment (including UDP header fields and IP addresses) as sequence of 16-bit integers
- checksum: addition (one's complement sum) of segment content
- checksum value put into UDP checksum field

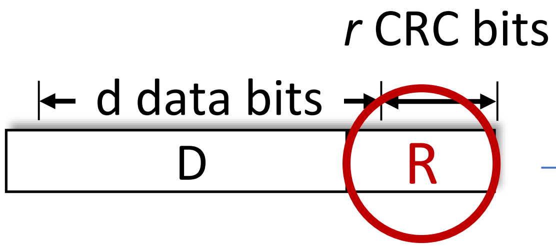
receiver:

- compute checksum of received segment
- check if computed checksum equals checksum field value:
  - not equal - error detected
  - equal - no error detected

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Cyclic Redundancy Check (CRC)

- the most powerful method
- D: data bits (given, think of these as a binary number)
- G: bit pattern (generator), of *r+1* bits (given)



bit pattern

$\langle D,R \rangle = D * 2^r$ XOR R

formula for bit pattern

*goal:* choose *r* CRC bits, R, such that <D,R> exactly divisible by G (mod 2)

- receiver knows G, divides <D,R> by G. If non-zero remainder: error detected!
- can detect all burst errors less than r+1 bits
- widely used in practice (Ethernet, 802.11 WiFi)

# Link layer, LANs: roadmap

- introduction
- error detection, correction
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# MAC addresses

- MAC (or LAN or physical or Ethernet) address:
  - function: used “locally” to get frame from one interface to another physically-connected interface (same subnet, 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

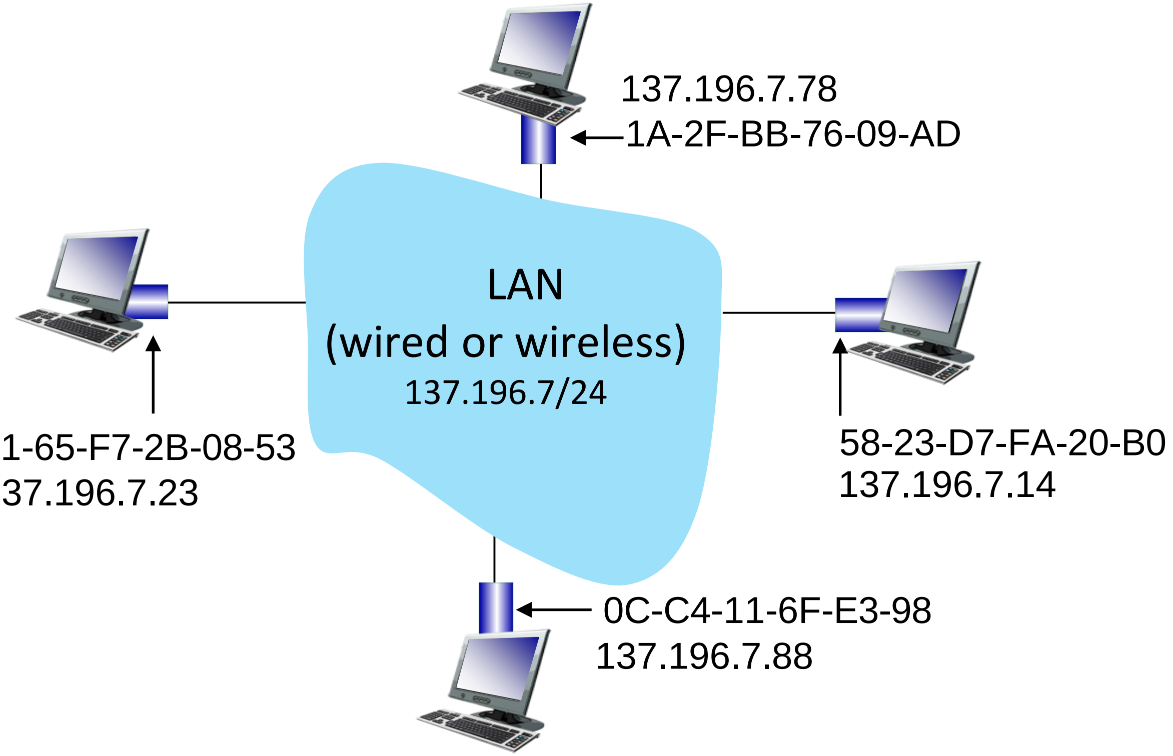
*hexadecimal (base 16) notation*
*(each “numeral” represents 4 bits)*

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# MAC addresses

each interface on LAN

- has unique 48-bit MAC address
- has a locally unique 32-bit IP address



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# MAC addresses

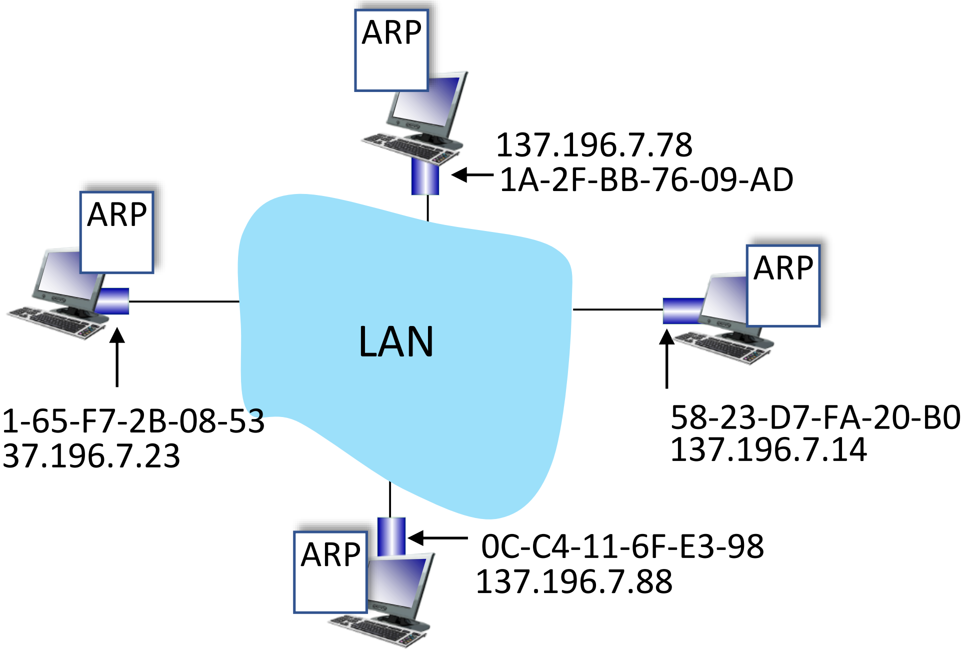
- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- MAC flat address: portability
  - can move interface from one LAN to another
  - recall IP address *not* portable: depends on IP subnet to which node is attached

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# ARP: address resolution protocol

*Question:* how to determine interface's MAC address, knowing its IP address? (IP addresses are NOT recognized by hardware)

*Address Resolution:* process of finding the hardware address (physical address) of a host given the IP address (logical address)



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

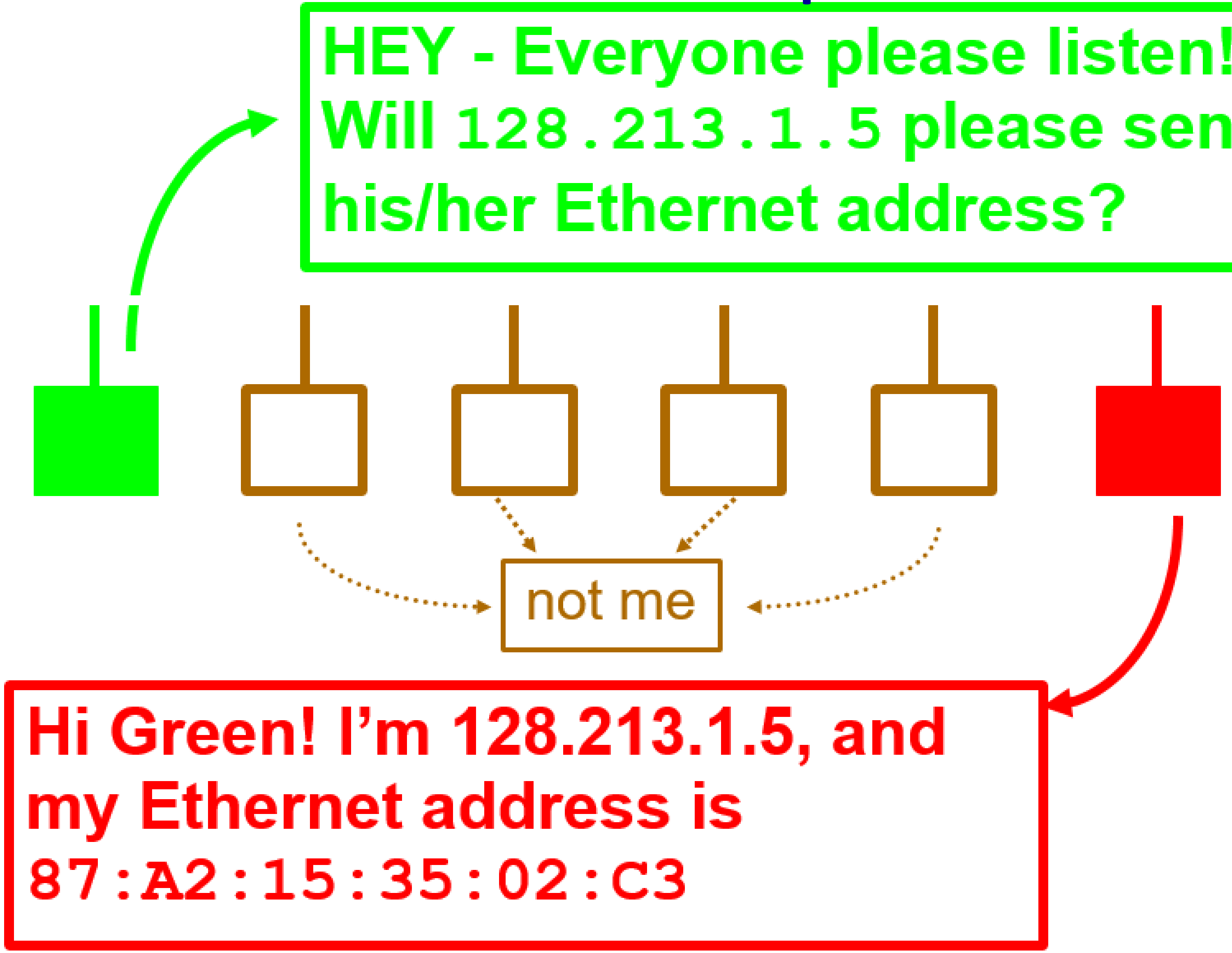
- IP/MAC address mappings for some LAN nodes:

  < IP address; MAC address; TTL>

- TTL (Time To Live): time after which address mapping will be forgotten

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# ARP: address resolution protocol



HEY - Everyone please listen!
Will 128.213.1.5 please send me his/her Ethernet address?

not me

Hi Green! I’m 128.213.1.5, and my Ethernet address is
87:A2:15:35:02:C3

* broadcast protocol (every host on the network receives the request)

* Layer 2 but should interoperate with Layer 3

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# ARP protocol in action

example: A wants to send datagram to B

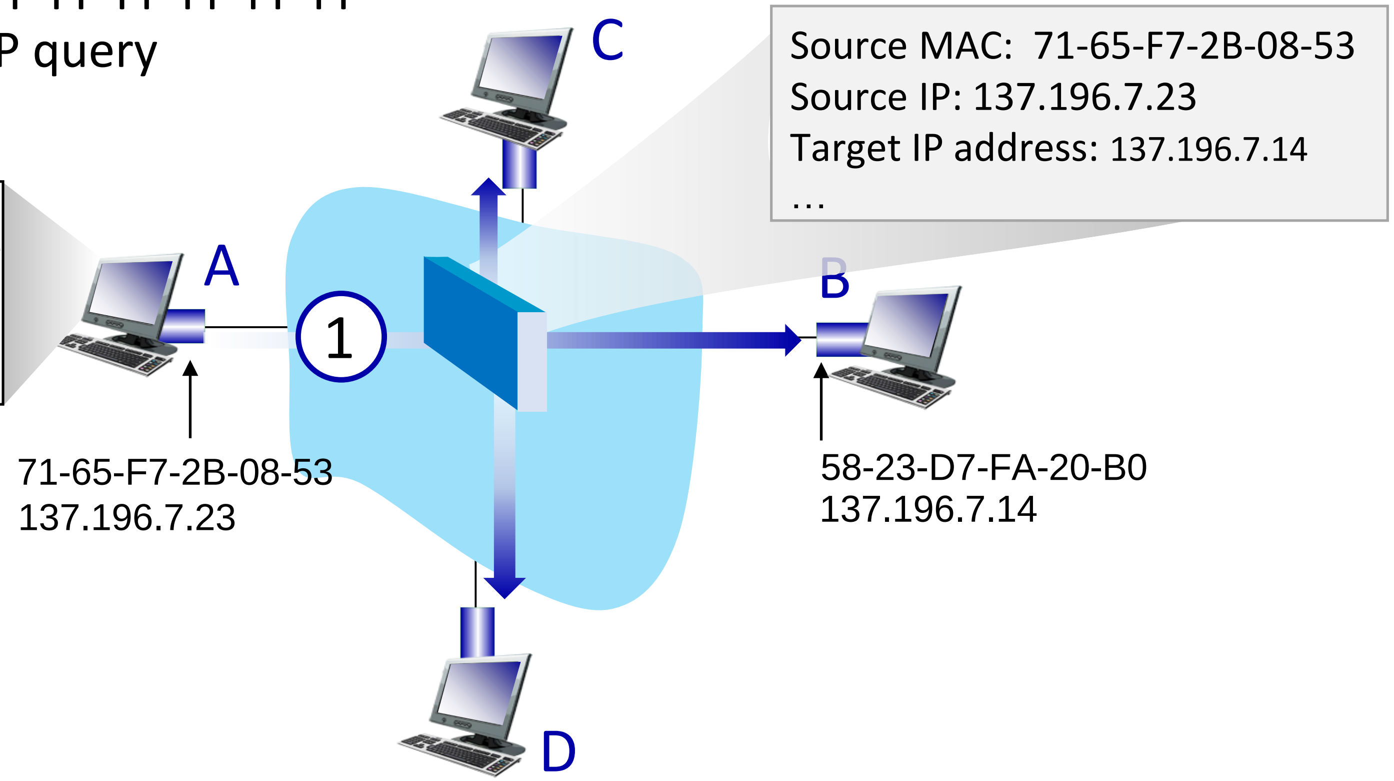
- B’s MAC address not in A’s ARP table, so A uses ARP to find B’s MAC address

1 A broadcasts ARP query, containing B's IP addr

- destination MAC address = FF-FF-FF-FF-FF-FF
- all nodes on LAN receive ARP query

ARP table in A

| IP addr | MAC addr | TTL |
|---|---|---|
|  |  |  |



Ethernet frame (sent to FF-FF-FF-FF-FF-FF)

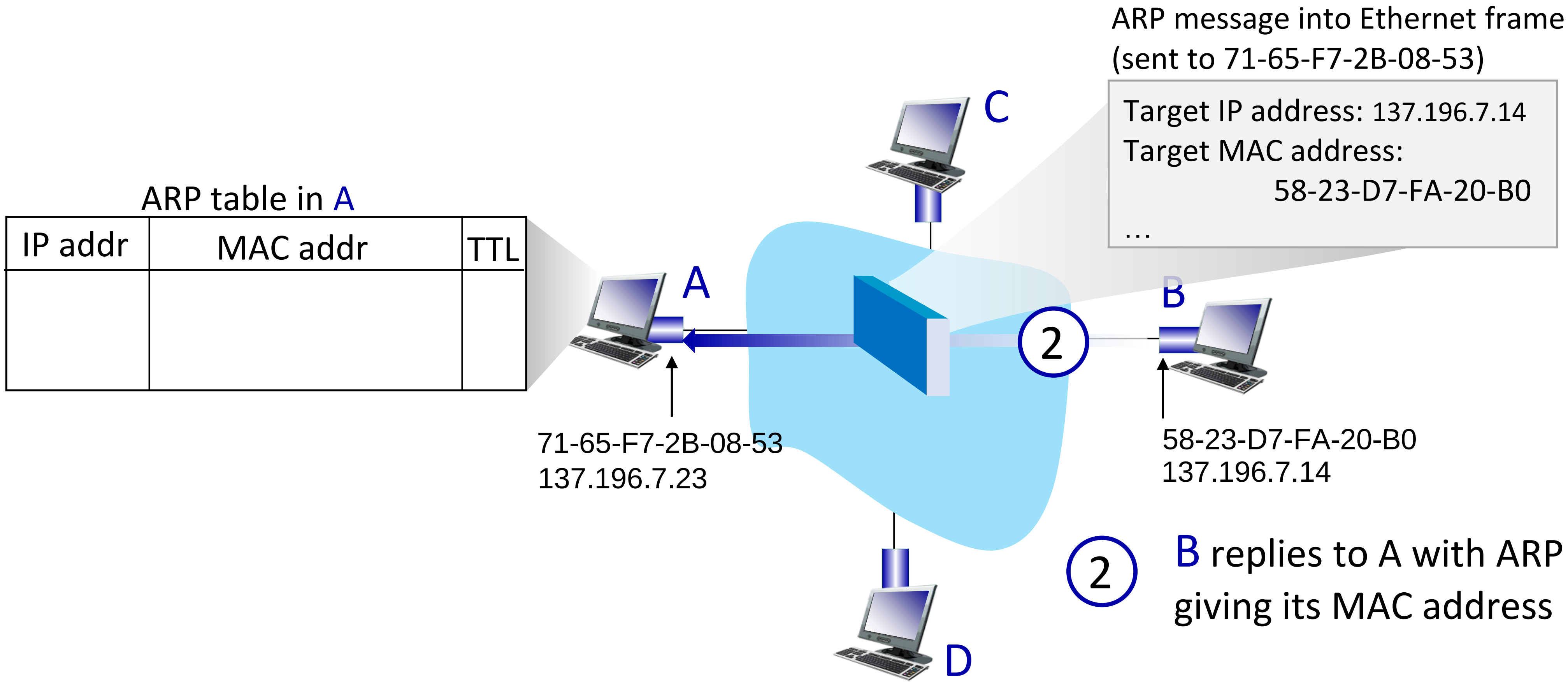
Source MAC: 71-65-F7-2B-08-53
Source IP: 137.196.7.23
Target IP address: 137.196.7.14
…

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# ARP protocol in action

example: A wants to send datagram to B

- B’s MAC address not in A’s ARP table, so A uses ARP to find B’s MAC address



ARP message into Ethernet frame (sent to 71-65-F7-2B-08-53)

Target IP address: 137.196.7.14
Target MAC address:
58-23-D7-FA-20-B0
…

ARP table in A

| IP addr | MAC addr | TTL |
|---|---|---|
|  |  |  |

2 B replies to A with ARP response, giving its MAC address

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

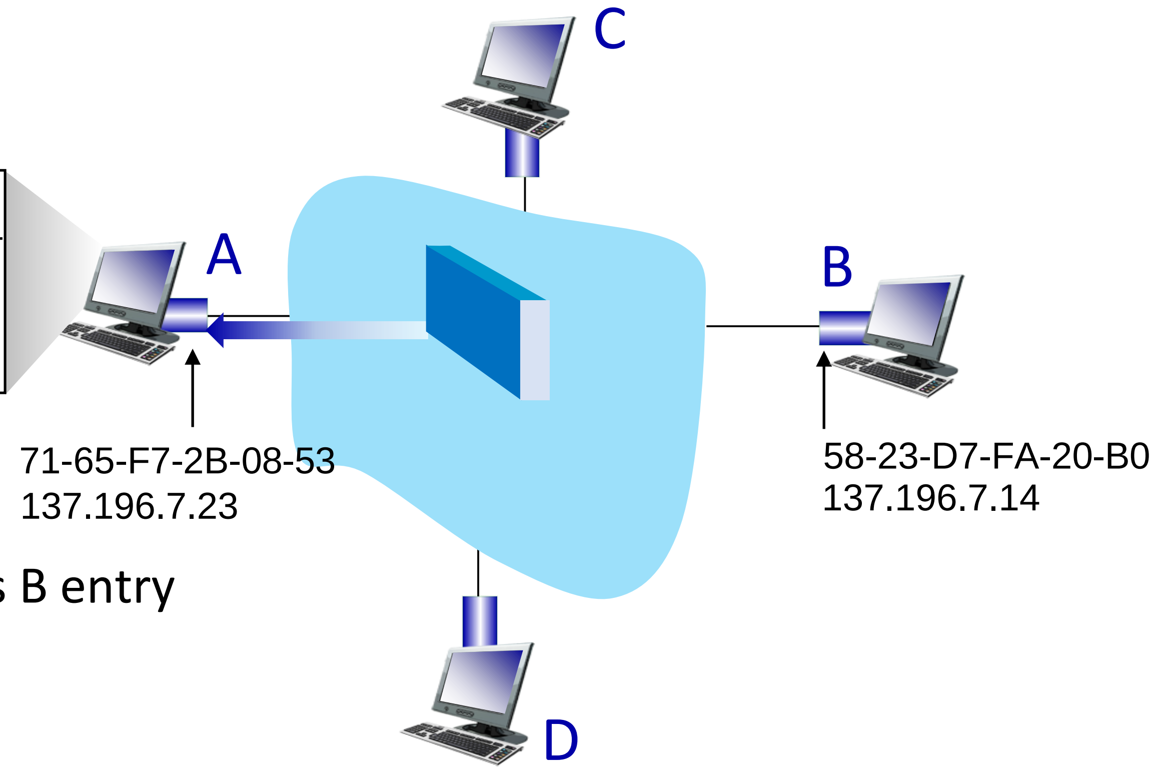
# ARP protocol in action

example: A wants to send datagram to B

- B’s MAC address not in A’s ARP table, so A uses ARP to find B’s MAC address

ARP table in A

| IP addr | MAC addr | TTL |
|---|---|---|
| 137.196. 7.14 | 58-23-D7-FA-20-B0 | 500 |

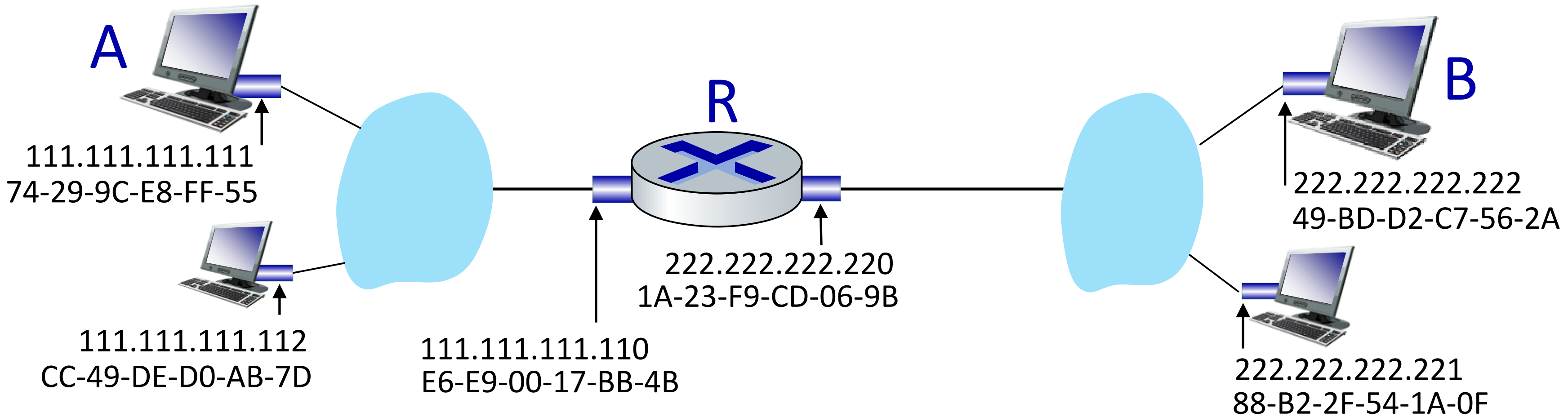


3 A receives B’s reply, adds B entry into its local ARP table

# Routing to another subnet: addressing

walkthrough: sending a datagram from *A* to *B* via *R*

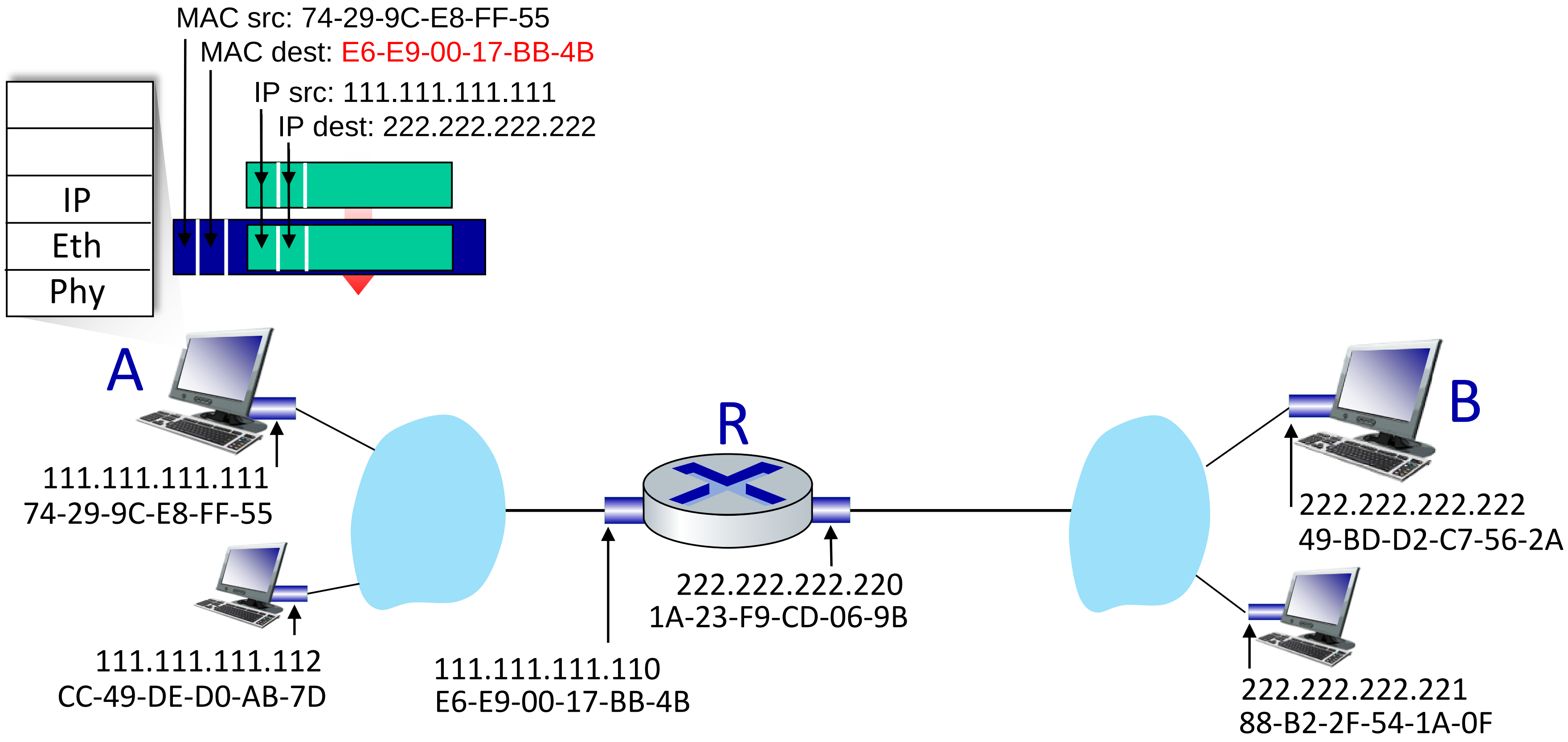
- focus on addressing – at IP (datagram) and MAC layer (frame) levels
- assume that:
  - A knows B's IP address
  - A knows IP address of first hop router, R
  - A knows R's MAC address



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

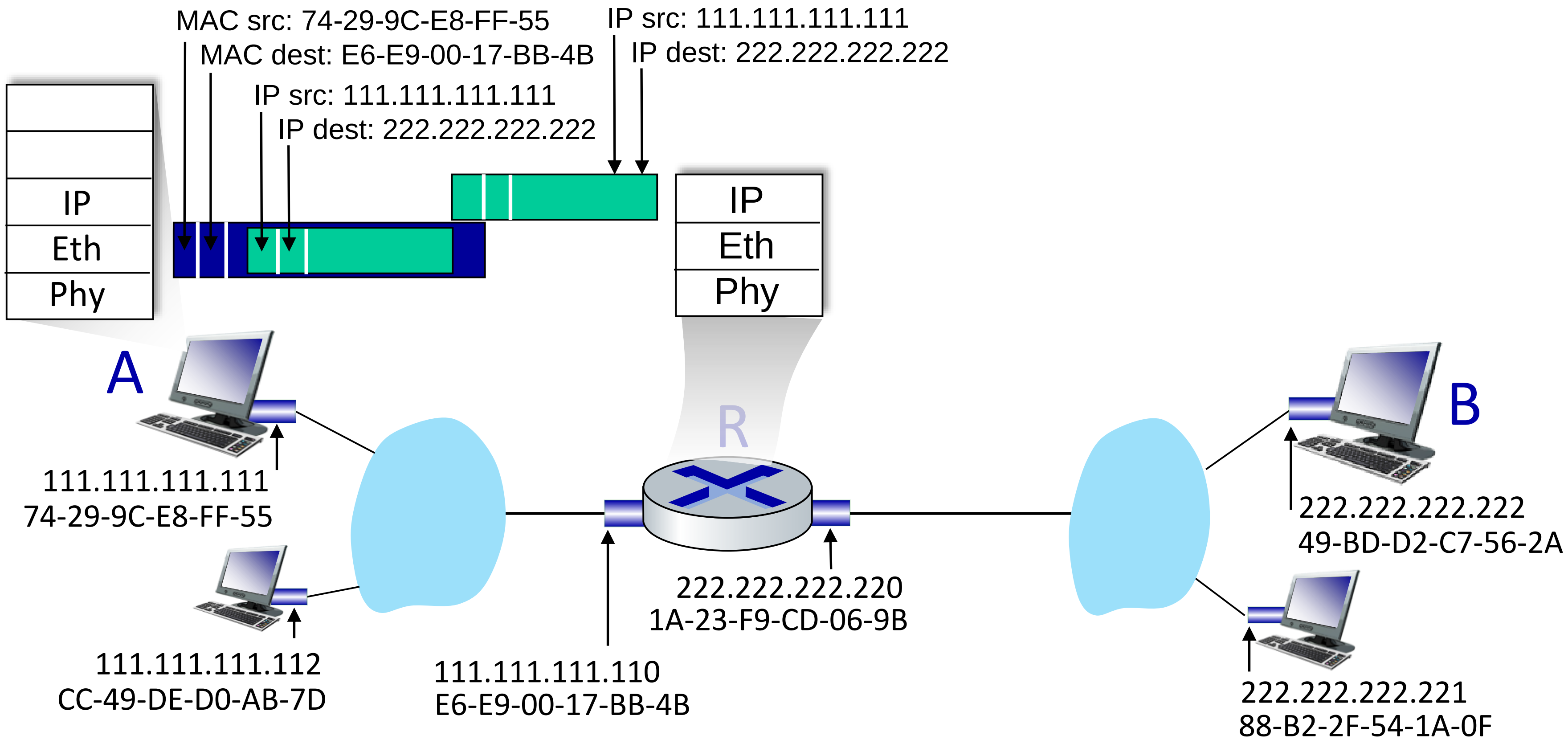
# Routing to another subnet: addressing

- A creates IP datagram with IP source A, destination B
- A creates link-layer frame containing A-to-B IP datagram
    - R's MAC address is frame's destination



# Routing to another subnet: addressing

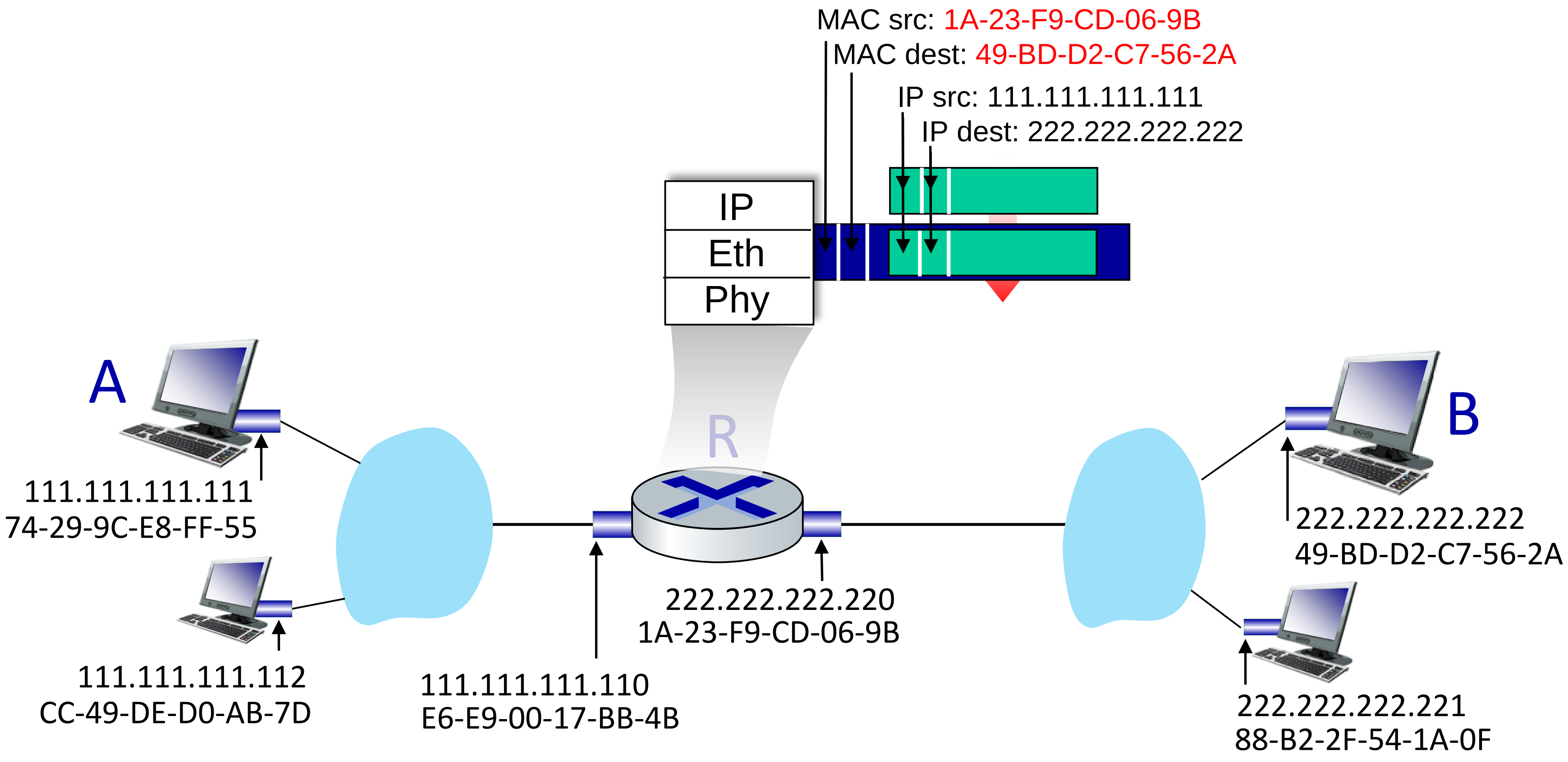
- frame sent from A to R
- frame received at R, datagram removed, passed up to IP



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Routing to another subnet: addressing

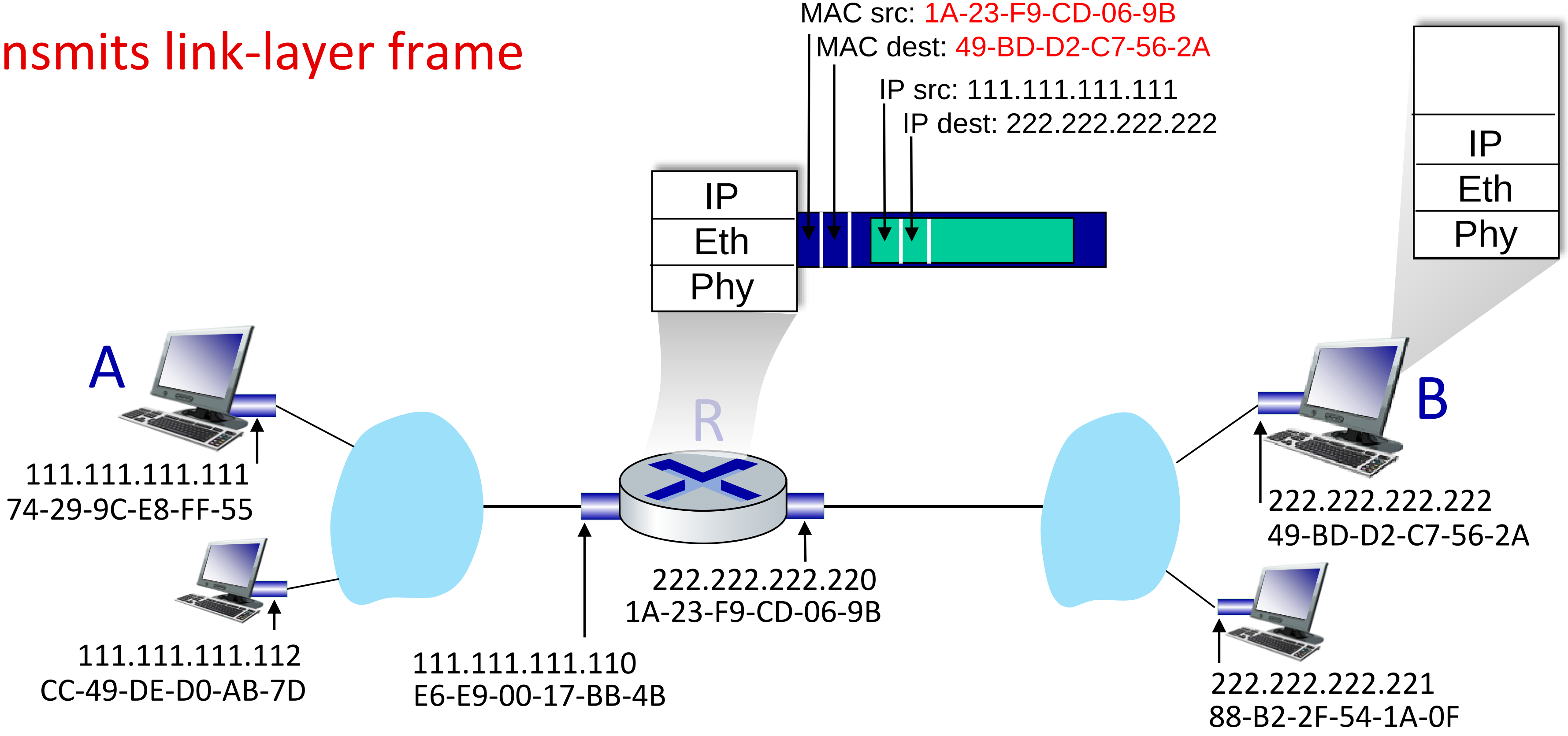
- R determines outgoing interface, passes datagram with IP source A, destination B to link layer
- R creates link-layer frame containing A-to-B IP datagram. Frame destination address: B's MAC address



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Routing to another subnet: addressing

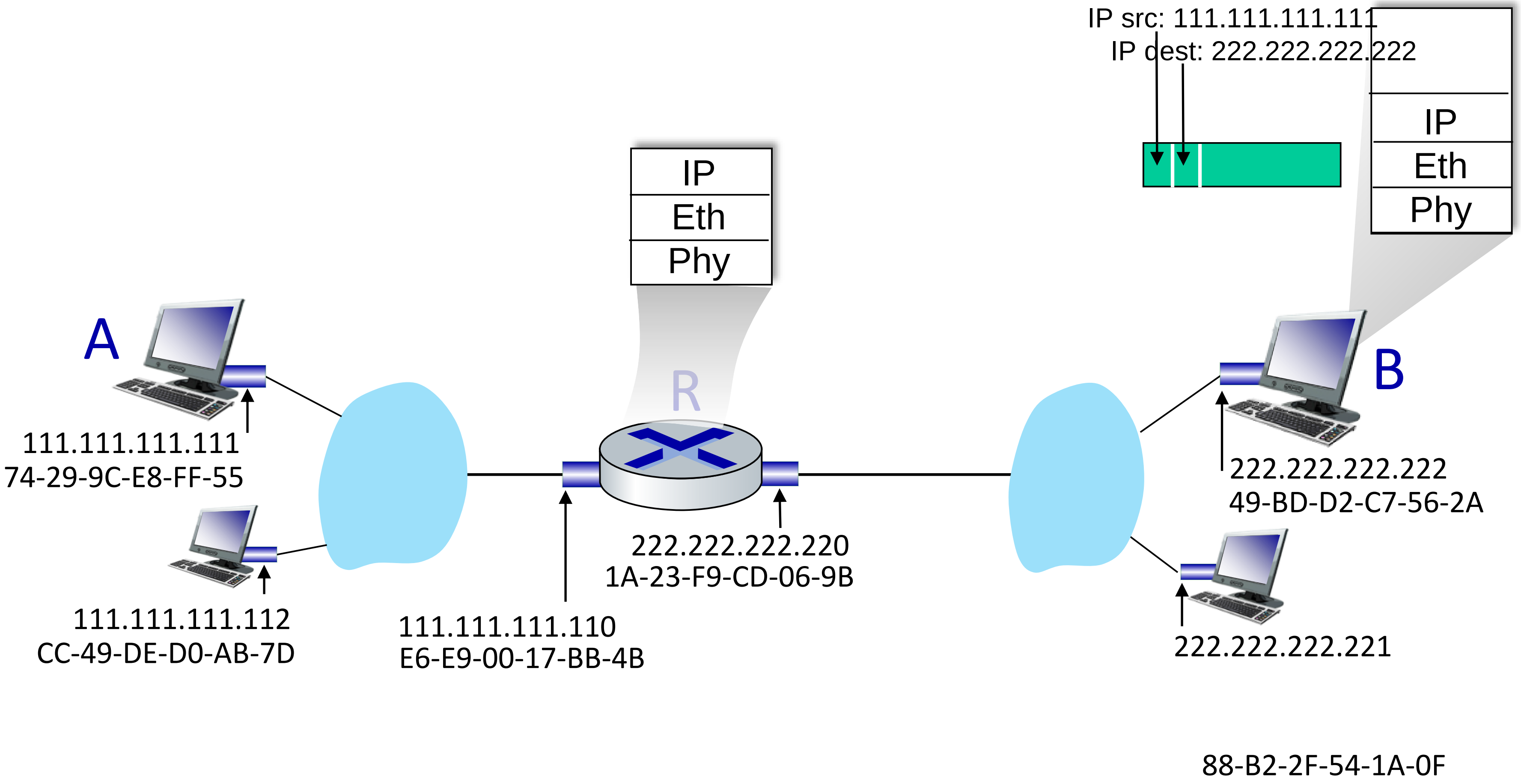
- R determines outgoing interface, passes datagram with IP source A, destination B to link layer
- R creates link-layer frame containing A-to-B IP datagram. Frame destination address: B's MAC address
- transmits link-layer frame



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Routing to another subnet: addressing

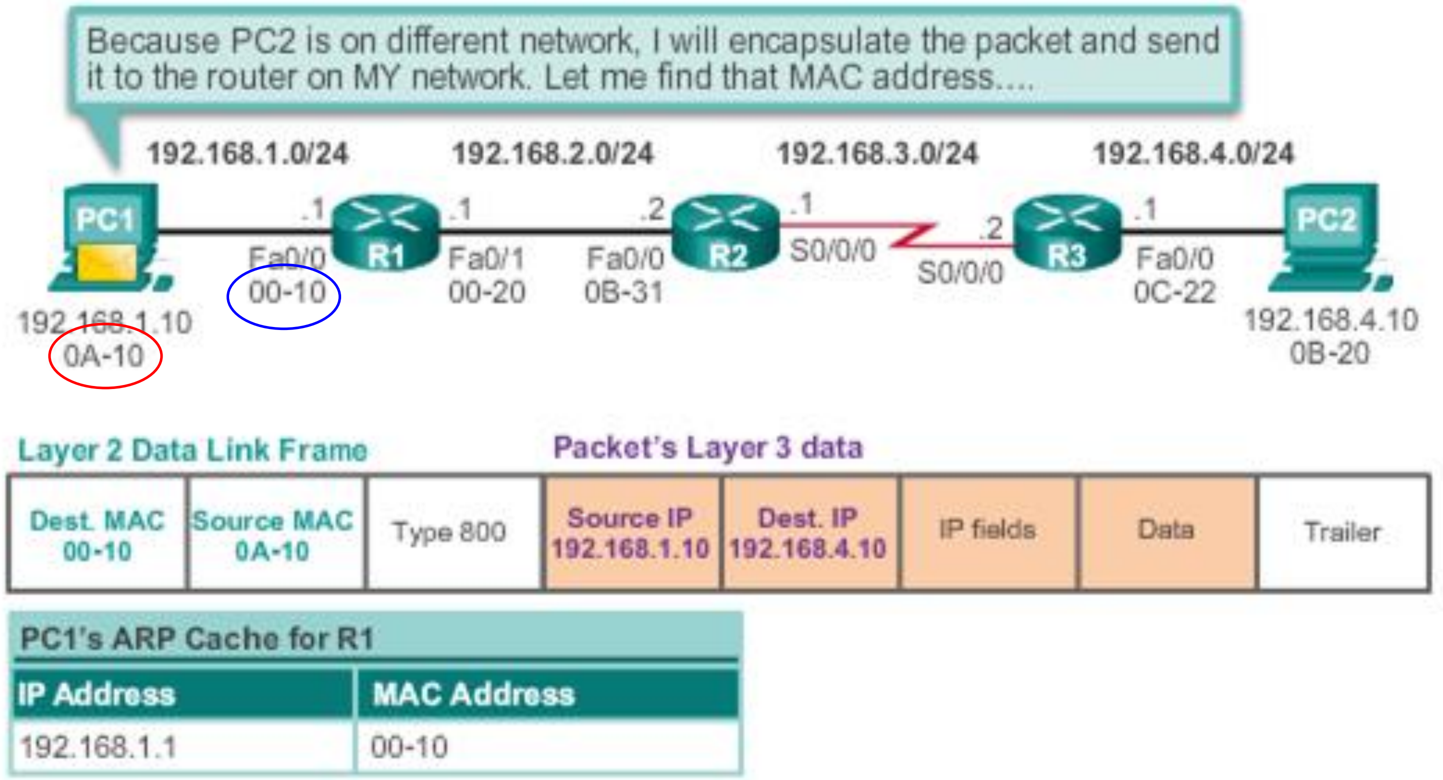
- B receives frame, extracts IP datagram destination B
- B passes datagram up protocol stack to IP



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Routing to another subnet: addressing

PC1 Sends a Packet to PC2



Because PC2 is on different network, I will encapsulate the packet and send it to the router on MY network. Let me find that MAC address....

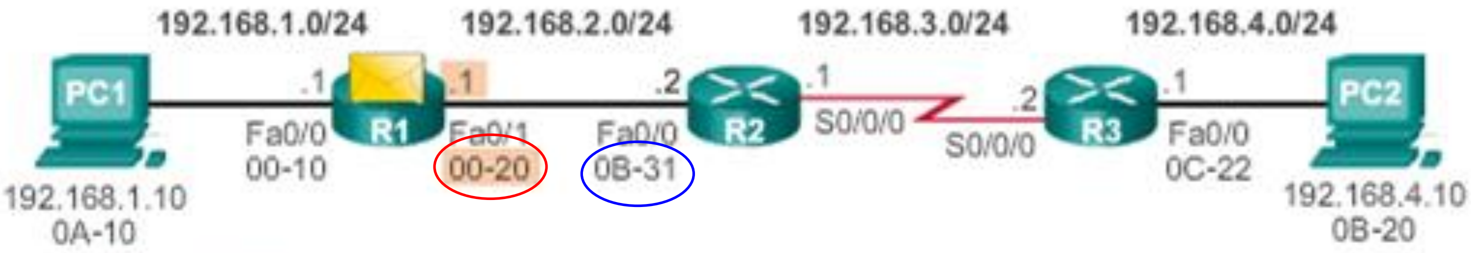
| Layer 2 Data Link Frame | | | Packet's Layer 3 data | | | | |
|---|---|---|---|---|---|---|---|
| Dest. MAC<br>00-10 | Source MAC<br>0A-10 | Type 800 | Source IP<br>192.168.1.10 | Dest. IP<br>192.168.4.10 | IP fields | Data | Trailer |

PC1's ARP Cache for R1

| IP Address | MAC Address |
|---|---|
| 192.168.1.1 | 00-10 |

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Routing to another subnet: addressing



Layer 2 Data Link Frame

Packet's Layer 3 data

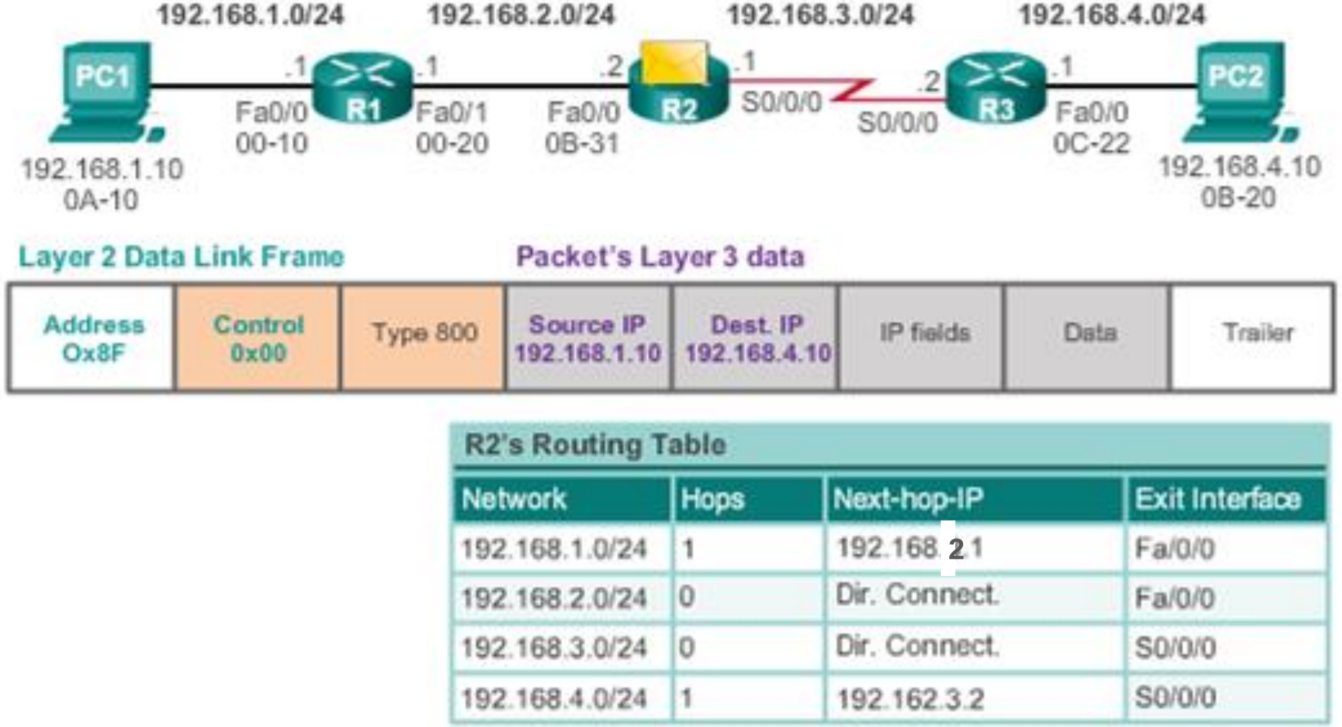
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Dest. MAC<br>0B-31 | Source MAC<br>00-20 | Type 800 | Source IP<br>192.168.1.10 | Dest. IP<br>192.168.4.10 | IP fields | Data | Trailer |

**R1's Routing Table**

| Network | Hops | Next-hop-IP | Exit Interface |
|---|---|---|---|
| 192.168.1.0/24 | 0 | Dir. Connect. | Fa0/0 |
| 192.168.2.0/24 | 0 | Dir. Connect. | Fa0/1 |
| 192.168.3.0/24 | 1 | 192.168.2.2 | Fa0/1 |
| 192.168.4.0/24 | 2 | 192.168.2.2 | Fa0/1 |

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Routing to another subnet: addressing

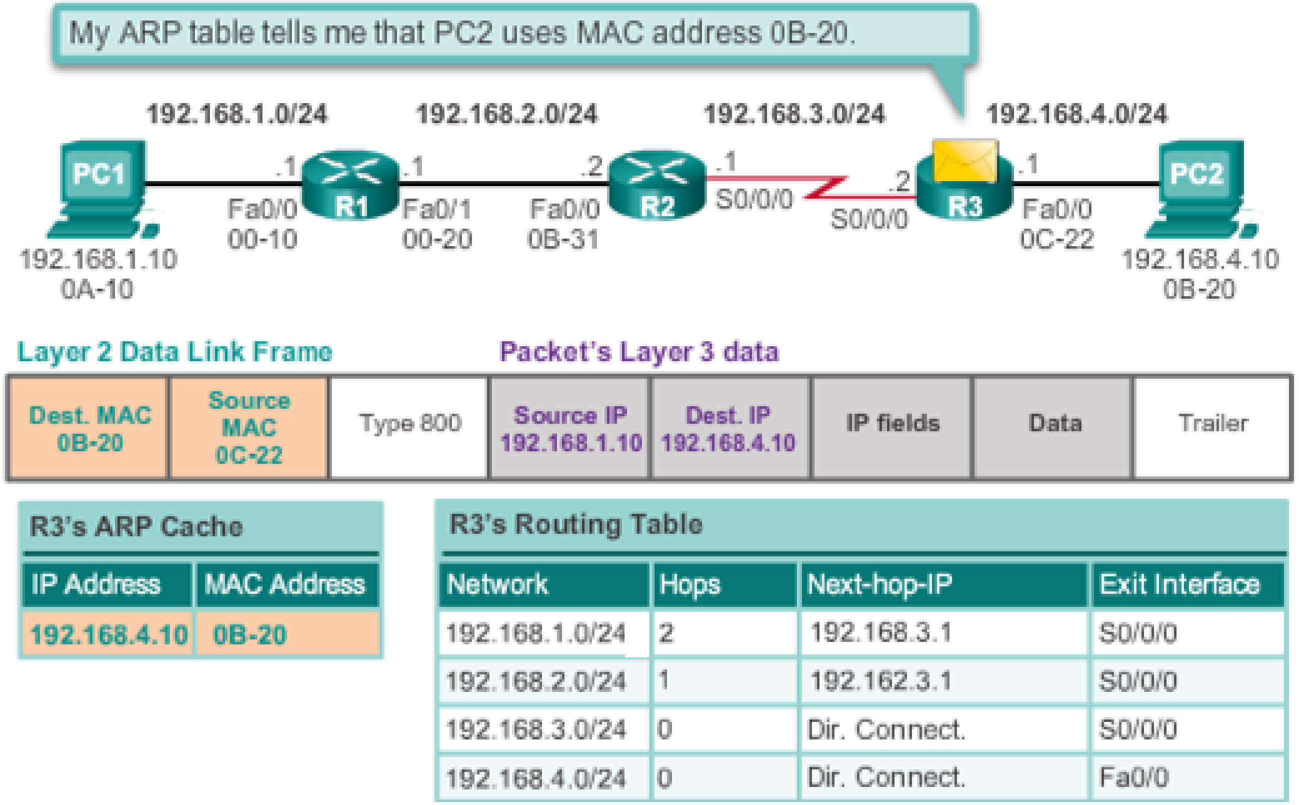


| Layer 2 Data Link Frame | | | Packet's Layer 3 data | | | | |
|---|---|---|---|---|---|---|---|
| Address<br>Ox8F | Control<br>0x00 | Type 800 | Source IP<br>192.168.1.10 | Dest. IP<br>192.168.4.10 | IP fields | Data | Trailer |

R2's Routing Table

| Network | Hops | Next-hop-IP | Exit Interface |
|---|---|---|---|
| 192.168.1.0/24 | 1 | 192.168.2.1 | Fa/0/0 |
| 192.168.2.0/24 | 0 | Dir. Connect. | Fa/0/0 |
| 192.168.3.0/24 | 0 | Dir. Connect. | S0/0/0 |
| 192.168.4.0/24 | 1 | 192.162.3.2 | S0/0/0 |

# Routing to another subnet: addressing


My ARP table tells me that PC2 uses MAC address 0B-20.

Layer 2 Data Link Frame | Packet's Layer 3 data

| Dest. MAC<br>0B-20 | Source MAC<br>0C-22 | Type 800 | Source IP<br>192.168.1.10 | Dest. IP<br>192.168.4.10 | IP fields | Data | Trailer |
|---|---|---|---|---|---|---|---|

R3's ARP Cache

| IP Address | MAC Address |
|---|---|
| 192.168.4.10 | 0B-20 |

R3's Routing Table

| Network | Hops | Next-hop-IP | Exit Interface |
|---|---|---|---|
| 192.168.1.0/24 | 2 | 192.168.3.1 | S0/0/0 |
| 192.168.2.0/24 | 1 | 192.162.3.1 | S0/0/0 |
| 192.168.3.0/24 | 0 | Dir. Connect. | S0/0/0 |
| 192.168.4.0/24 | 0 | Dir. Connect. | Fa0/0 |

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Link layer, LANs: roadmap

- introduction
- error detection, correction
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

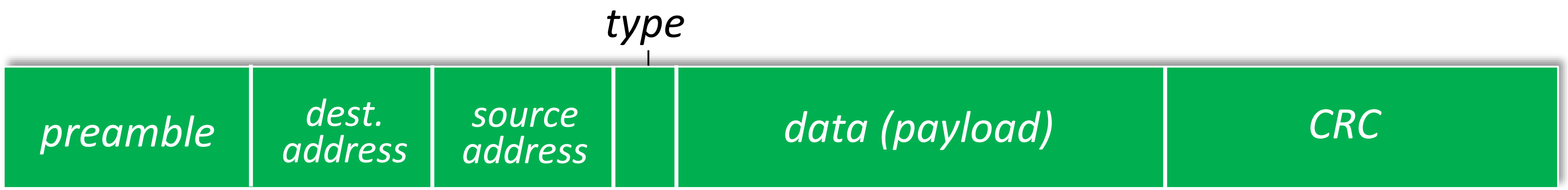
# Ethernet

"dominant" wired LAN technology:

- first widely used LAN technology
- simpler, cheap

# Ethernet frame structure

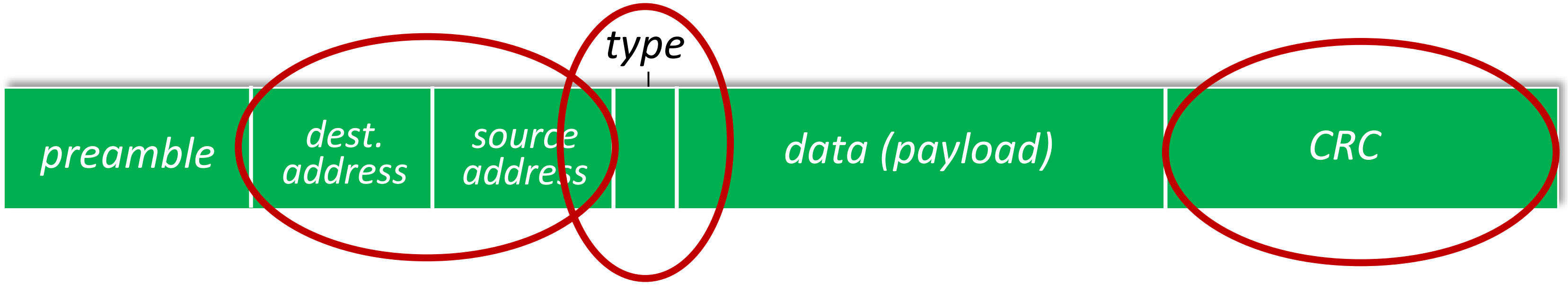
sending interface encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame



*preamble:*

- used to synchronize receiver, sender clock rates (10 Mbps, 100 Mbps, or 1 Gbps)
- 8 bytes

# Ethernet frame structure (more)



- addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- type: indicates higher layer protocol
  - mostly IP but others possible, e.g., Novell IPX, AppleTalk
  - used to demultiplex up at receiver
- CRC: cyclic redundancy check at receiver
  - error detected: frame is dropped

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

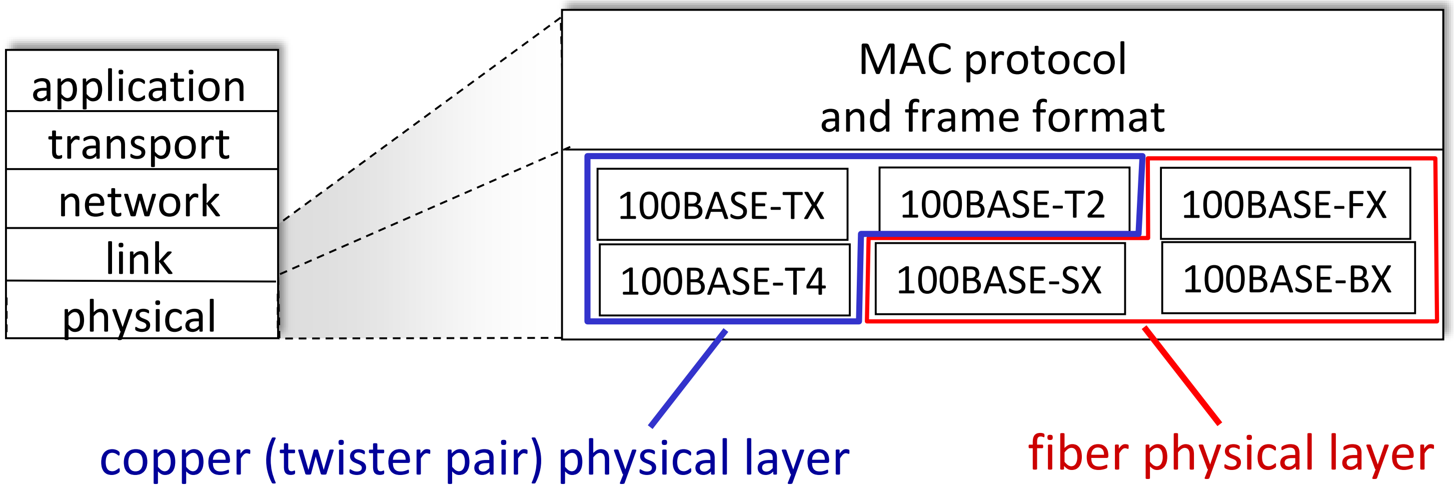
# Ethernet: unreliable, connectionless

- connectionless: no handshaking between sending and receiving NICs
- unreliable: receiving NIC doesn't send ACKs
  - data in dropped frames recovered only if initial sender uses higher layer reliable data transfer (e.g., TCP), otherwise dropped data lost

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# 802.3 Ethernet standards: link & physical layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps
  - different physical layer media: fiber, cable



# Link layer, LANs: roadmap

- introduction
- error detection, correction
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs

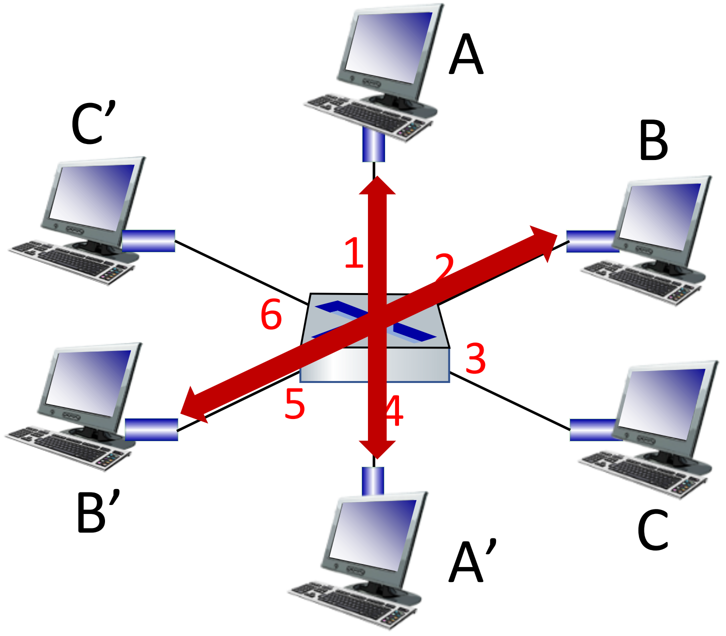
The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Ethernet switch

- Switch is a link-layer device: takes an *active* role
  - store, forward Ethernet frames
  - examine incoming frame's MAC address, *selectively* forward frame to one-or-more outgoing links
- transparent: hosts *unaware* of presence of switches
- plug-and-play, self-learning

# Switch: multiple simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link:
  - no collisions; full duplex
- switching: A-to-A’ and B-to-B’ can transmit simultaneously, without collisions (but A-to-A’ and C to A’ can not happen simultaneously)



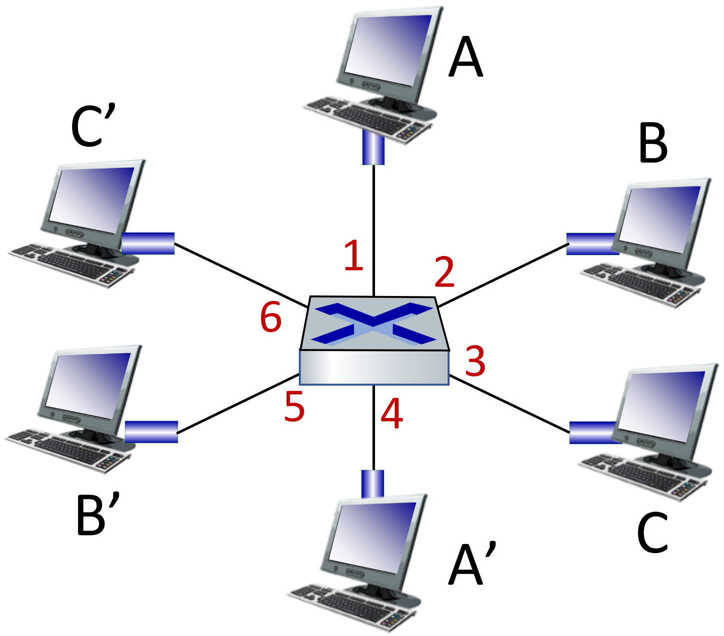
switch with six interfaces (1,2,3,4,5,6)

# Switch forwarding table

*Q:* how does switch know A' reachable via interface 4, B' reachable via interface 5?

*A:* each switch has a switch table, each entry:

- (MAC address of host, interface to reach host)
- like a routing table

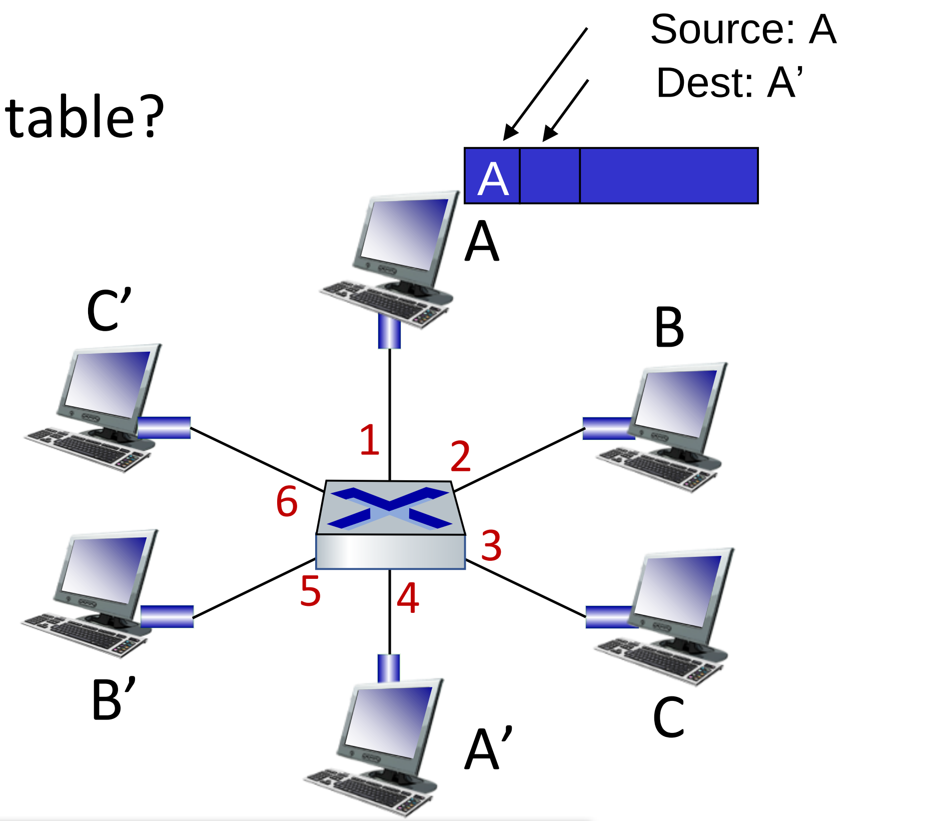


The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Switch: self-learning

how are entries created, maintained in switch table?

- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table



| MAC addr | interface | TTL |
|---|---|---|
| *A* | *1* | *60* |

*Switch table (initially empty)*

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Switch: frame filtering/forwarding

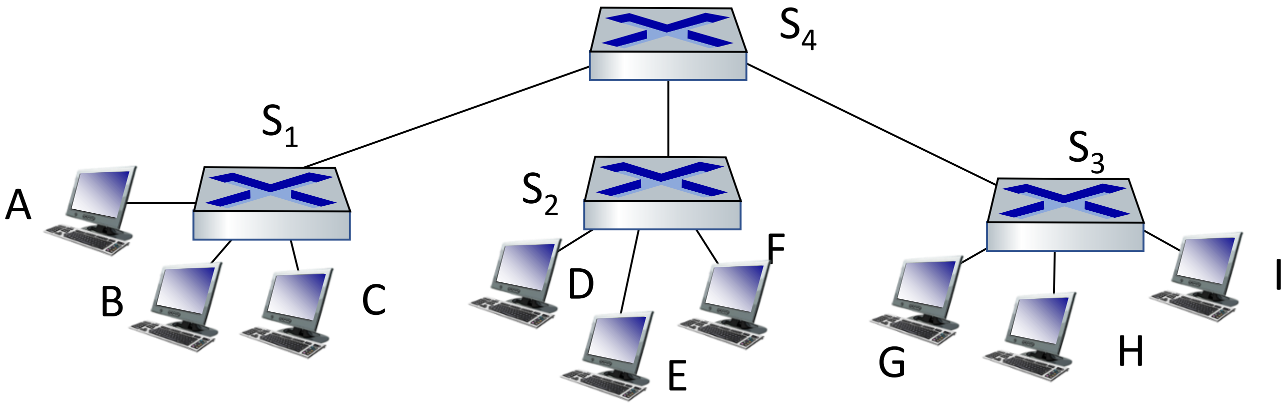
```
when  frame received at switch:

    1. record incoming link, MAC address of sending host
    2. index switch table using MAC destination address
    3. if entry found for destination
        then {
        if destination on segment from which frame arrived
            then drop frame
             else forward frame on interface indicated by entry
          }
         else flood  /* forward on all interfaces except arriving interface */
```

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Interconnecting switches

self-learning switches can be connected together:

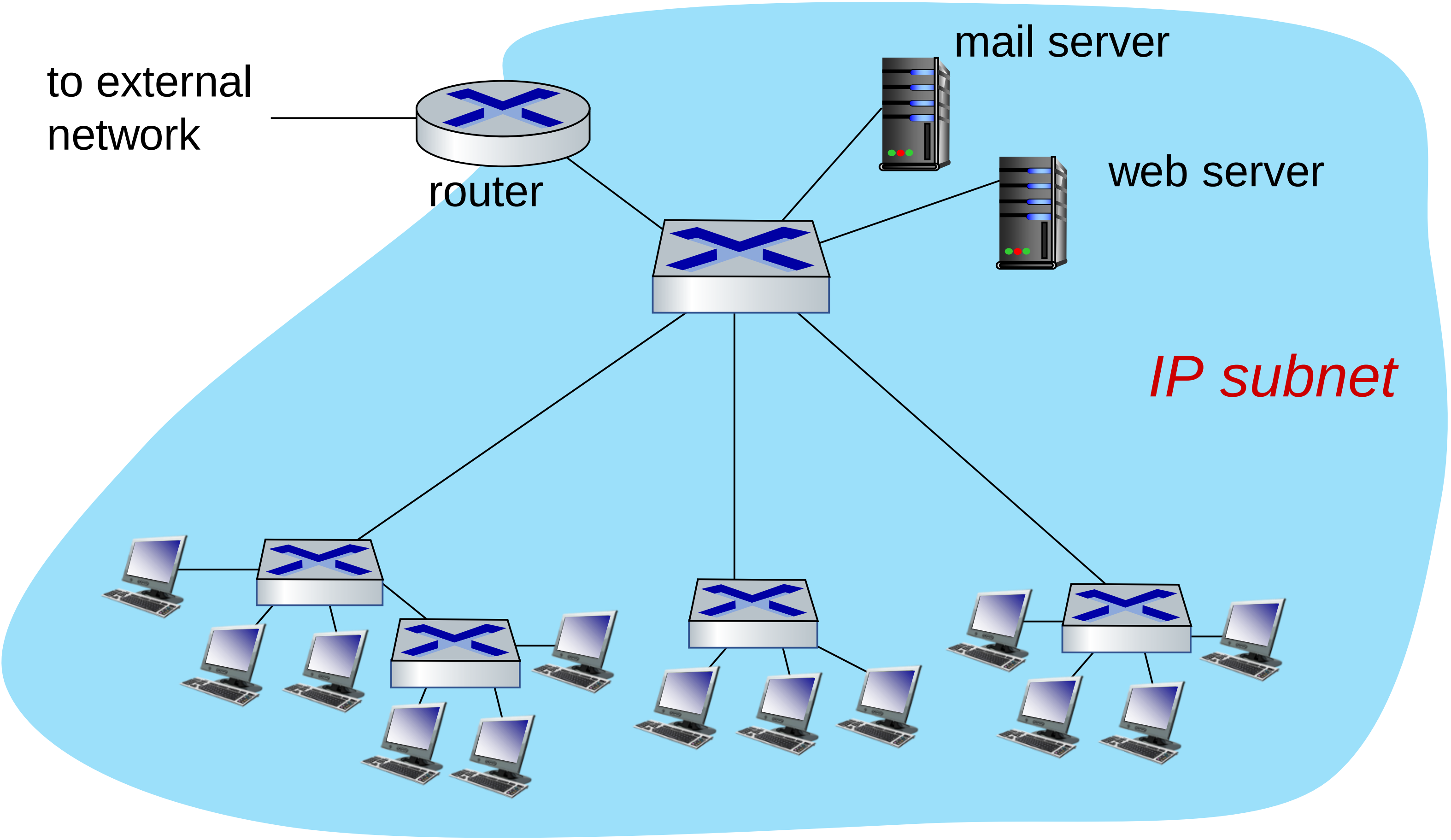


*Q:* sending from A to G - how does $S_1$ know to forward frame destined to G via $S_4$ and $S_3$?

- *A:* self learning (works exactly the same as in single-switch case)

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Small institutional network



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

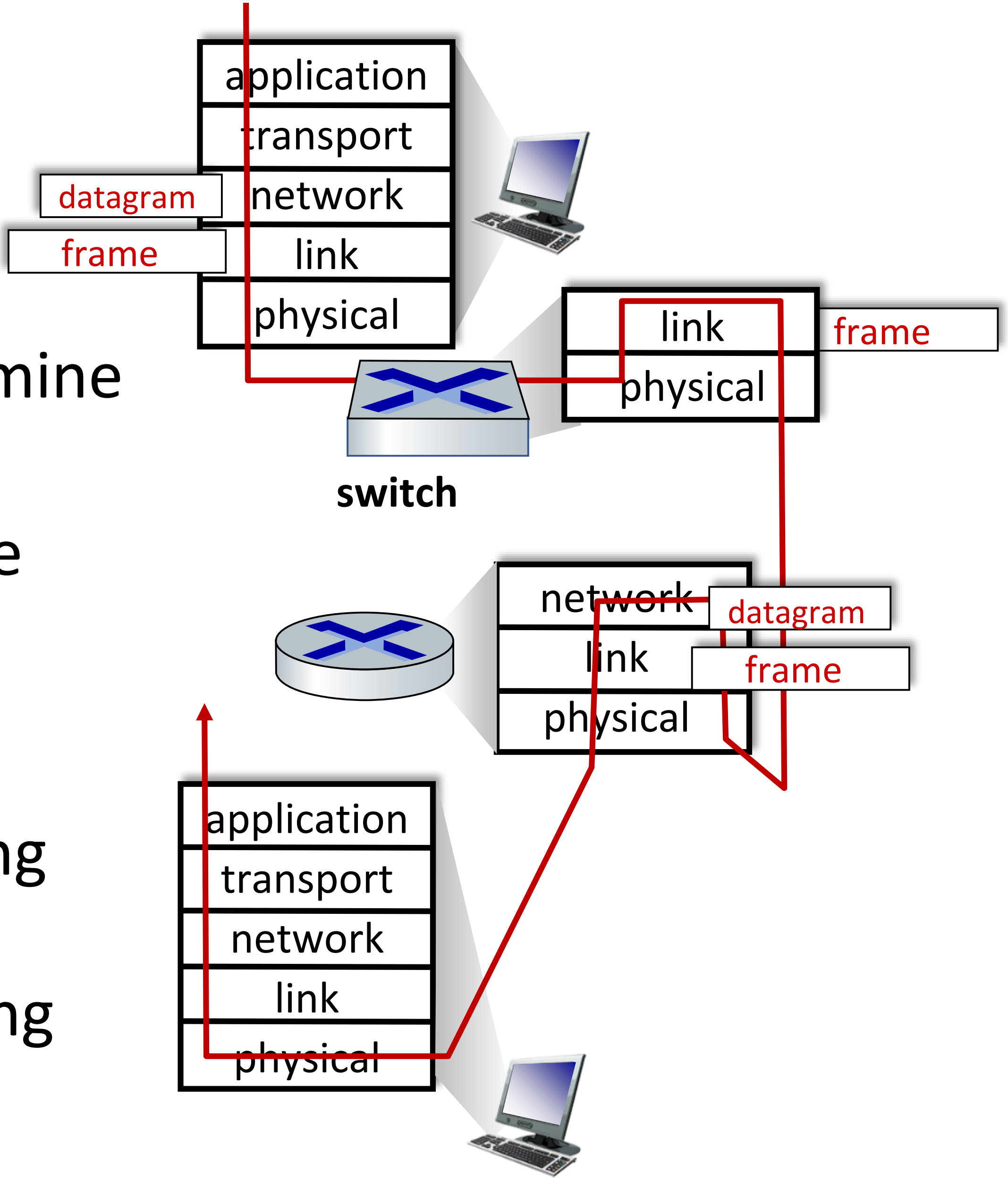
# Switches vs. routers

## both are store-and-forward:

- *routers*: network-layer devices (examine network-layer headers)
- *switches:* link-layer devices (examine link-layer headers)

## both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Link layer, LANs: roadmap

- introduction
- error detection, correction
- LANs
  - addressing, ARP
  - Ethernet
  - switches
  - VLANs

The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Virtual LANs (VLANs): motivation

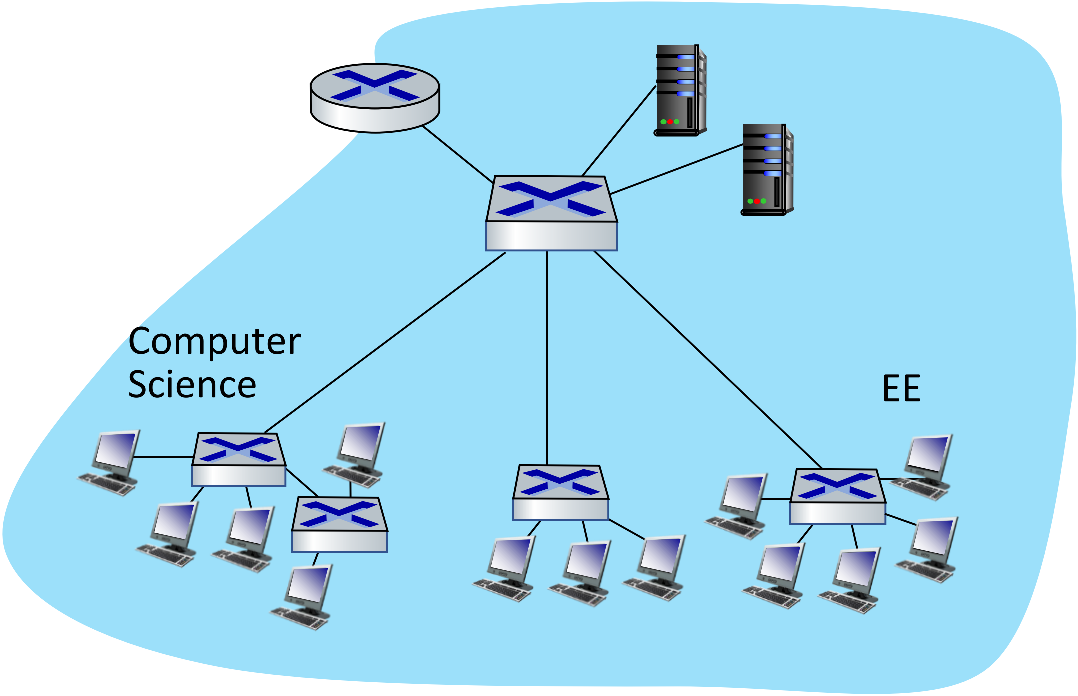
*Q:* what happens as LAN sizes scale, users change point of attachment?

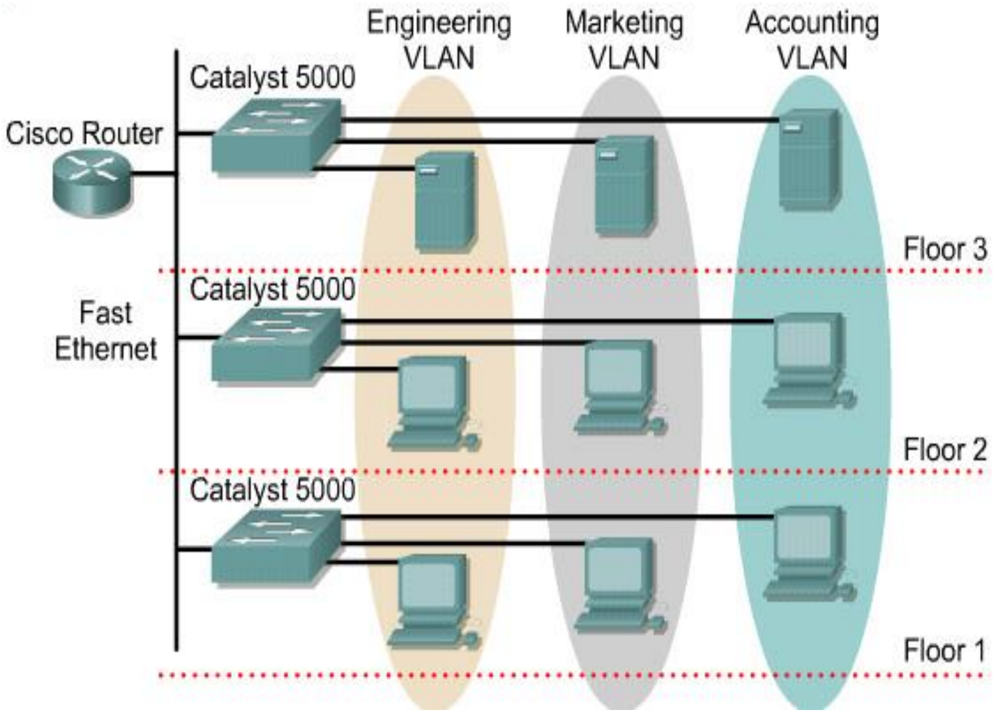
VLANs logically segment switched networks

Packets are only switched between ports that are designated for the same VLAN

The key benefit: organizing the LAN logically instead of physically

Layer 3 routing allows the router to send packets to the three different VLANs (interconnect)





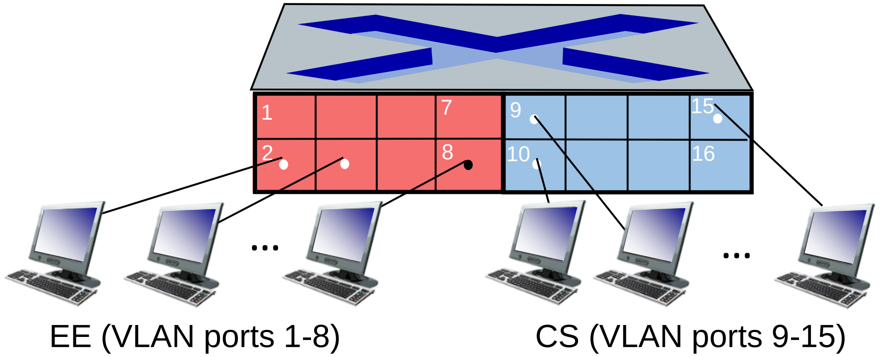
The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Port-based VLANs

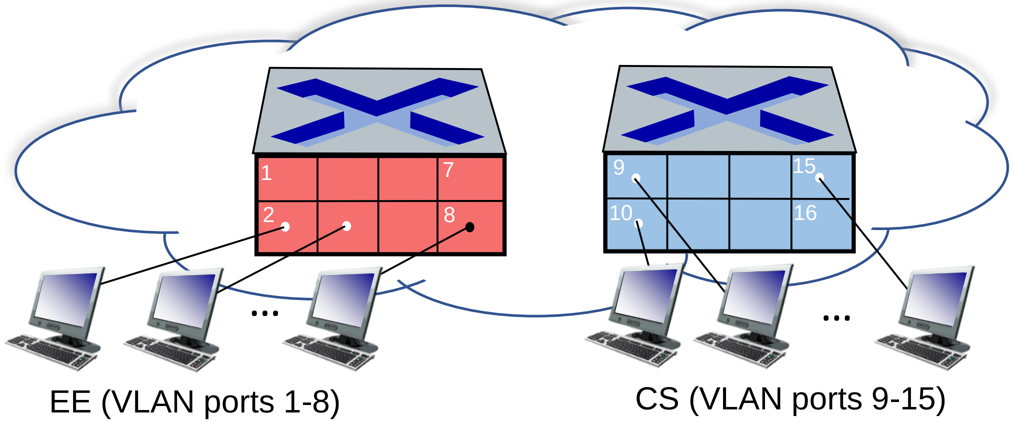
## Virtual Local Area Network (VLAN)

switch(es) supporting VLAN capabilities can be configured to define multiple *virtual* LANS over single physical LAN infrastructure.

port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



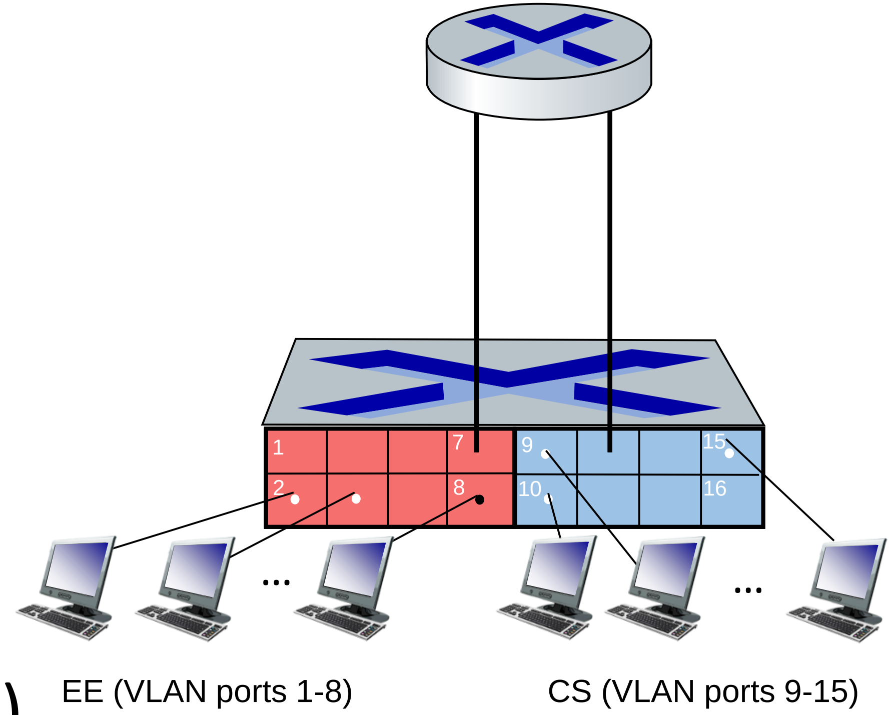
… operates as multiple virtual switches



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020

# Port-based VLANs

- traffic isolation: frames to/from ports 1-8 can *only* reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- dynamic membership: ports can be dynamically assigned among VLANs
- forwarding between VLANS: done via routing (just as with separate switches)
  - in practice vendors sell combined switches plus routers



The slides are based on the slides by Computer Networking: A Top-Down Approach 8th edition, Jim Kurose, Keith Ross, Pearson, 2020