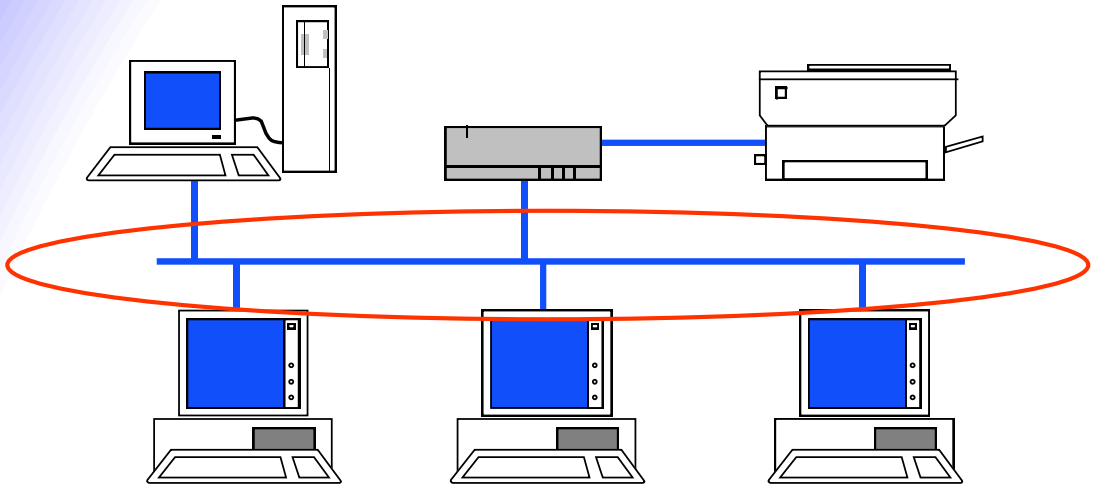
5. Local Area Network (LAN)

* Ethernet
* Address Resolution Protocol (ARP)
* Virtual Local Area Network (VLAN)
* wireless LAN

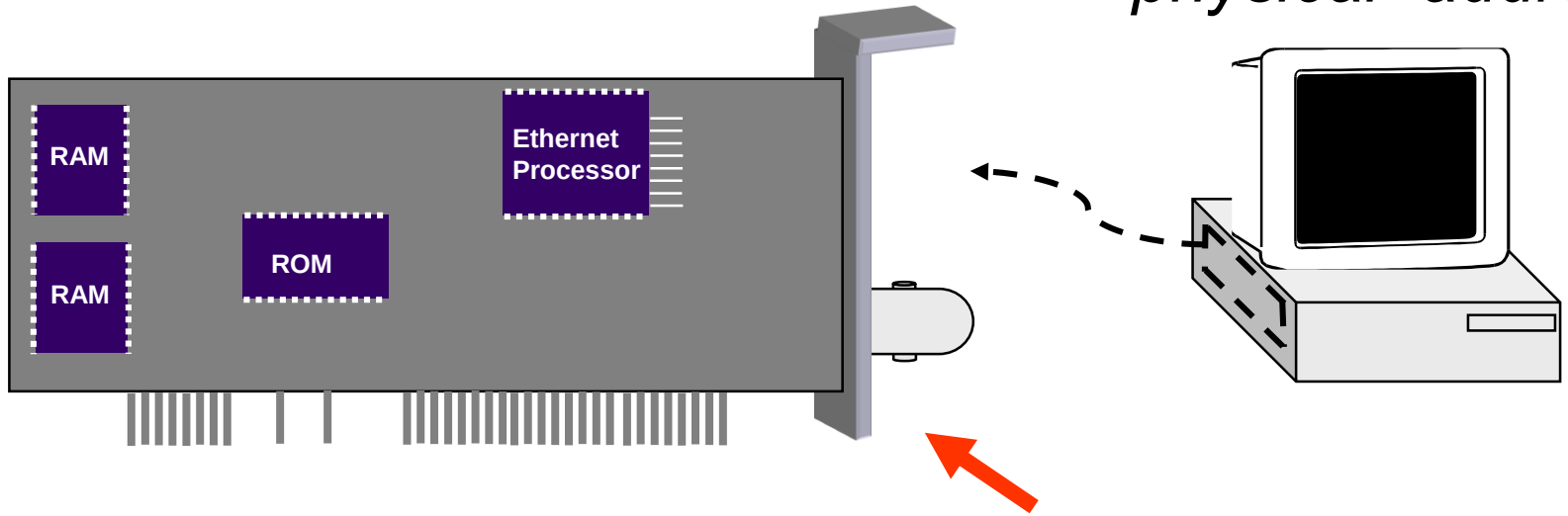
5.1 overview

Local area means:

- Private ownership
  - freedom from regulatory constraints of WANs
- Short distance (~1km) between computers
  - low cost
  - very high-speed, relatively error-free communication
  - complex error control unnecessary
- Machines are constantly moved
  - Keeping track of location of computers a chore
  - Simply give each machine a unique address
  - ***Broadcast*** *all messages to all machines in the LAN*
- Need a *medium access control (MAC) protocol*

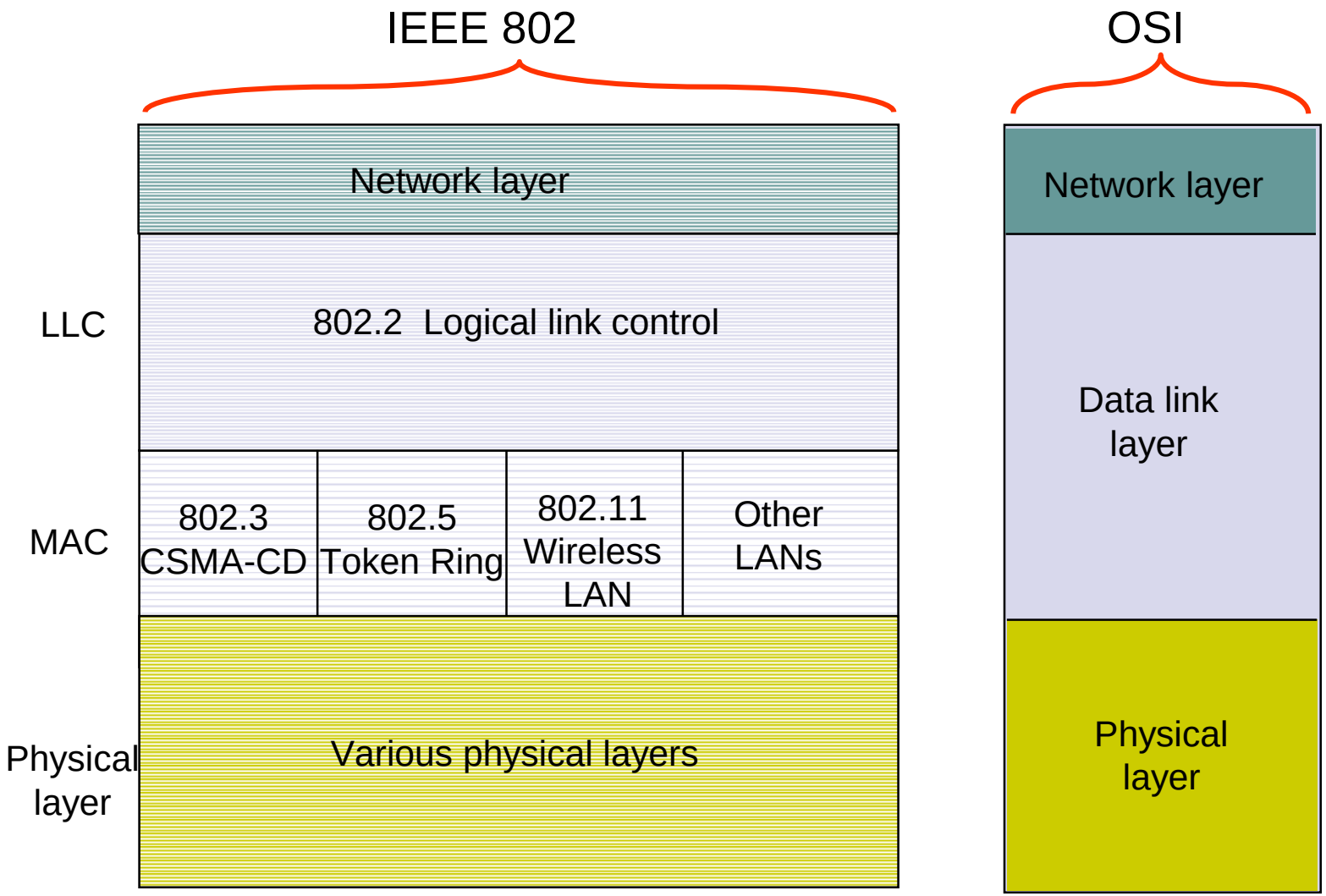


- Transmission Medium
- Network Interface Card (NIC)
- *Unique MAC "physical" address*

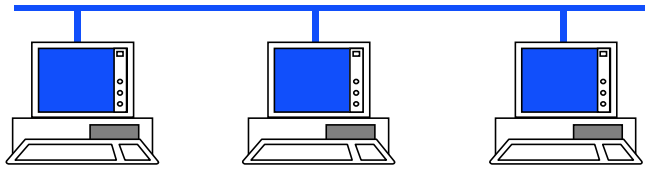


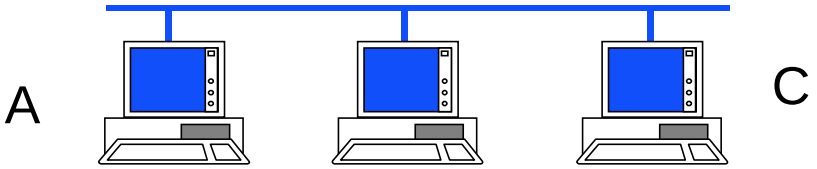
- In IEEE 802.1, Data Link Layer divided into:

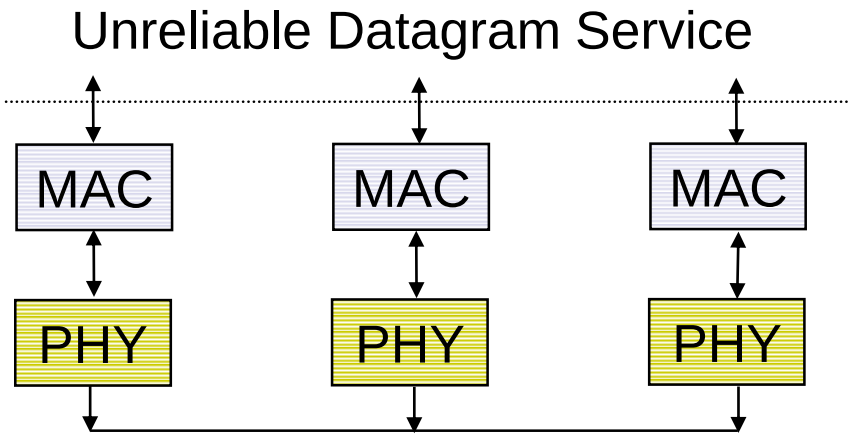
1. Medium Access Control Sublayer
   - Coordinate access to medium
   - Connectionless frame transfer service
   - Machines identified by MAC/physical address
   - Broadcast frames with MAC addresses
2. Logical Link Control Sublayer
   - Between Network layer & MAC sublayer

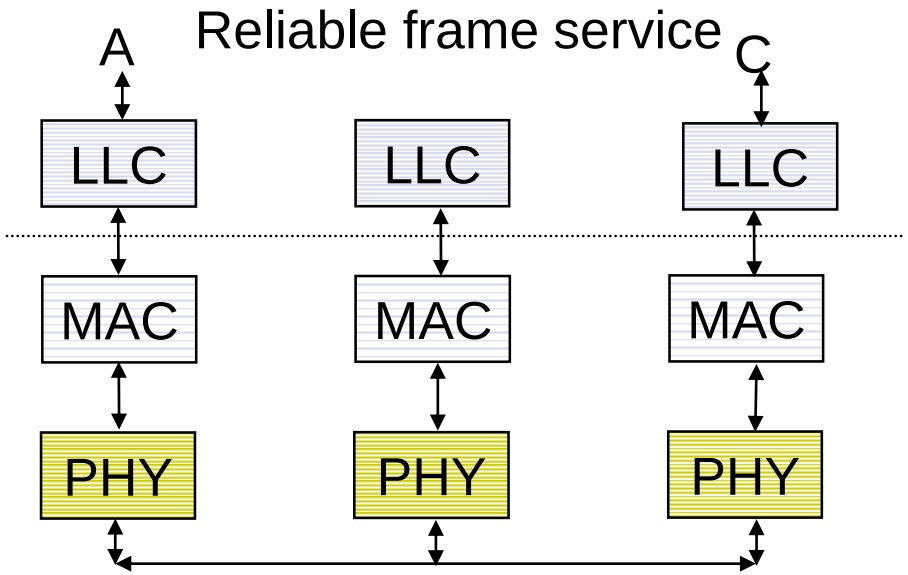

IEEE 802
OSI
Network layer
LLC
802.2 Logical link control
MAC
802.3 CSMA-CD
802.5 Token Ring
802.11 Wireless LAN
Other LANs
Physical layer
Various physical layers
Network layer
Data link layer
Physical layer

- IEEE 802.2: LLC enhances service provided by MAC







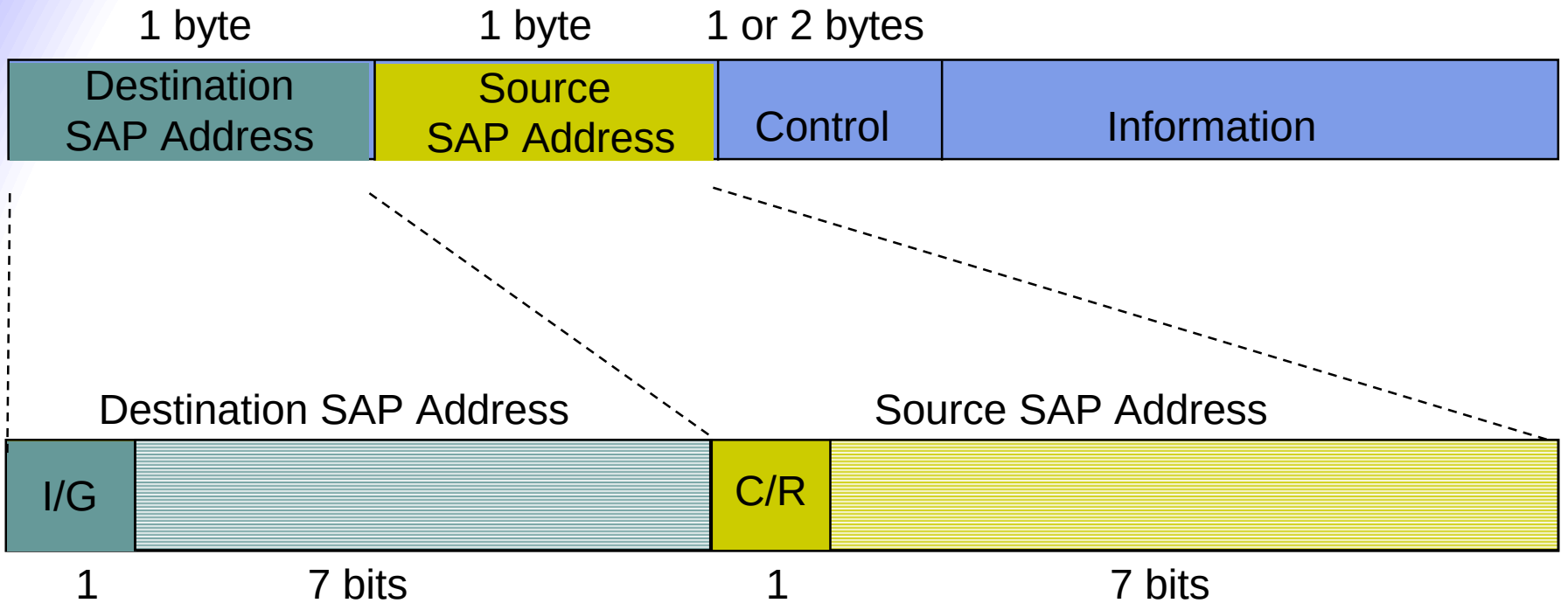


Logical Link Control Services

- Type 1: Unacknowledged connectionless service
  - Unnumbered frame mode of HDLC
- Type 2: Reliable connection-oriented service
  - Asynchronous balanced mode of HDLC
- Type 3: Acknowledged connectionless service

- Additional addressing
  - A workstation has a single MAC physical address
  - Can handle several logical connections, distinguished by their SAP (service access points).

LLC PDU Structure

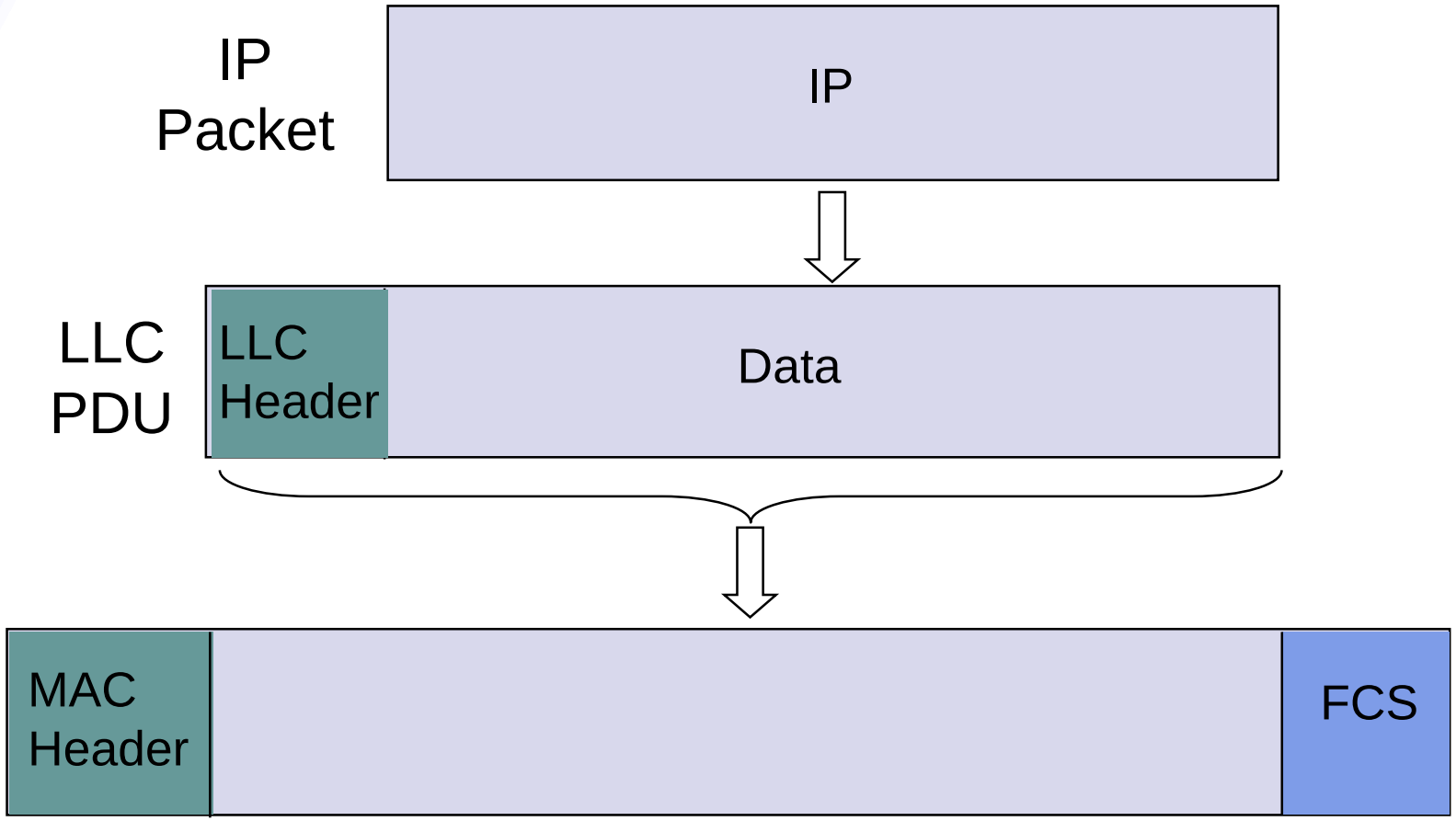


I/G = Individual or group address
C/R = Command or response frame

Examples of SAP Addresses:

06	IP packet
E0	Novell IPX
FE	OSI packet
AA	SubNetwork Access protocol (SNAP)

Encapsulation of MAC frames



5.2 Ethernet

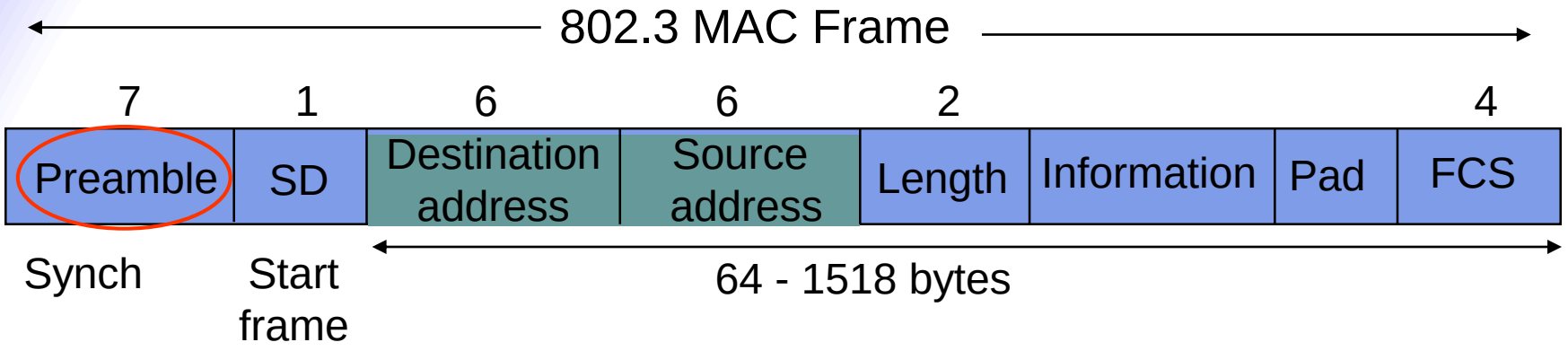
- 1970 ALOHAnet radio network deployed in Hawaiian islands
- 1973 Metcalf and Boggs invent Ethernet, random access in wired net
- 1979 DIX Ethernet II Standard
- 1985 IEEE 802.3 LAN Standard (10 Mbps)
- 1995 Fast Ethernet (100 Mbps)
- 1998 Gigabit Ethernet
- 2002 10 Gigabit Ethernet
- Ethernet is the dominant LAN standard

MAC Protocol:

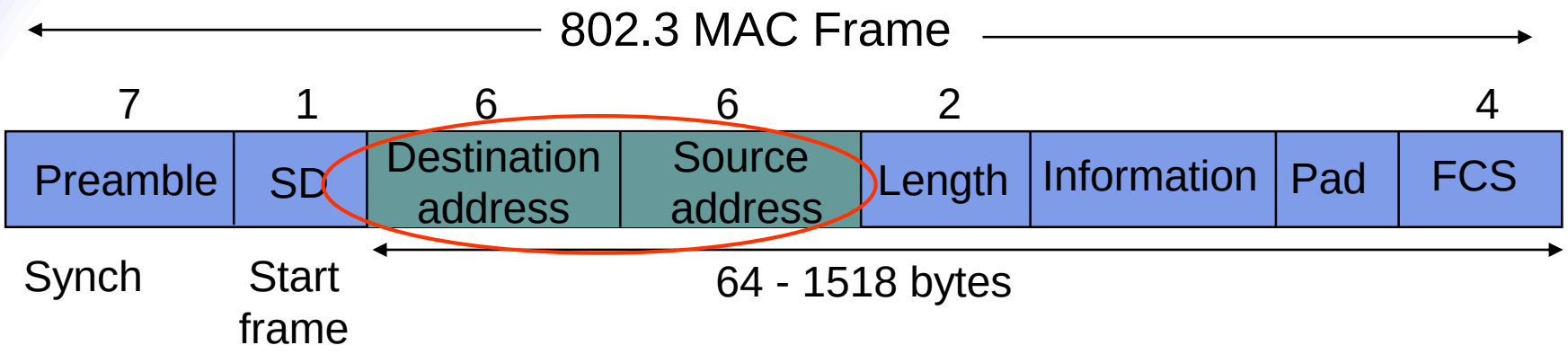
- CSMA/CD
- *Slot Time* is the critical system parameter
  - upper bound on time to detect collision
  - upper bound on time to acquire channel
  - upper bound on length of frame segment generated by collision
  - quantum for retransmission scheduling
  - max{round-trip propagation, MAC jam time}
- Truncated binary exponential backoff
  - for retransmission n: $0 < r < 2^k$, where $k=\min(n,10)$
  - Give up after 16 retransmissions

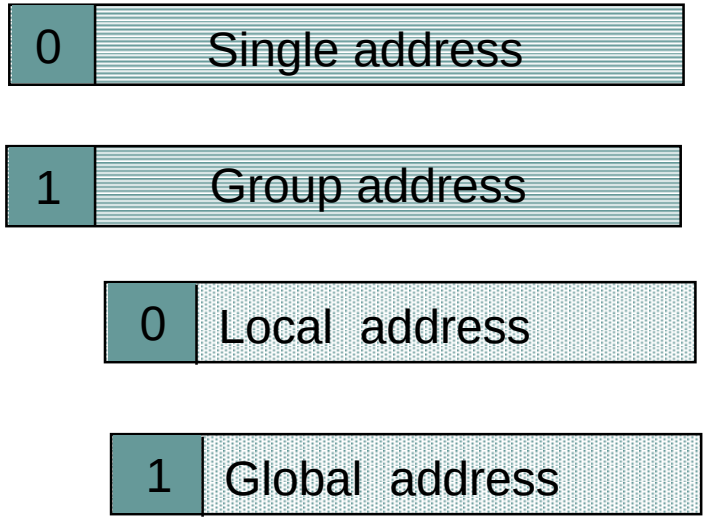
- Transmission Rate: 10 Mbps
- Min Frame: 512 bits = 64 bytes
- Slot time: 512 bits/10 Mbps = 51.2 μsec
  - 51.2 μsec x $2x10^5$ Km/sec =10.24 Km, 1 way
  - 5.12 Km round trip distance
- Max Length: 2500 meters + 4 repeaters

- *Each x10 increase in bit rate, must be accompanied by x10 decrease in distance*



- Every frame transmission begins “from scratch”
- Preamble helps receivers synchronize their clocks to transmitter clock
- 7 bytes of 10101010 generate a square wave
- Start frame byte changes to 1010101**1**
- Receivers look for change in 10 pattern

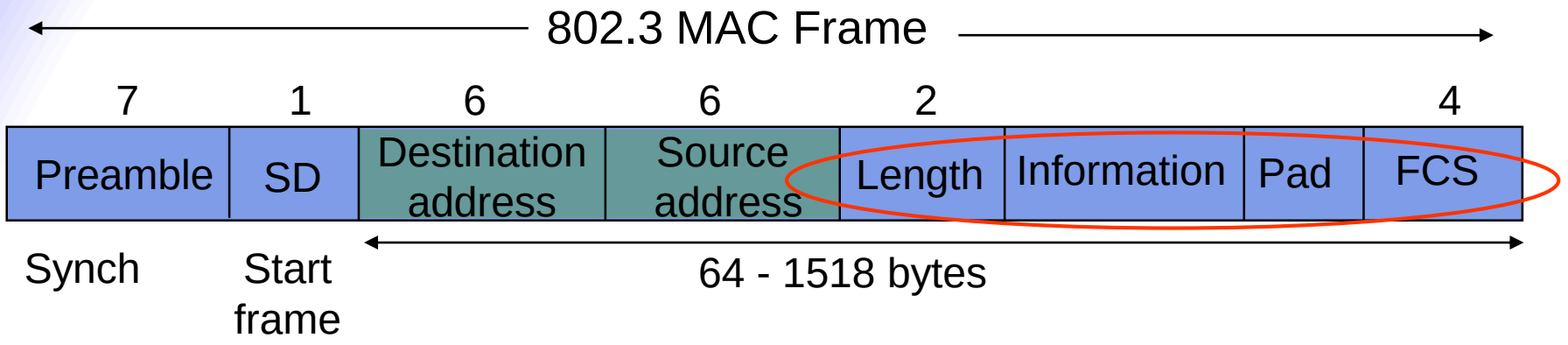




- Destination address
- single address
- group address
- broadcast = 111...111

Addresses

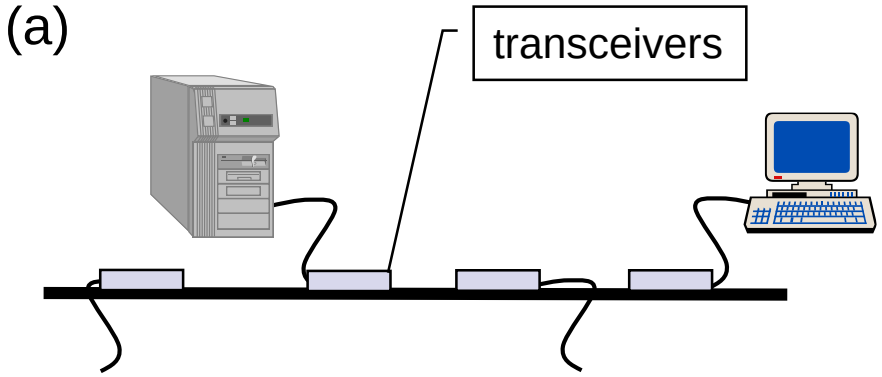
- local or global
- Global addresses
- first 24 bits assigned to manufacturer;
- next 24 bits assigned by manufacturer
- Cisco 00-00-0C
- 3COM 02-60-8C

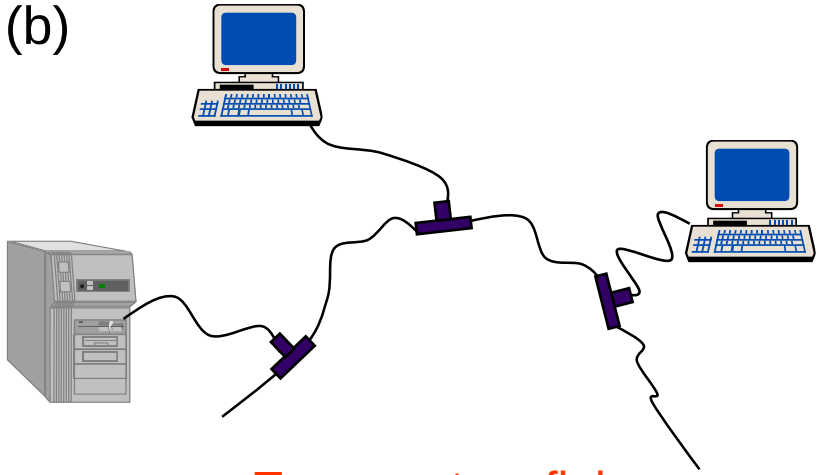


- Length: # bytes in information field
  - Max frame 1518 bytes, excluding preamble & SD
  - Max information 1500 bytes: 05DC
- Pad: ensures min frame of 64 bytes
- FCS: CCITT-32 CRC, covers addresses, length, information, pad fields
  - NIC discards frames with improper lengths or failed CRC

IEEE 802.3 Physical Layer

	10base5	10base2	10baseT	10baseFX
Medium	Thick coax	Thin coax	Twisted pair	Optical fiber
Max. Segment Length	500 m	200 m	100 m	2 Km
Topology	Bus	Bus	Star	Point-to-point link

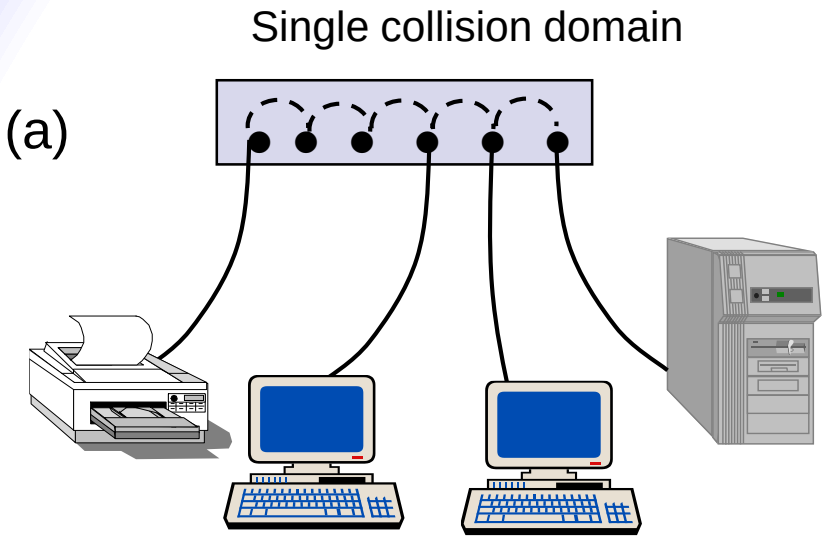




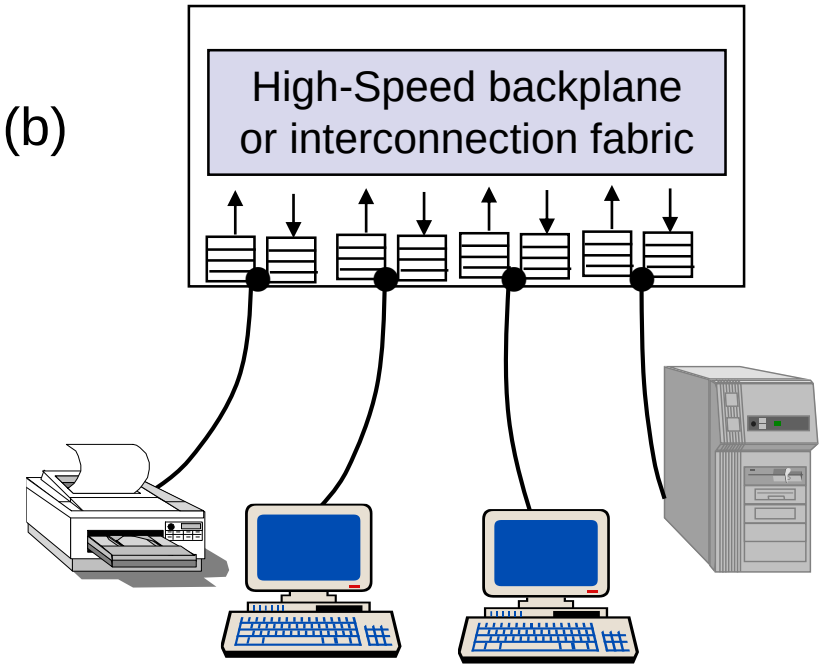
Hubs & Switches!

Thick Coax: Stiff, hard to work with

T connectors flaky



Twisted Pair Cheap
Easy to work with
Reliable
Star-topology CSMA-CD



Twisted Pair Cheap
Bridging increases scalability
Separate collision domains
Full duplex operation

	100baseT4	100baseT	100baseFX
Medium	Twisted pair category 3 UTP 4 pairs	Twisted pair category 5 UTP two pairs	Optical fiber multimode Two strands
Max. Segment Length	100 m	100 m	2 Km
Topology	Star	Star	Star

To preserve compatibility with 10 Mbps Ethernet:

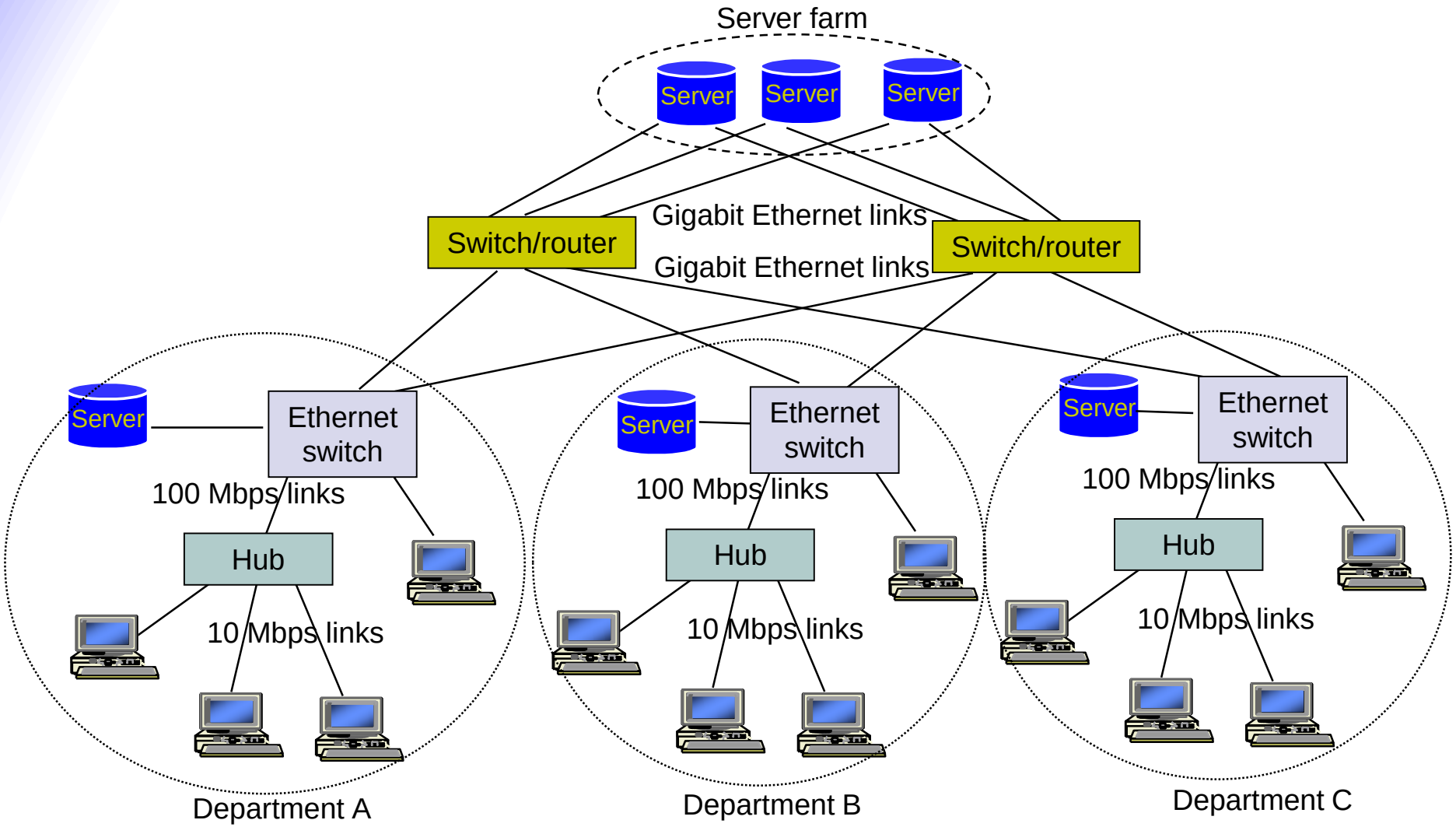
- Same frame format, same interfaces, same protocols
- Hub topology only with twisted pair & fiber
- Bus topology & coaxial cable abandoned
- Category 3 twisted pair (ordinary telephone grade) requires 4 pairs
- Category 5 twisted pair requires 2 pairs (most popular)

	1000baseSX	1000baseLX	1000baseCX	1000baseT
Medium	Optical fiber multimode Two strands	Optical fiber single mode Two strands	Shielded copper cable	Twisted pair category 5 UTP
Max. Segment Length	550 m	5 Km	25 m	100 m
Topology	Star	Star	Star	Star

- Slot time increased to 512 bytes
- Small frames need to be extended to 512 bytes
- Frame bursting to allow stations to transmit burst of short frames
- Frame structure preserved but CSMA-CD essentially abandoned
- Extensive deployment in backbone of enterprise data networks and in server farms
- Most prevalent LAN today

	10GbaseSR	10GBaseLR	10GbaseEW	10GbaseLX4
Medium	Two optical fibers Multimode at 850 nm 64B66B code	Two optical fibers Single-mode at 1310 nm 64B66B	Two optical fibers Single-mode at 1550 nm SONET compatibility	Two optical fibers multimode/single-mode with four wavelengths at 1310 nm band 8B10B code
Max. Segment Length	300 m	10 Km	40 Km	300 m – 10 Km

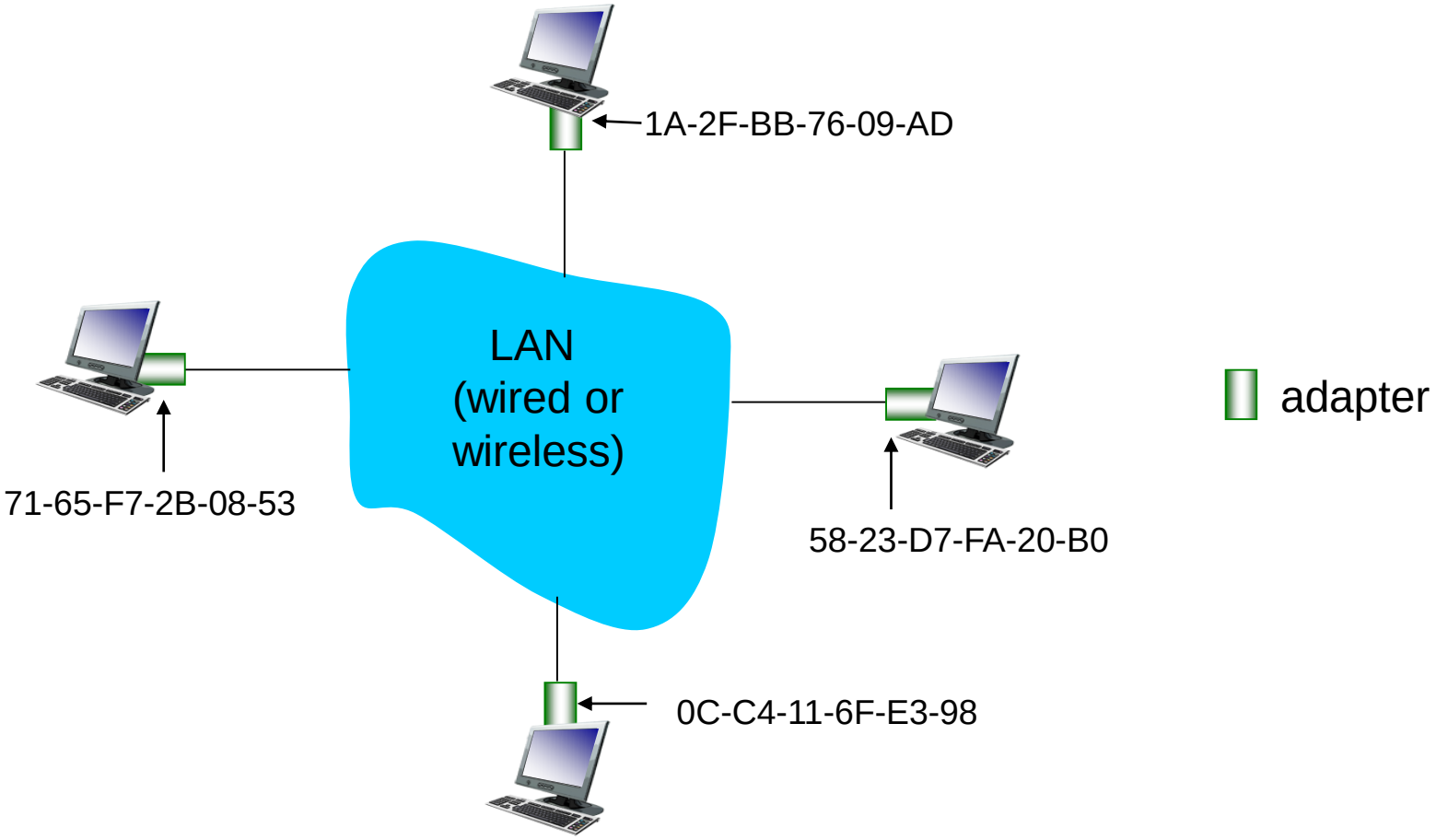
- Frame structure preserved
- CSMA-CD protocol officially abandoned
- LAN PHY for local network applications
- WAN PHY for wide area interconnection using SONET OC-192c
- Extensive deployment in metro networks anticipated


Server farm
Server
Server
Server
Gigabit Ethernet links
Switch/router
Gigabit Ethernet links
Switch/router
Server
Ethernet switch
100 Mbps links
Hub
10 Mbps links
Department A
Server
Ethernet switch
100 Mbps links
Hub
10 Mbps links
Department B
Server
Ethernet switch
100 Mbps links
Hub
10 Mbps links
Department C

5.3 ARP

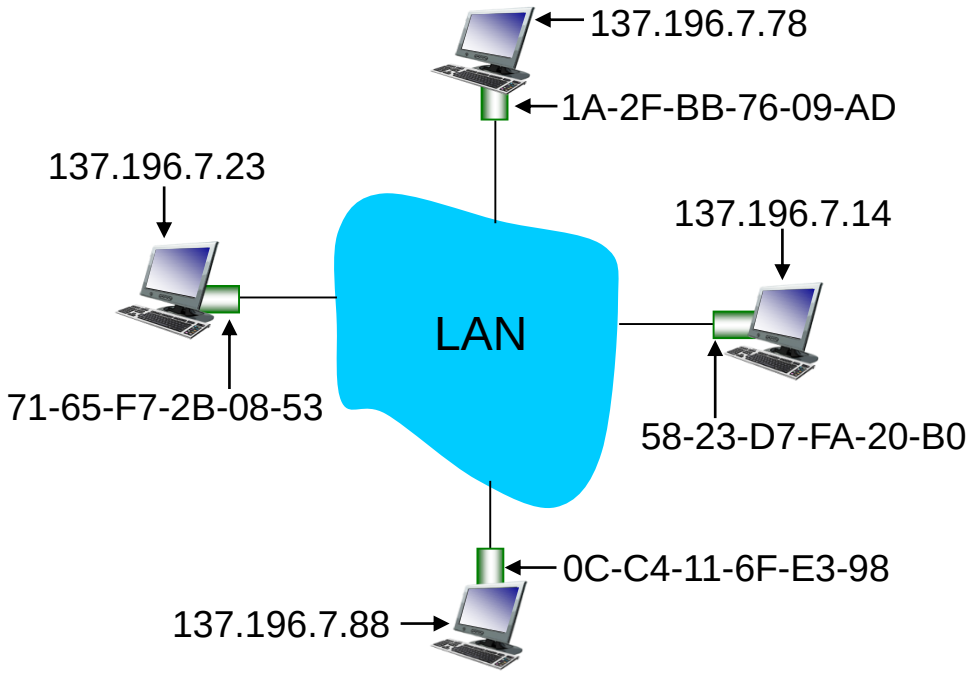
- 32-bit IP address:
  - *network-layer* address for interface
  - used for layer 3 (network layer) forwarding
- MAC (or LAN or physical or Ethernet) address:
  - function: *used ‘locally” to get frame from one interface to another physically-connected interface (same network, in IP-addressing sense)*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

each adapter on LAN has unique *LAN* address



- 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

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)

- 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
- ARP is "plug-and-play":
  - nodes create their ARP tables *without intervention from net administrator*

H1 wants to learn physical address of H3 -> broadcasts an ARP request

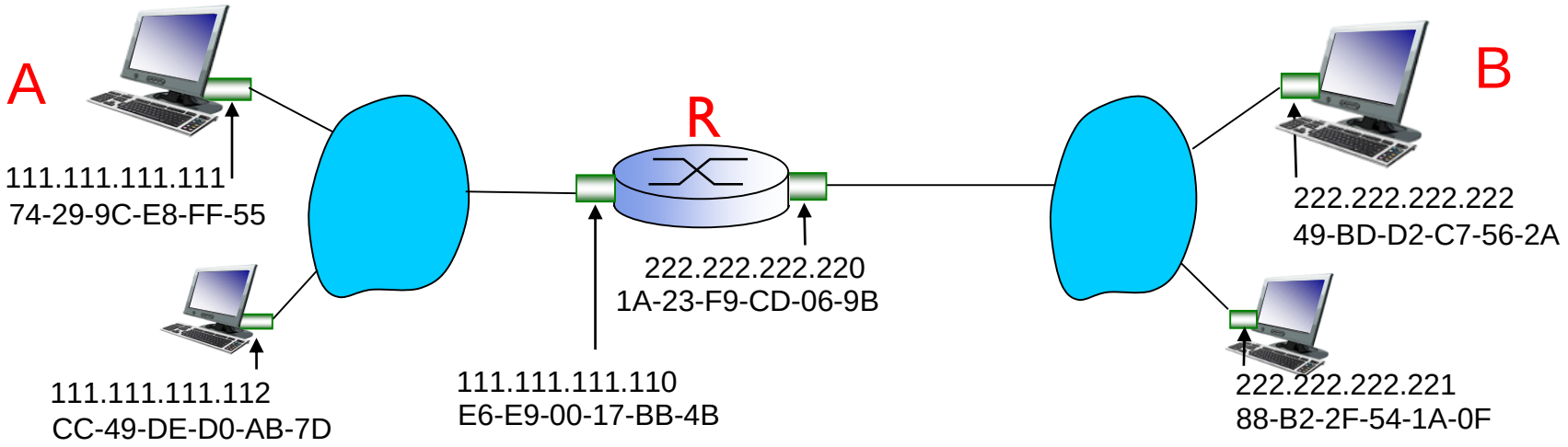
ARP request (what is the MAC address of 150.100.76.22?)

Every host receives the request, but only H3 reply with its physical address

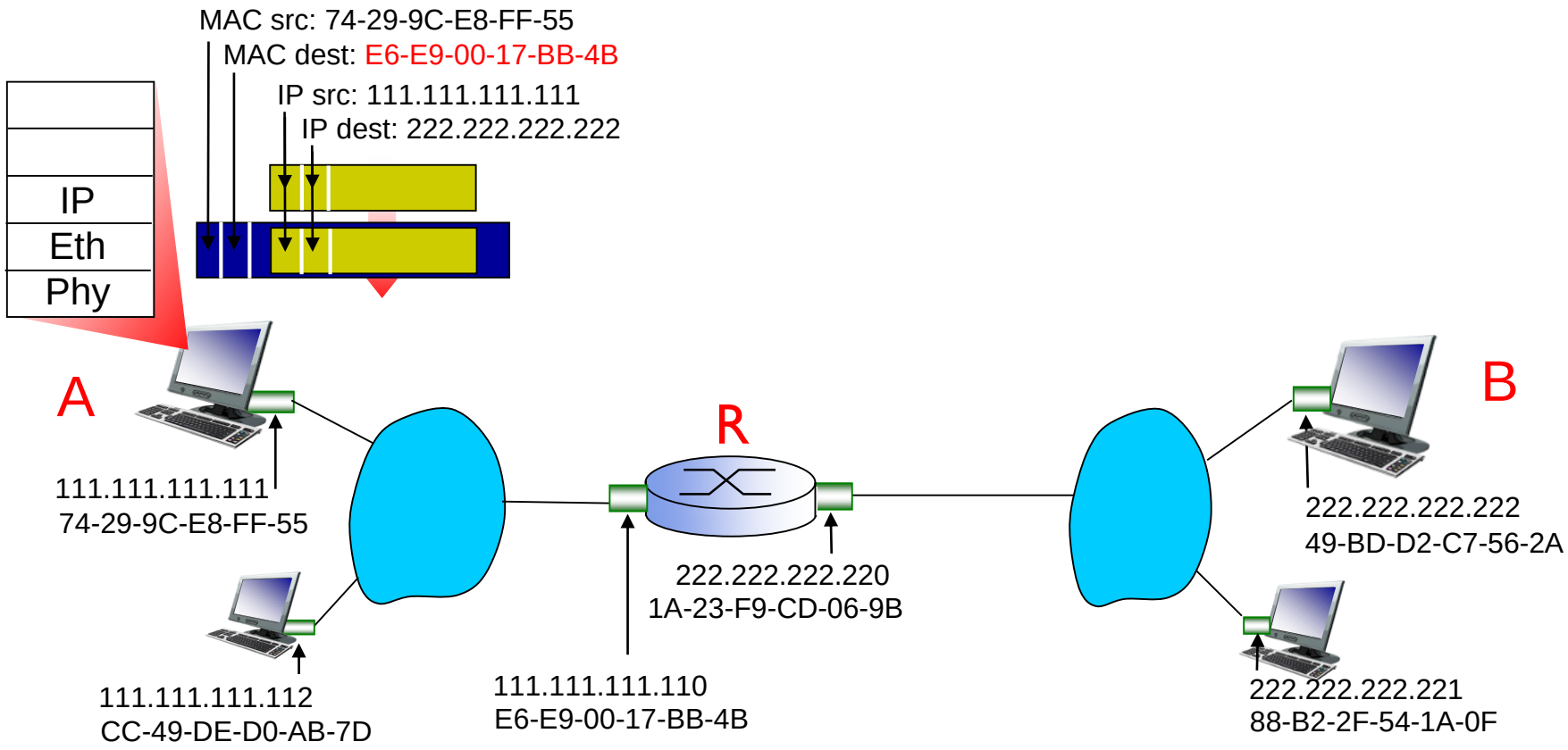
ARP response (my MAC address is 08:00:5a:3b:94)

walkthrough: send datagram from A to B via R

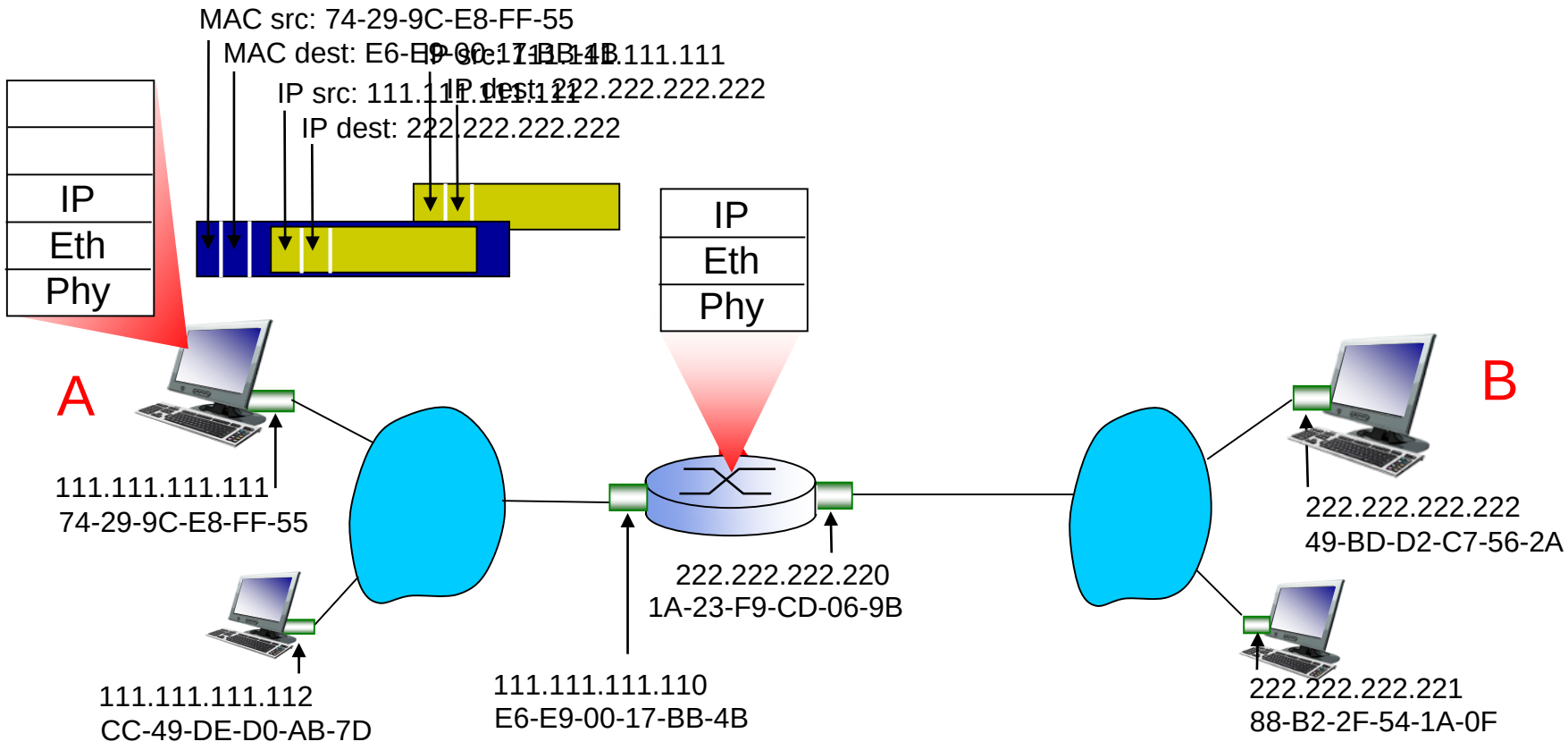
- focus on addressing – at IP (datagram) and MAC layer (frame)
- assume A knows B's IP address
- assume A knows IP address of first hop router, R (how?)
- assume A knows R's MAC address (how?)



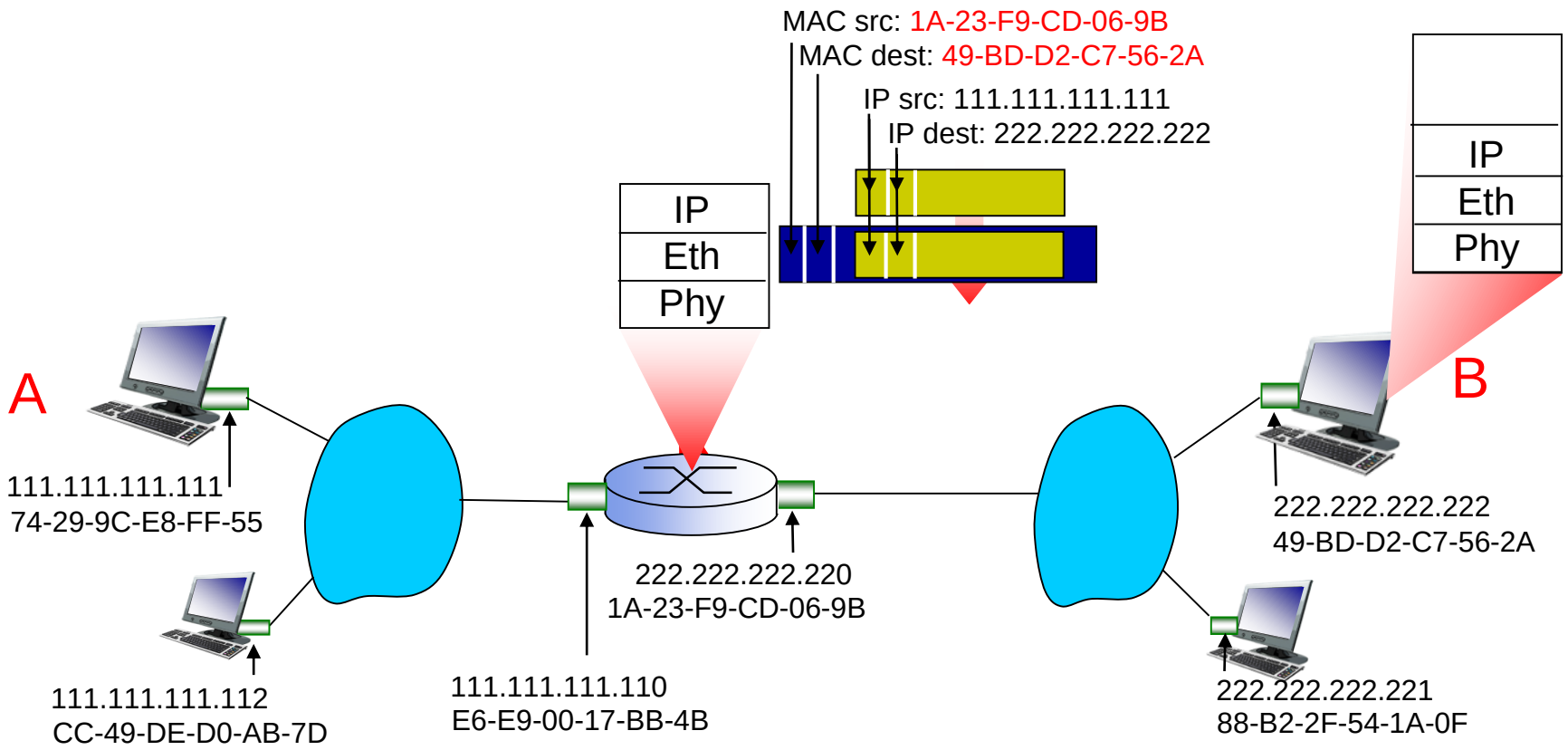
- A creates IP datagram with IP source A, destination B
- A creates link-layer frame with R's MAC address as dest, frame contains A-to-B IP datagram



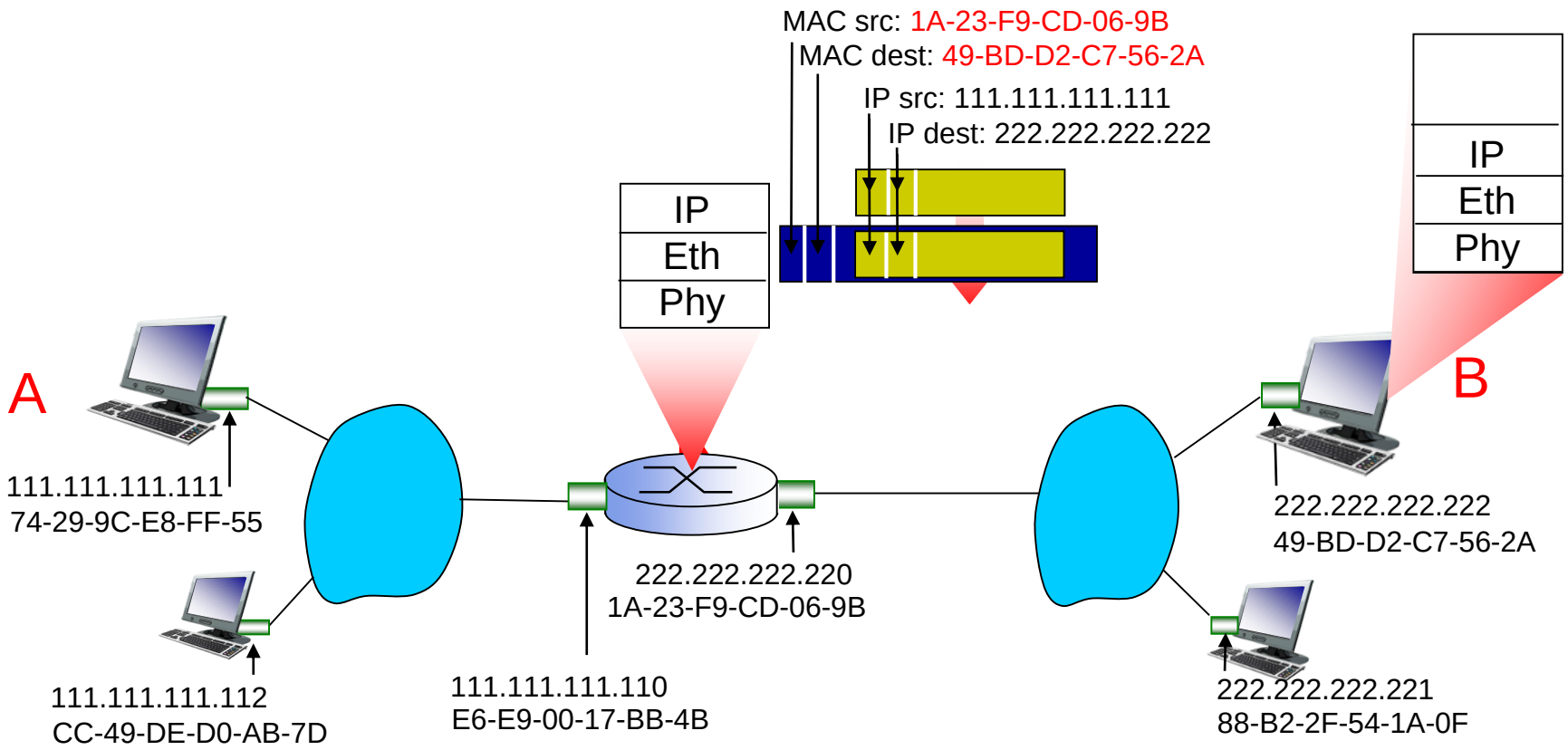
- frame sent from A to R
- frame received at R, datagram removed, passed up to IP



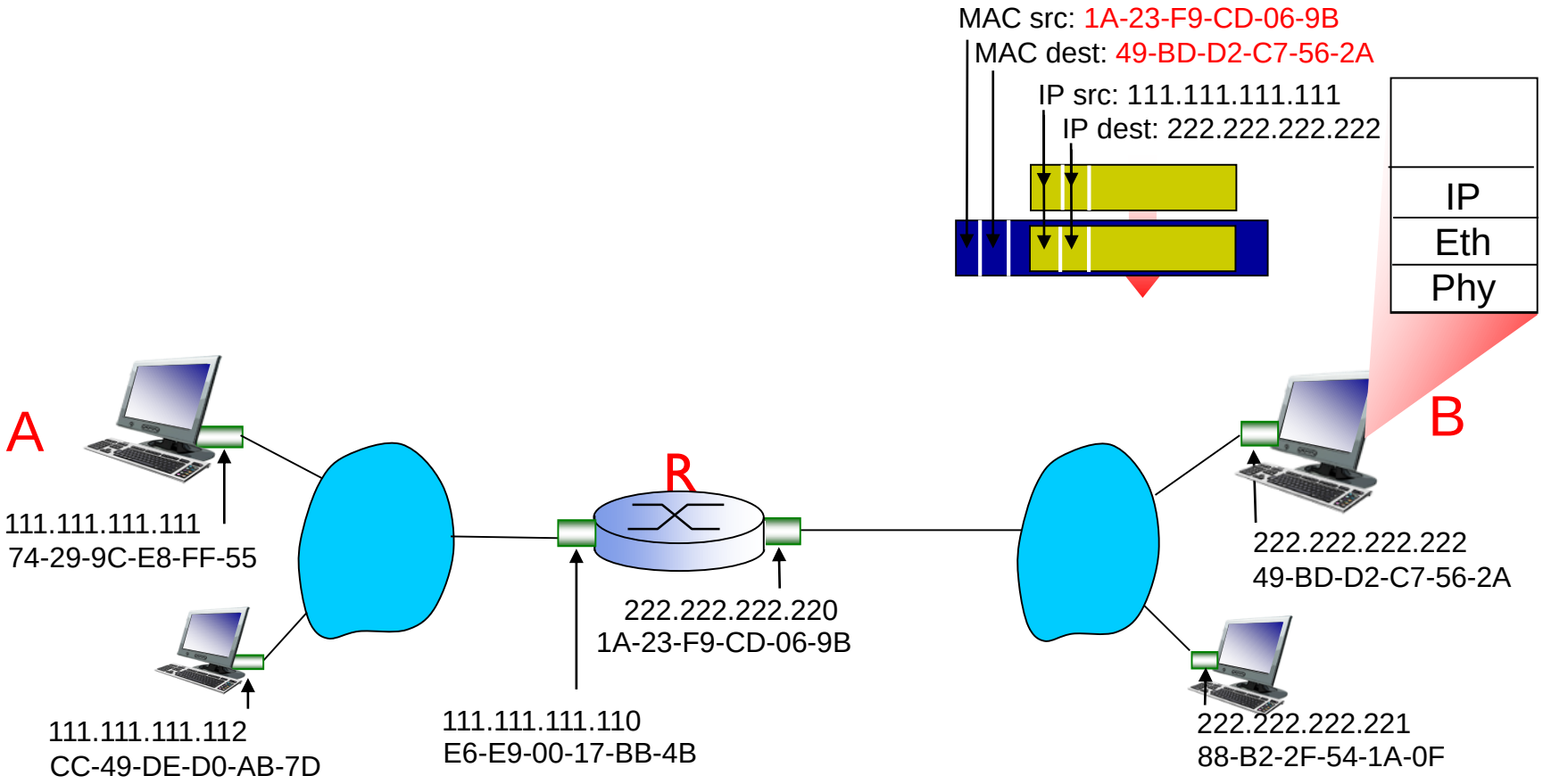
- R forwards datagram with IP source A, destination B
- R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram



- 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



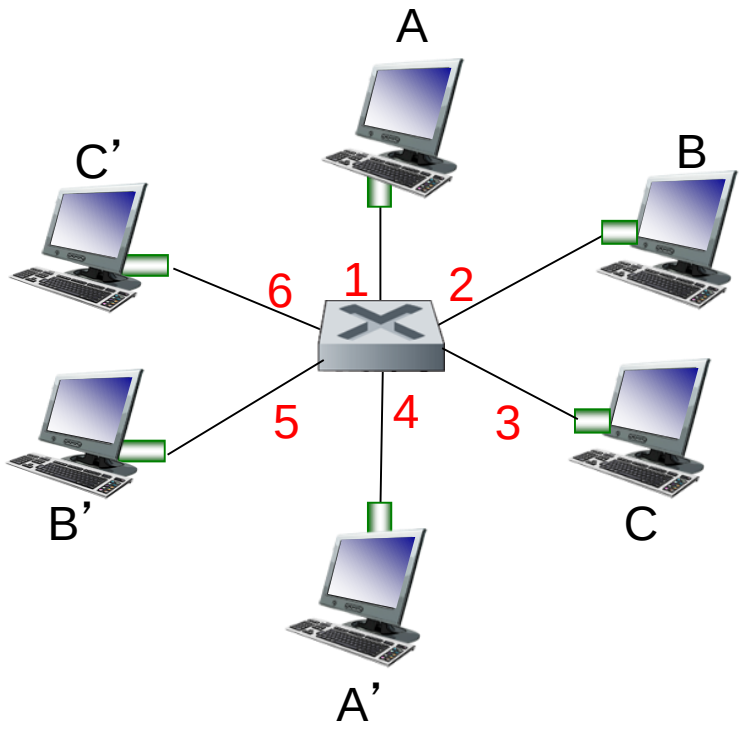
- R forwards datagram with IP source A, destination B
- R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram



5.4 switch and VLAN

- 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 when frame is to be forwarded on segment, uses CSMA/CD to access segment
- *transparent*
  - hosts are unaware of presence of switches
- *plug-and-play, self-learning*
  - switches do not need to be configured

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, but no collisions; full duplex
  - each link is its own collision domain
- *switching:* A-to-A’ and B-to-B’ can transmit simultaneously, without collisions



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

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

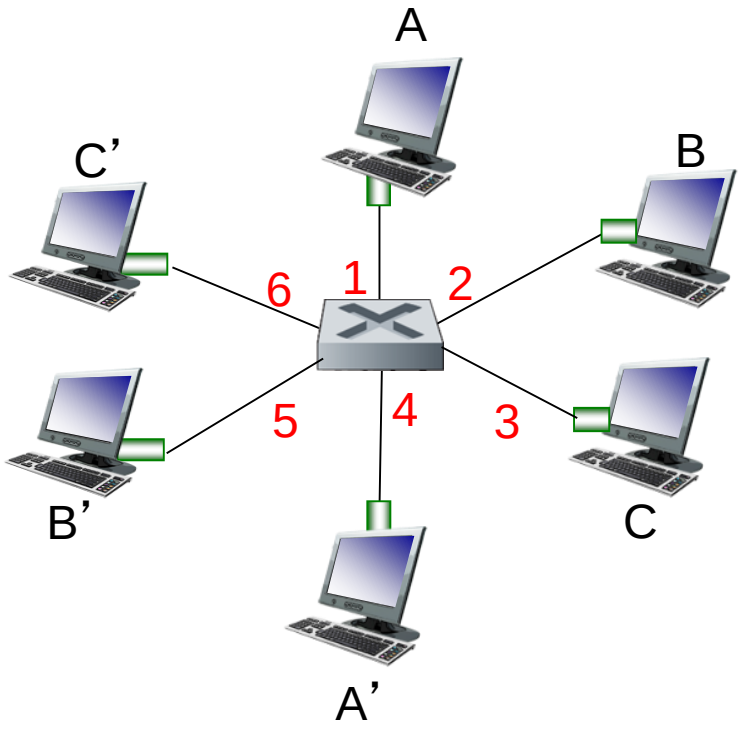
- A: each switch has a switch table,

  each entry:

  - (MAC address of host, interface to reach host, time stamp)
  - looks like a routing table!

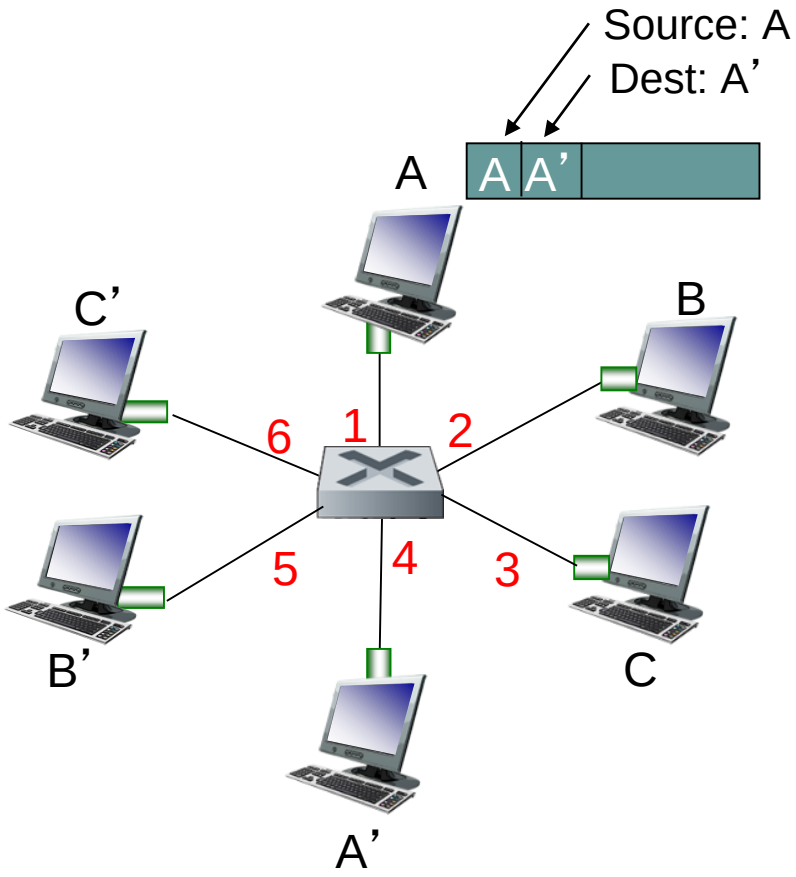
Q: how are entries created, maintained in switch table?

- something like a routing protocol?



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

- 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*

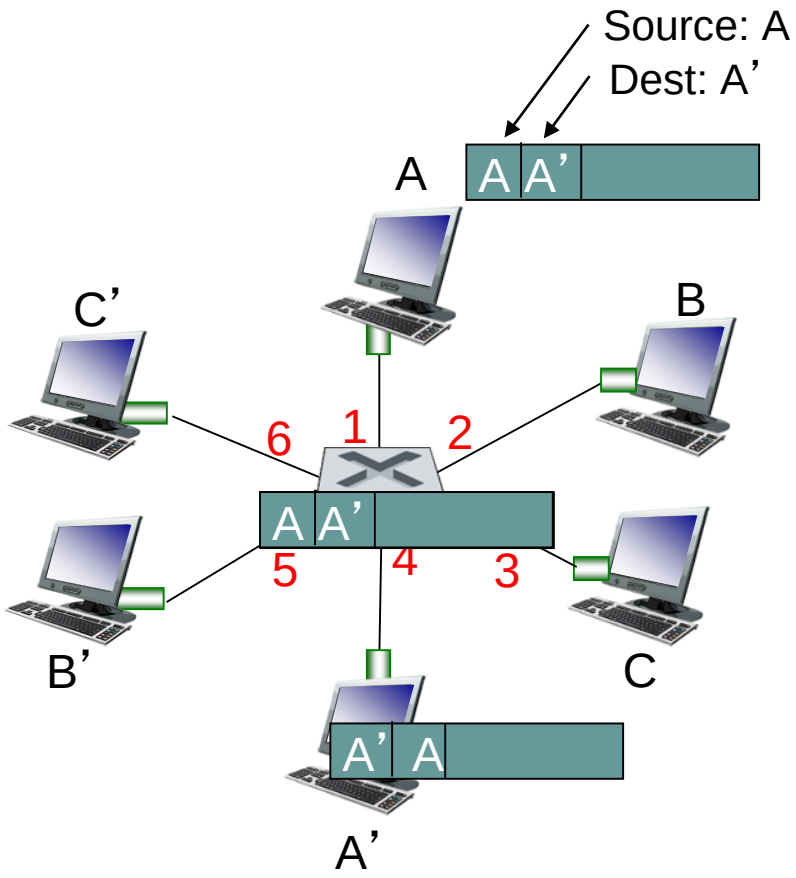
Switch table (initially empty)

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 */
```

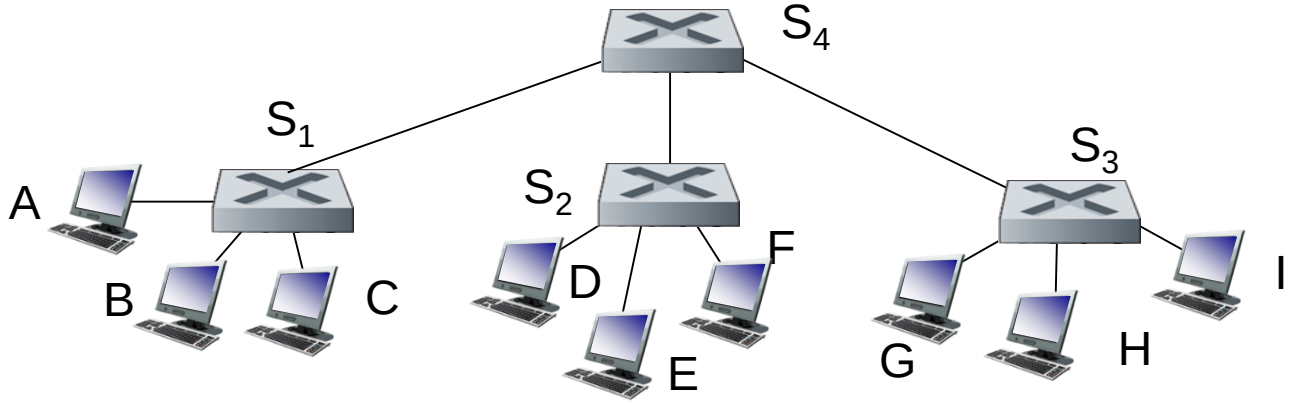
- frame destination, A', locaton unknown: *flood*
  - destination A location known: selectively send on just one link



MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

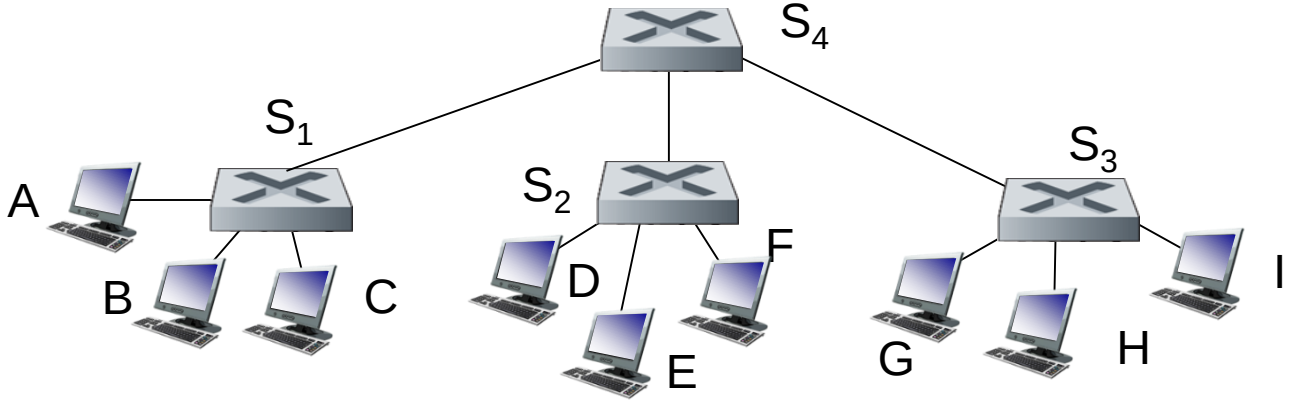
- switches can be connected together



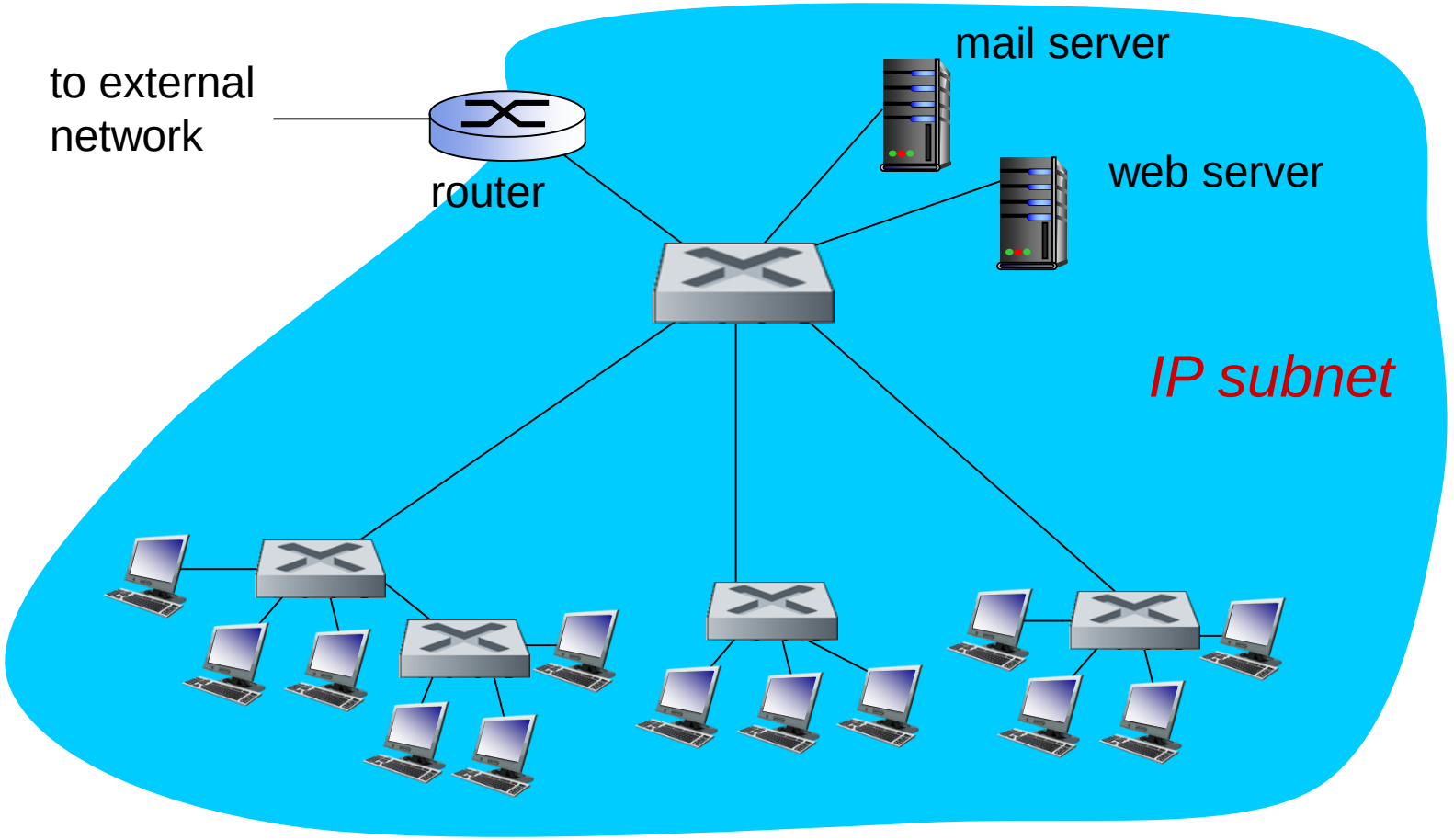
Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

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

Suppose C sends frame to I, I responds to C



- Q: show switch tables and packet forwarding in S_1, S_2, S_3, S_4


to external
network
router
mail server
web server
IP subnet

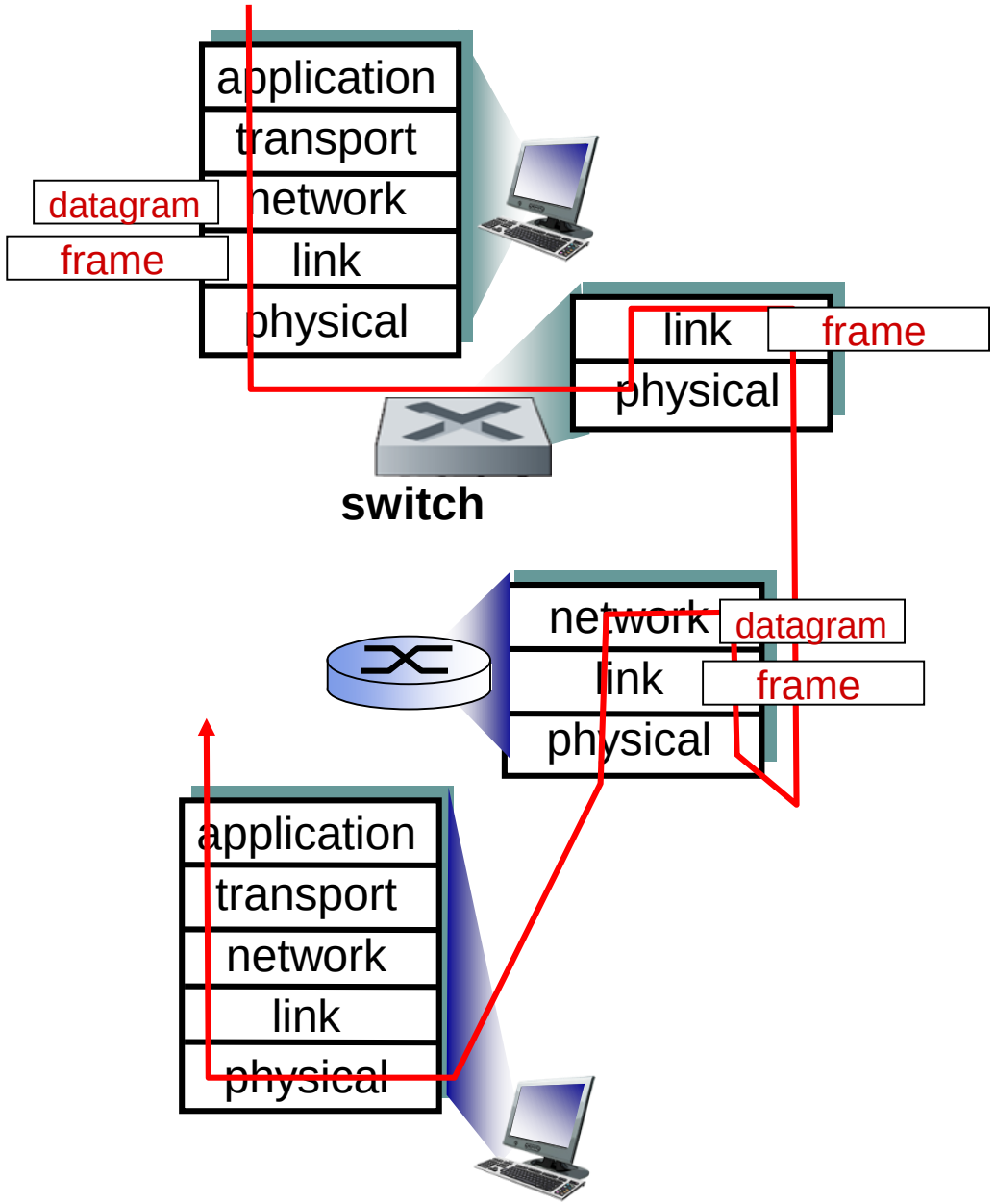
Switches vs. routers

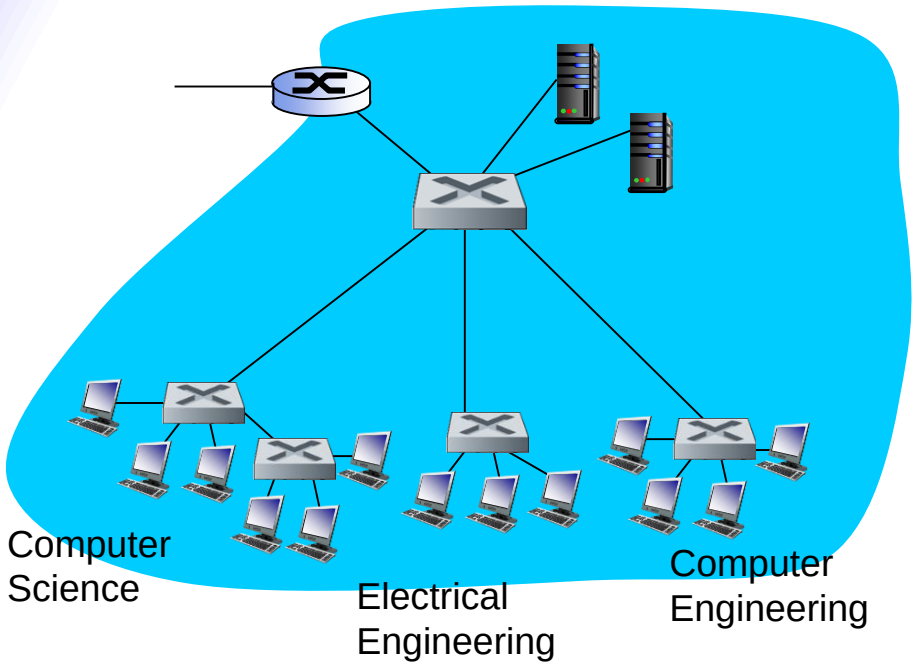
both are store-and-forward:

- *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

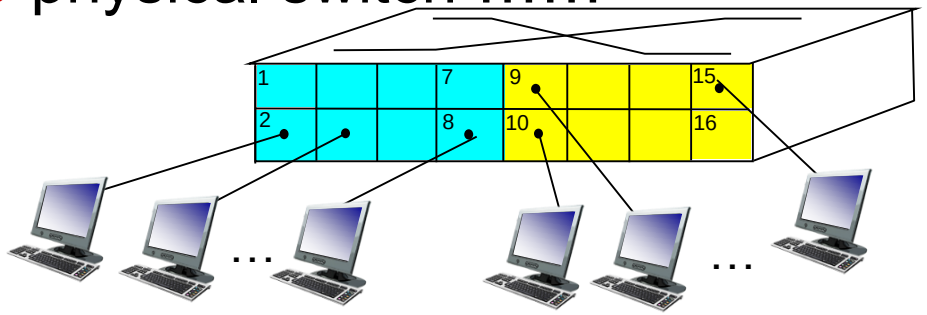




consider:

- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
  - security/privacy, efficiency issues

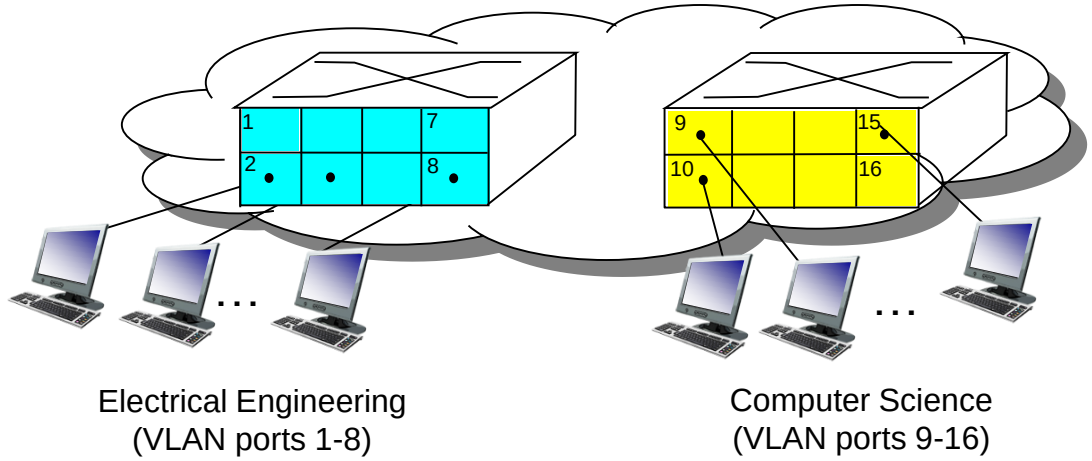
port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



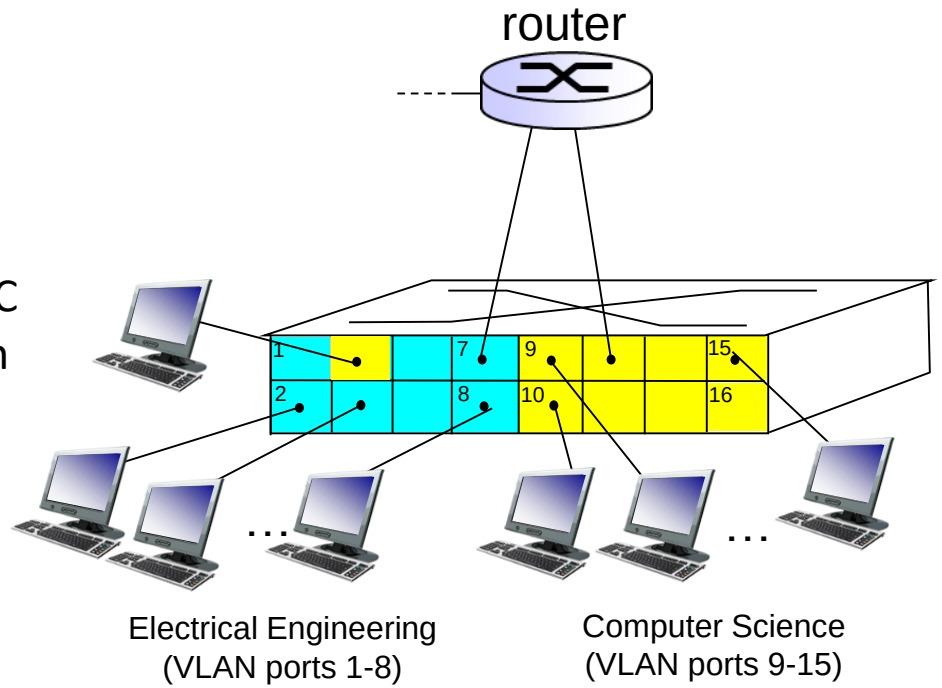
Virtual Local Area Network

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

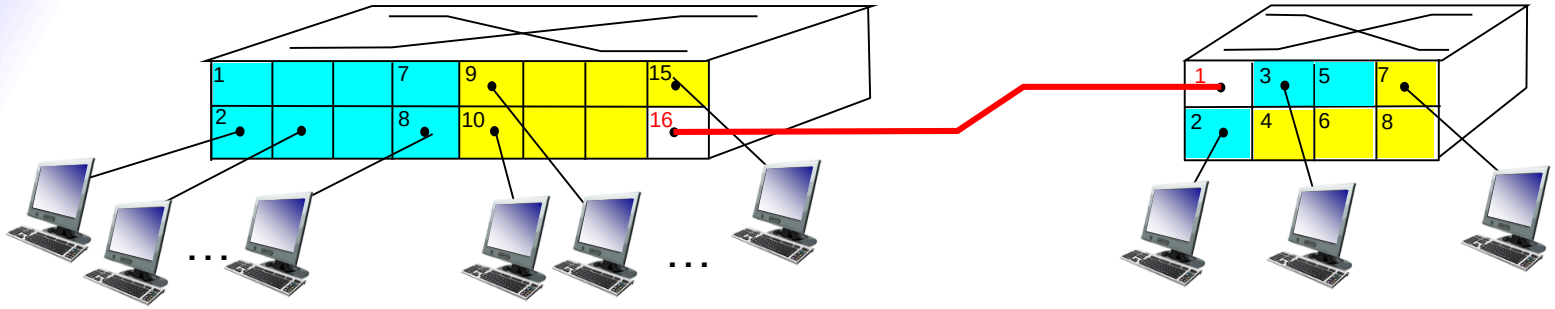
… operates as *multiple* virtual switches



- *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

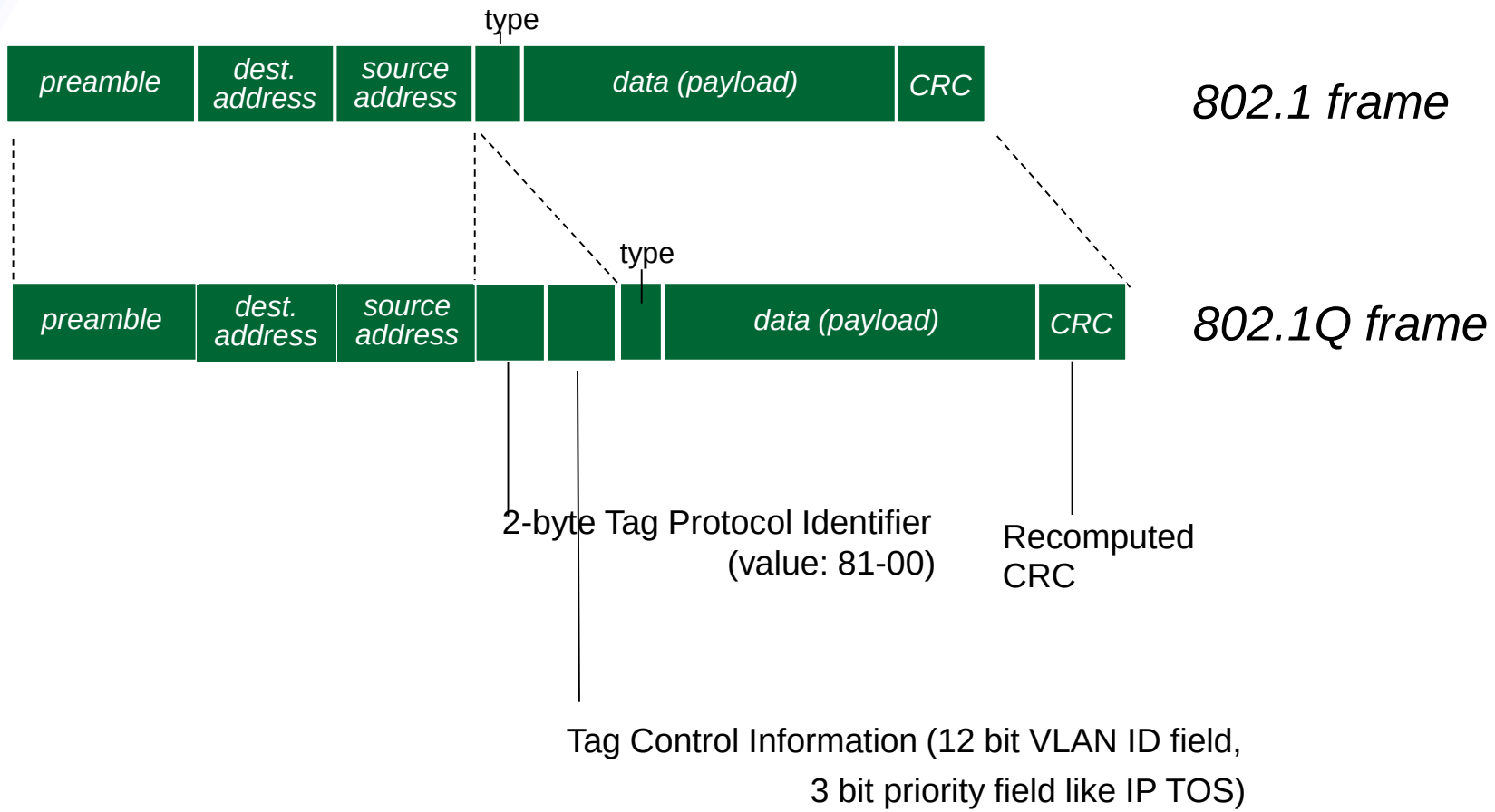


Electrical Engineering
(VLAN ports 1-8)

Computer Science
(VLAN ports 9-15)

Ports 2,3,5 belong to EE VLAN
Ports 4,6,7,8 belong to CS VLAN

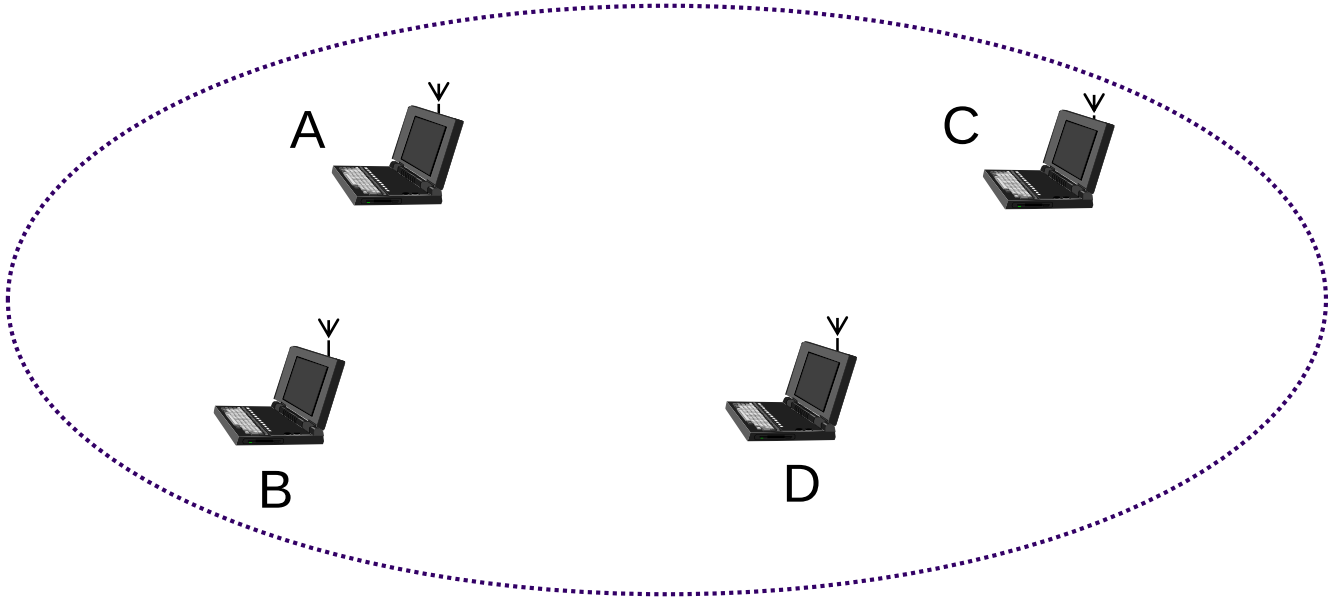
- *trunk port:* carries frames between VLANS defined over multiple physical switches
  - frames forwarded within VLAN between switches can't be conventional 802.1 frames (must carry VLAN ID info)
  - 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports


type
preamble
dest. address
source address
data (payload)
CRC
802.1 frame
type
preamble
dest. address
source address
data (payload)
CRC
802.1Q frame
2-byte Tag Protocol Identifier (value: 81-00)
Recomputed CRC
Tag Control Information (12 bit VLAN ID field, 3 bit priority field like IP TOS)

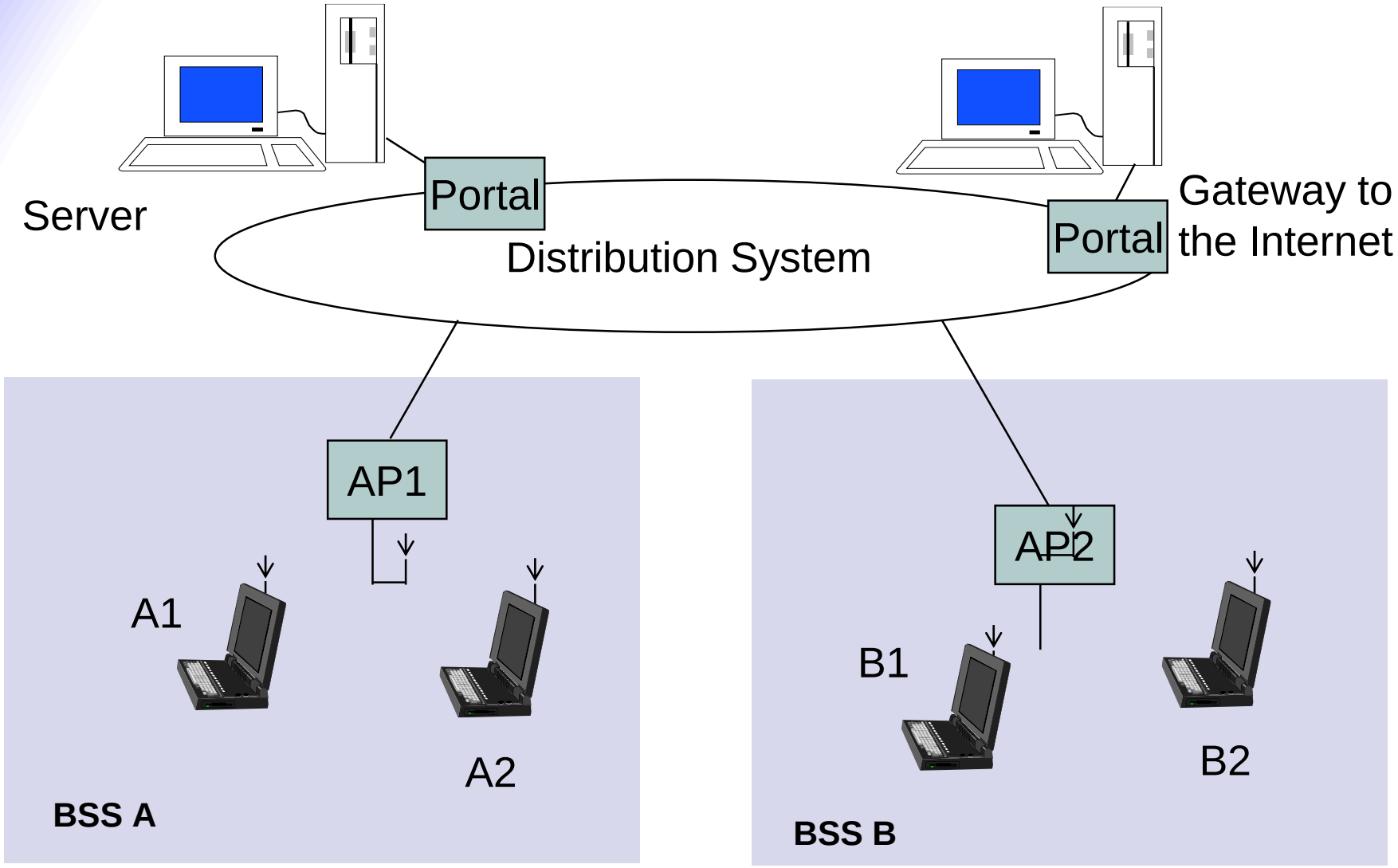
5.5 wireless LAN

- Wireless communications compelling
  - ✓ Easy, low-cost deployment
  - ✓ Mobility & roaming: Access information anywhere
  - ✓ Supports personal devices
    - ✓ PDAs, laptops, data-cell-phones
  - ✓ Supports communicating devices
    - ✓ Cameras, location devices, wireless identification
  - × Signal strength varies in space & time
  - × Signal can be captured by snoopers
  - × Spectrum is limited & usually regulated

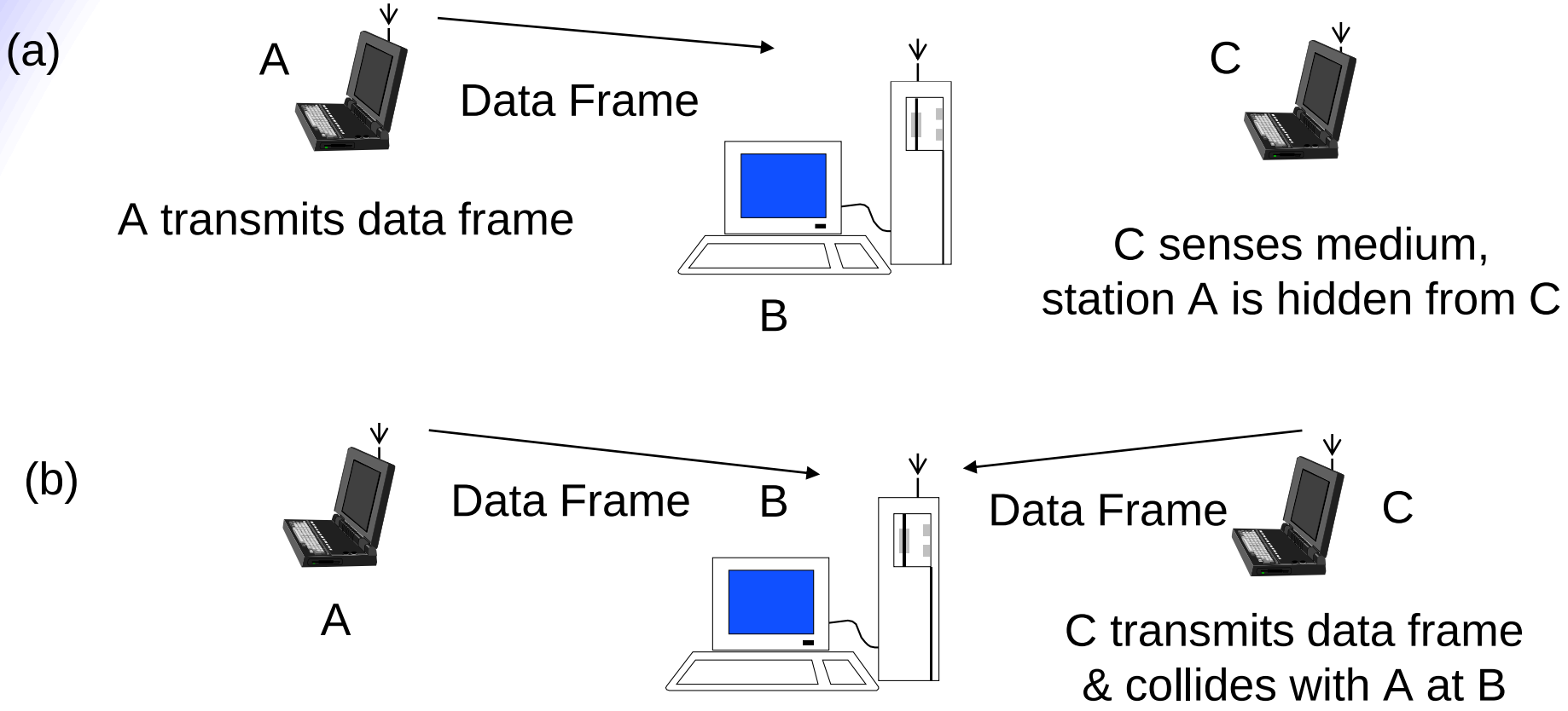
Ad Hoc Communications



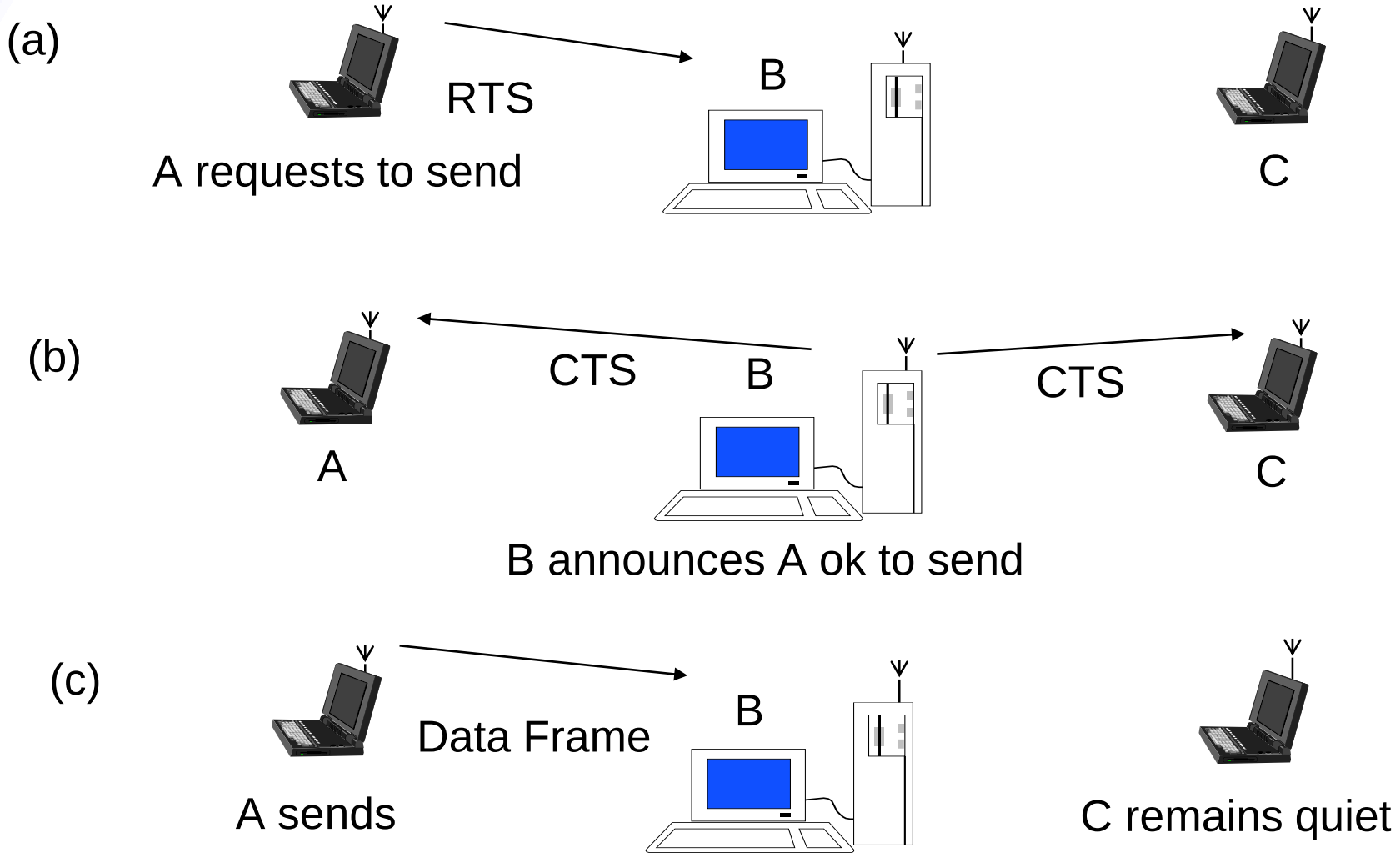
- Temporary association of group of stations
  - Within range of each other
  - Need to exchange information
  - E.g. Presentation in meeting, or distributed computer game, or both



- Permanent Access Points provide access to Internet



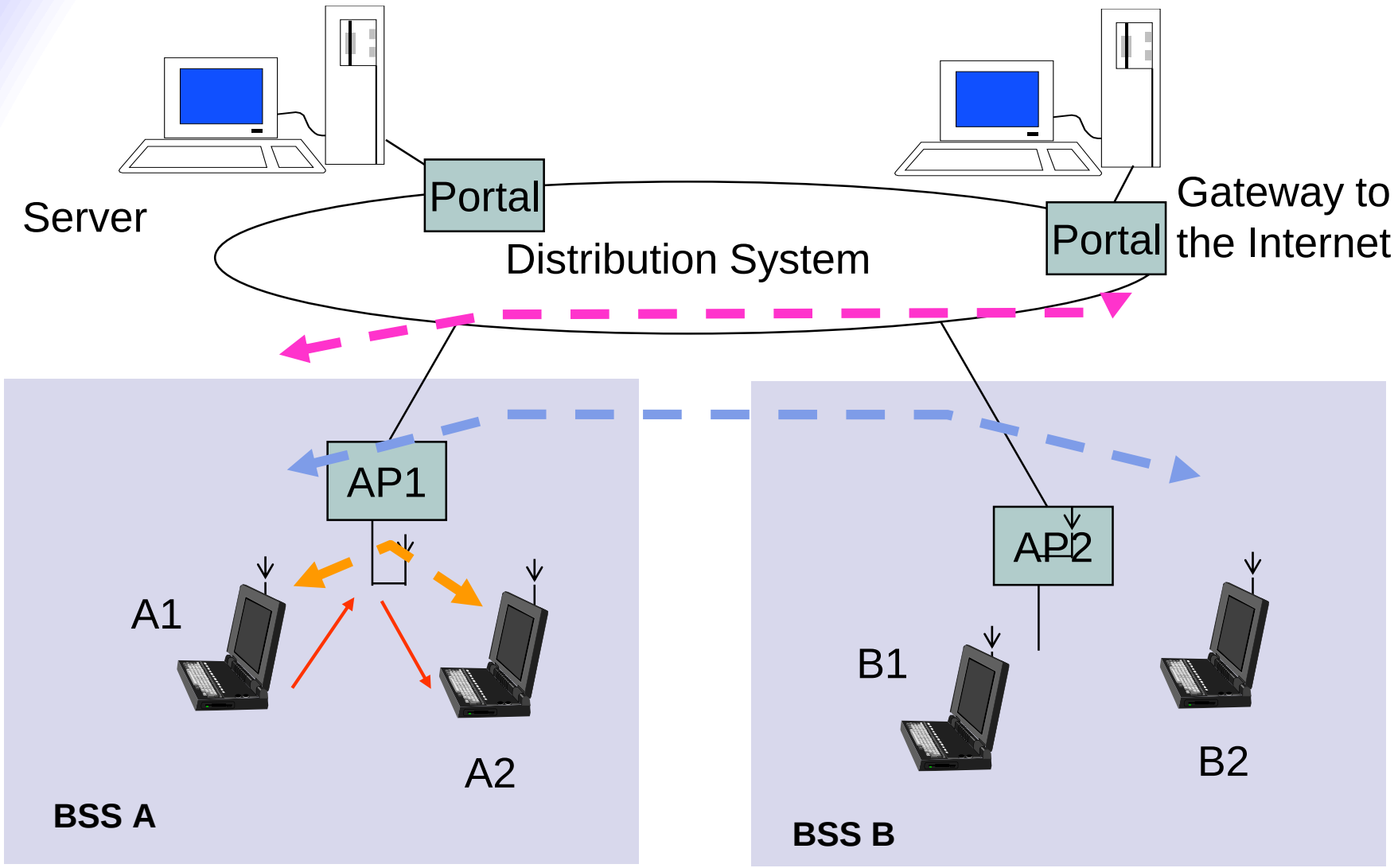
- New MAC: CSMA with *Collision Avoidance*


(a)
RTS
B
A requests to send
C
(b)
CTS
B
CTS
A
C
B announces A ok to send
(c)
Data Frame
B
A sends
C remains quiet

IEEE 802.11 Wireless LAN

- Stimulated by availability of *unlicensed spectrum*
  - U.S. Industrial, Scientific, Medical (ISM) bands
  - 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz
- Targeted wireless LANs @ 20 Mbps
- MAC for high speed wireless LAN
- Ad Hoc & Infrastructure networks
- Variety of physical layers

- *Basic Service Set* (BSS)
  - Group of stations that *coordinate their access* using a given instance of MAC
  - Located in a *Basic Service Area* (BSA)
  - Stations in BSS can communicate with each other
  - Distinct collocated BSS's can coexist
- *Extended Service Set* (ESS)
  - Multiple BSSs interconnected by *Distribution System (DS)*
  - Each BSS is like a cell and stations in BSS communicate with an *Access Point* (AP)
  - *Portals* attached to DS provide access to Internet


Server
Portal
Distribution System
Portal
Gateway to
the Internet
AP1
AP2
A1
A2
B1
B2
BSS A
BSS B

- Stations within BSS can communicate via AP
- DS provides *distribution services*:
  - Transfer MAC SDUs between APs in ESS
  - Transfer MSDUs between portals & BSSs in ESS
  - Transfer MSDUs between stations in same BSS
    - Multicast, broadcast, or stations's preference
- ESS looks like single BSS to LLC layer

- Select AP and establish *association* with AP
  - Then can send/receive frames via AP & DS
- *Reassociation service* to move from one AP to another AP
- *Dissociation service* to terminate association
- *Authentication service* to establish identity of other stations
- *Privacy service* to keep contents secret

- MAC sublayer responsibilities
  - Channel access
  - PDU addressing, formatting, error checking
  - Fragmentation & reassembly of MAC SDUs
- MAC security service options
  - Authentication & privacy
- MAC management services
  - Roaming within ESS
  - Power management

Chapter Summary

- Ethernet
- addressing and ARP
- switch and VLAN
- 802.11 wireless LAN

Reference

Chapter 6, Communication Networks: Fundamental Concepts and Key Architectures