COMPUTER NETWORKS

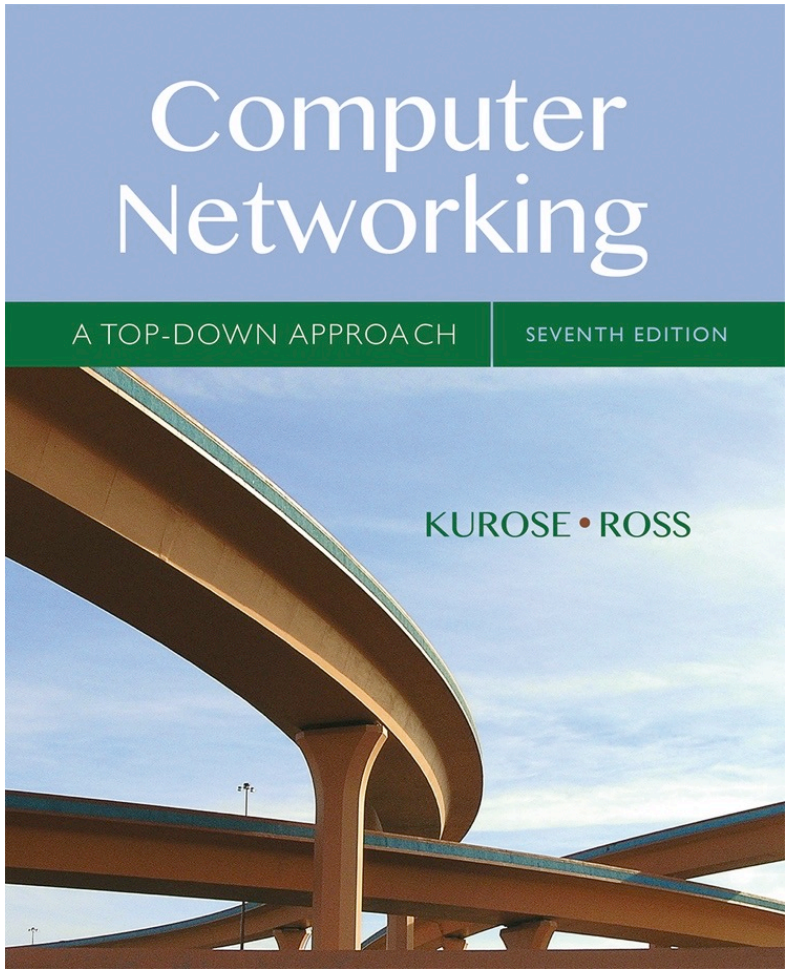
Ashwini M Joshi

Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

PES UNIVERSITY ONLINE

Text Book



Slides adapted from

Computer Networking: A Top-Down Approach

Jim Kurose, Keith Ross
Pearson, 2017
8th Edition

COMPUTER NETWORKS

Link Layer and LAN

Ashwini M Joshi
Department of Computer Science and Engineering

Unit – 5 Link Layer and LAN Roadmap

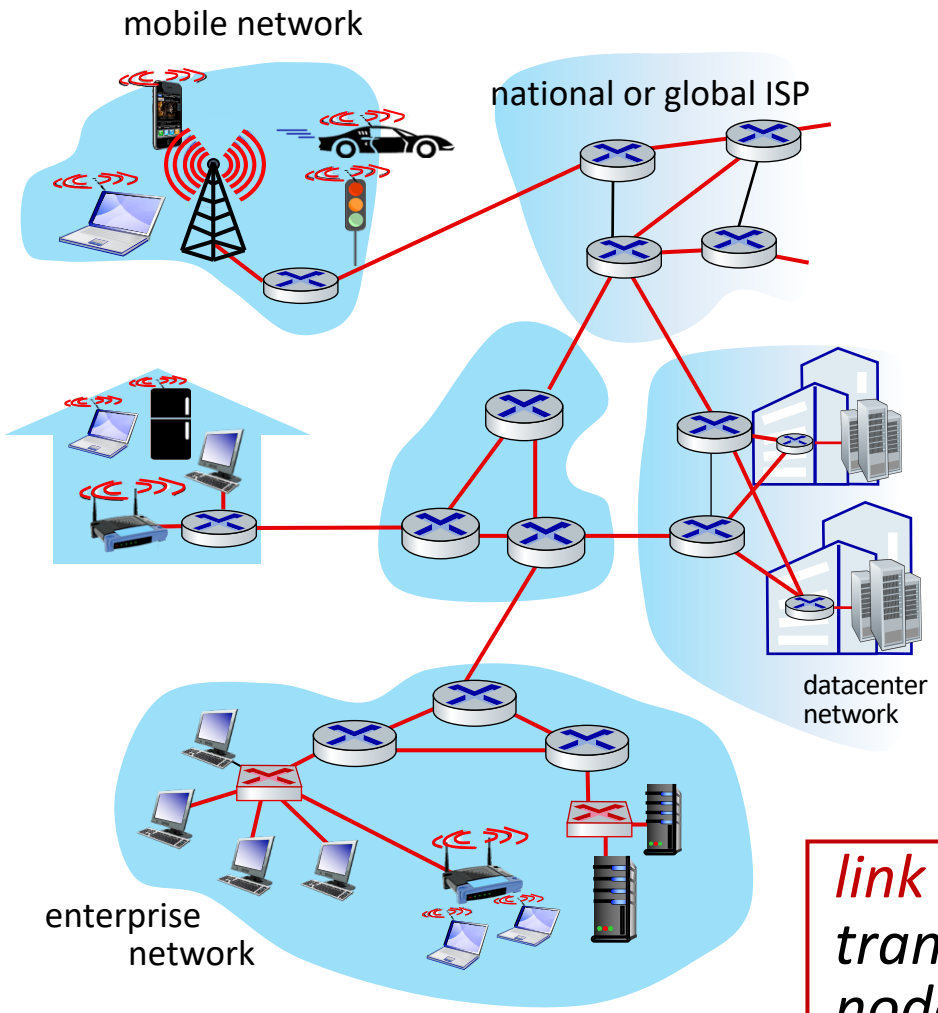
- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

COMPUTER NETWORKS

Class 47 : Intro to Link layer : Learning Objectives

- Introduction to link layer
- Error detection and correction techniques
  - Parity Checks
  - Internet Checksum
  - Cyclic Redundancy Check

Introduction to Link layer



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

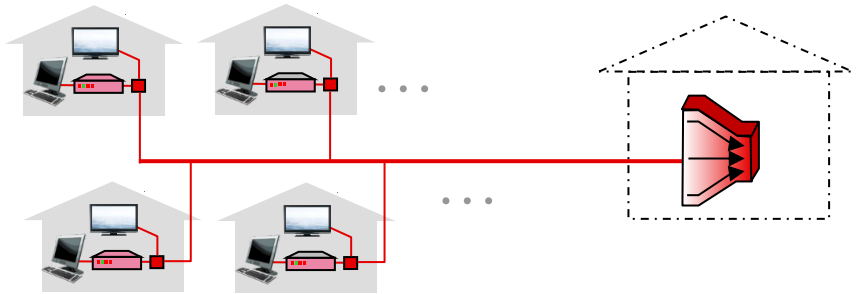
Link layer : context

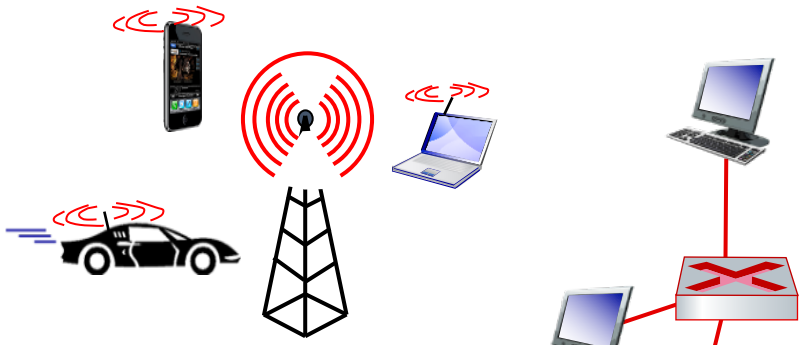
- Datagram transferred by different link protocols over different links:
  - e.g., WiFi on first link, Ethernet on next link
- Each link protocol provides different services
  - e.g., may or may not provide reliable data transfer over link

transportation analogy:

- trip from Princeton to Lausanne
  - limo: Princeton to JFK
  - plane: JFK to Geneva
  - train: Geneva to Lausanne
- tourist = datagram
- transport segment = communication link
- transportation mode = link-layer protocol
- travel agent = routing algorithm

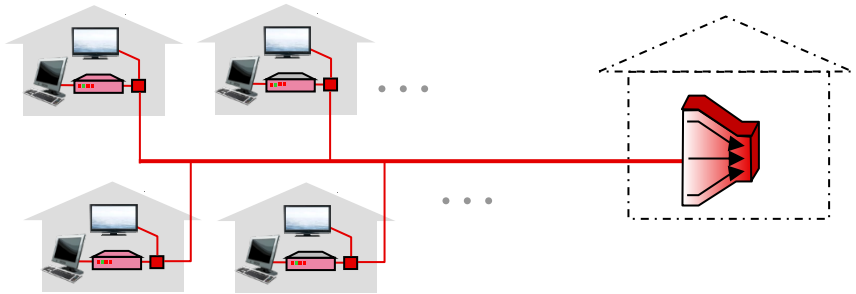
Link layer : services

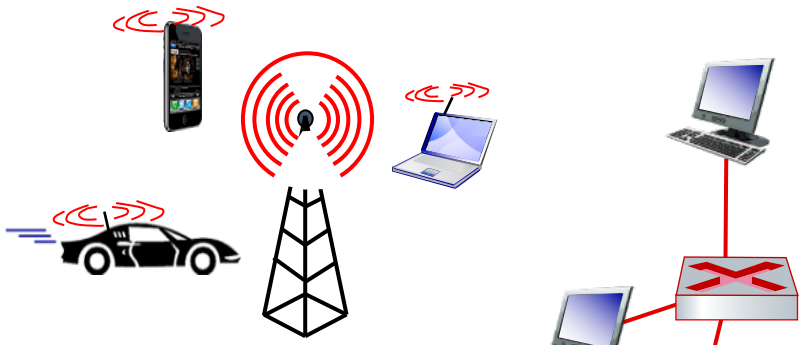




- Framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - “MAC” addresses in frame headers identify source, destination (different from IP address!)

Link layer : services

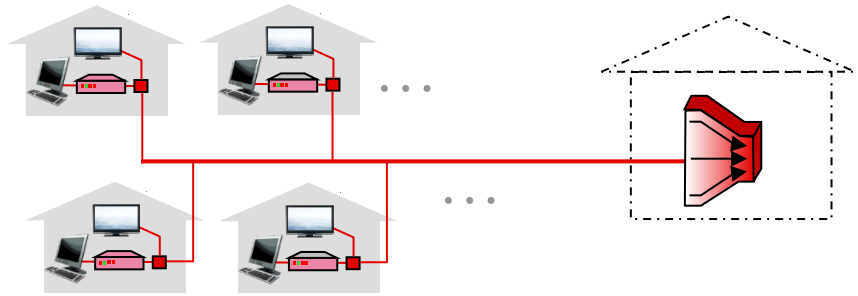


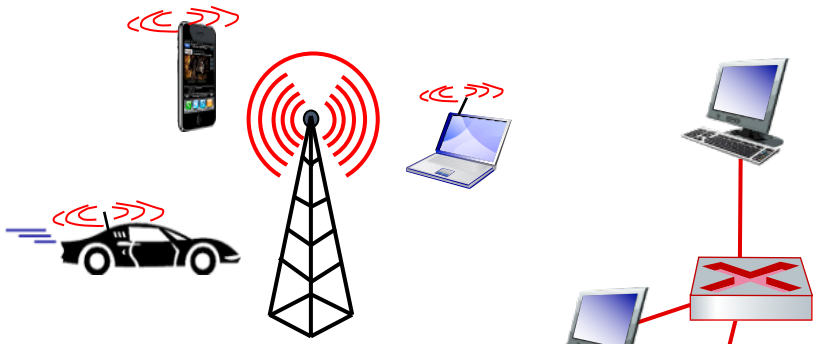


- Reliable delivery between adjacent nodes
  - we already know how to do this!
  - seldom used on low bit-error links
  - wireless links: high error rates
    - *Q:* why both link-level and end-end reliability?

COMPUTER NETWORKS

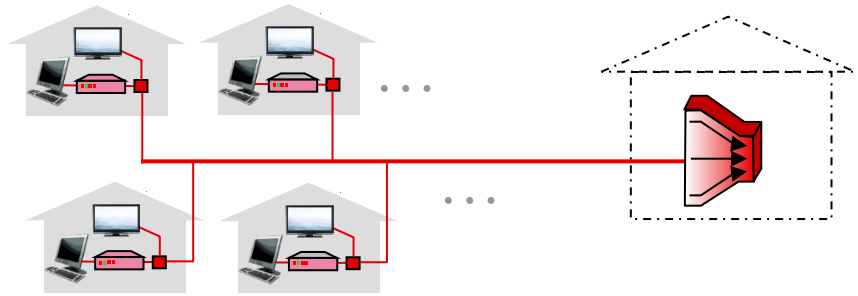
Link layer : services (more)

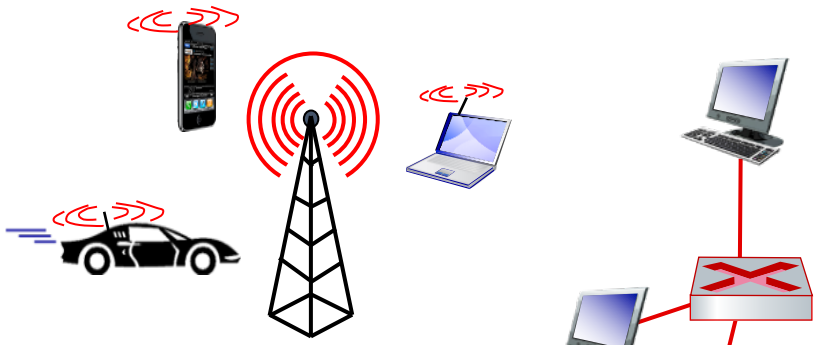




- Flow control:
  - pacing between adjacent sending and receiving nodes
- Error detection:
  - errors caused by signal attenuation, noise.
  - receiver detects errors, signals retransmission, or drops frame

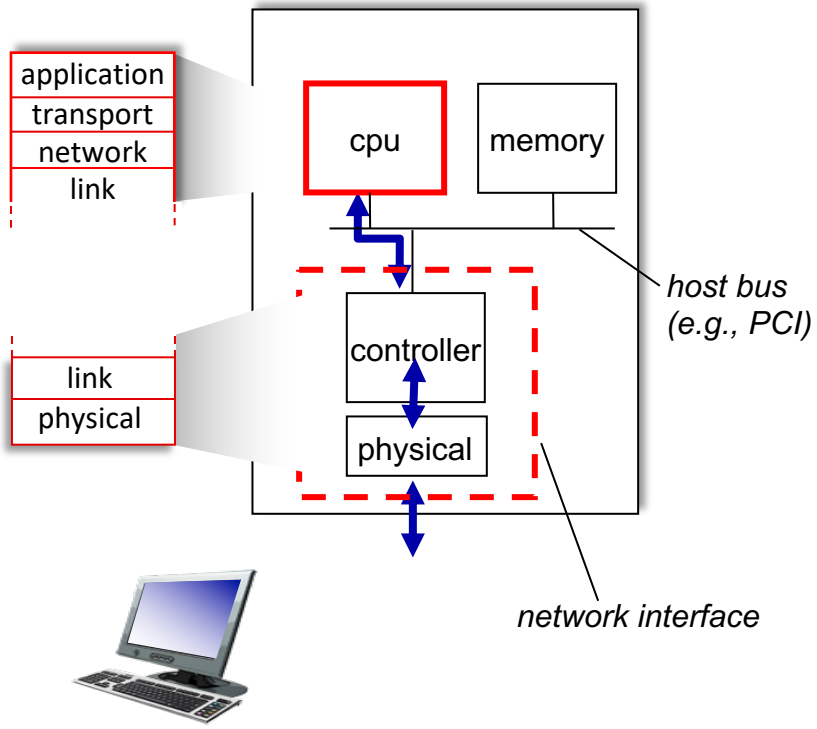
Link layer : services (more)





- 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

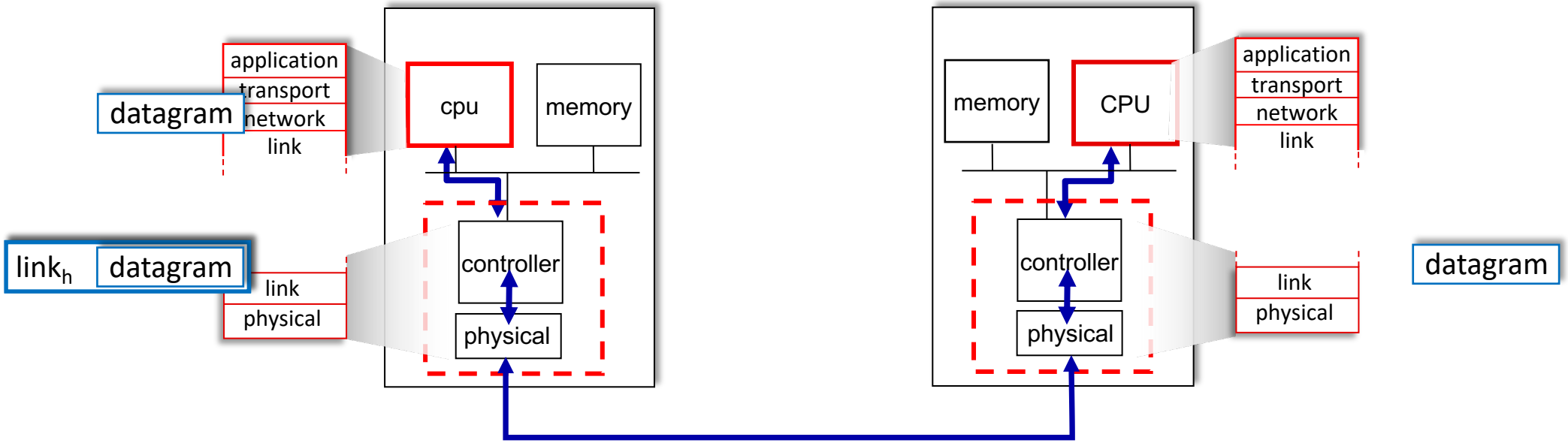
Where is the link layer implemented?



- In each-and-every host
- Link layer implemented in *network interface card* (NIC) or on a chip
  - Ethernet, WiFi card or chip
  - implements link, physical layer
- Attaches into host's system buses
- Combination of hardware, software, firmware

COMPUTER NETWORKS

Interfaces communicating



Sending side:

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

Receiving side:

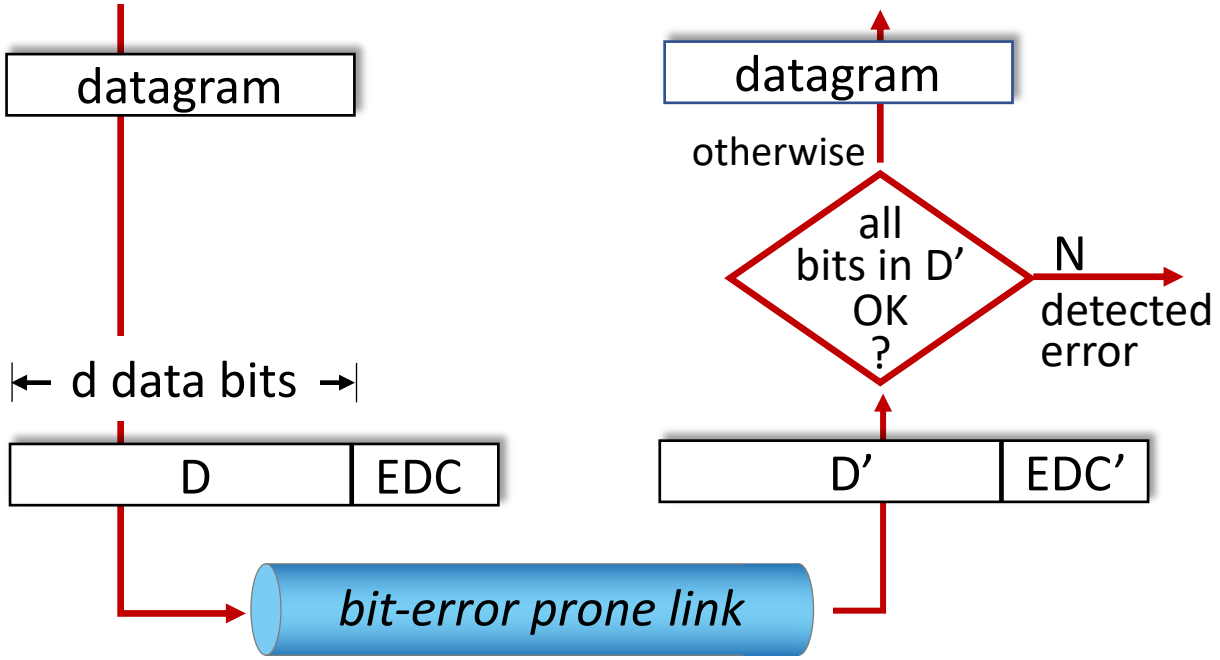
- looks for errors, reliable data transfer, flow control, etc.
- extracts datagram, passes to upper layer at receiving side

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

Error detection

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

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



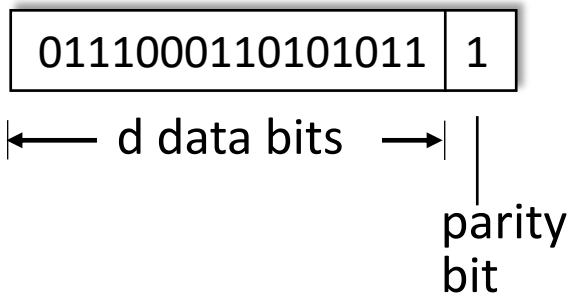
Error detection not 100% reliable!

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

Parity checking

Single bit parity:

- detect single bit errors



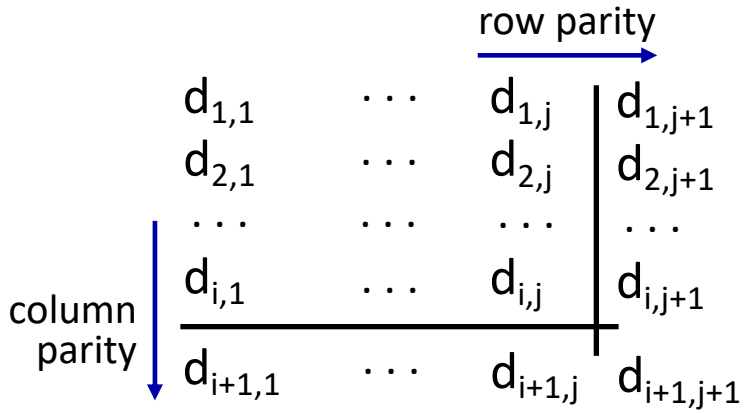
Even parity: set parity bit so there is an even number of 1's

no errors:

1	0	1	0	1	1
1	1	1	1	0	0
0	1	1	1	0	1
1	0	1	0	1	0

Two-dimensional bit parity:

- detect *and correct* single bit errors



detected and correctable single-bit error:

1	0	1	0	1	1
1	0	1	1	0	0
0	1	1	1	0	1
1	0	1	0	1	0

parity error

parity error

* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Internet checksum (review)

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. *But maybe errors nonetheless?* More later ….

Cyclic Redundancy Check (CRC)

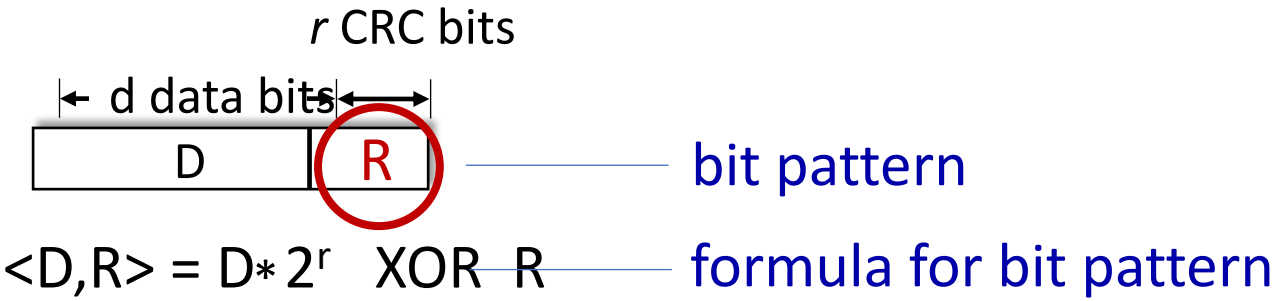
- More powerful error-detection coding
- D: data bits (given, think of these as a binary number)
- G: bit pattern (generator), of *r+1* bits (given)

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)



Cyclic Redundancy Check (CRC) : example

We want:

$D \cdot 2^r \ XOR \ R = nG$

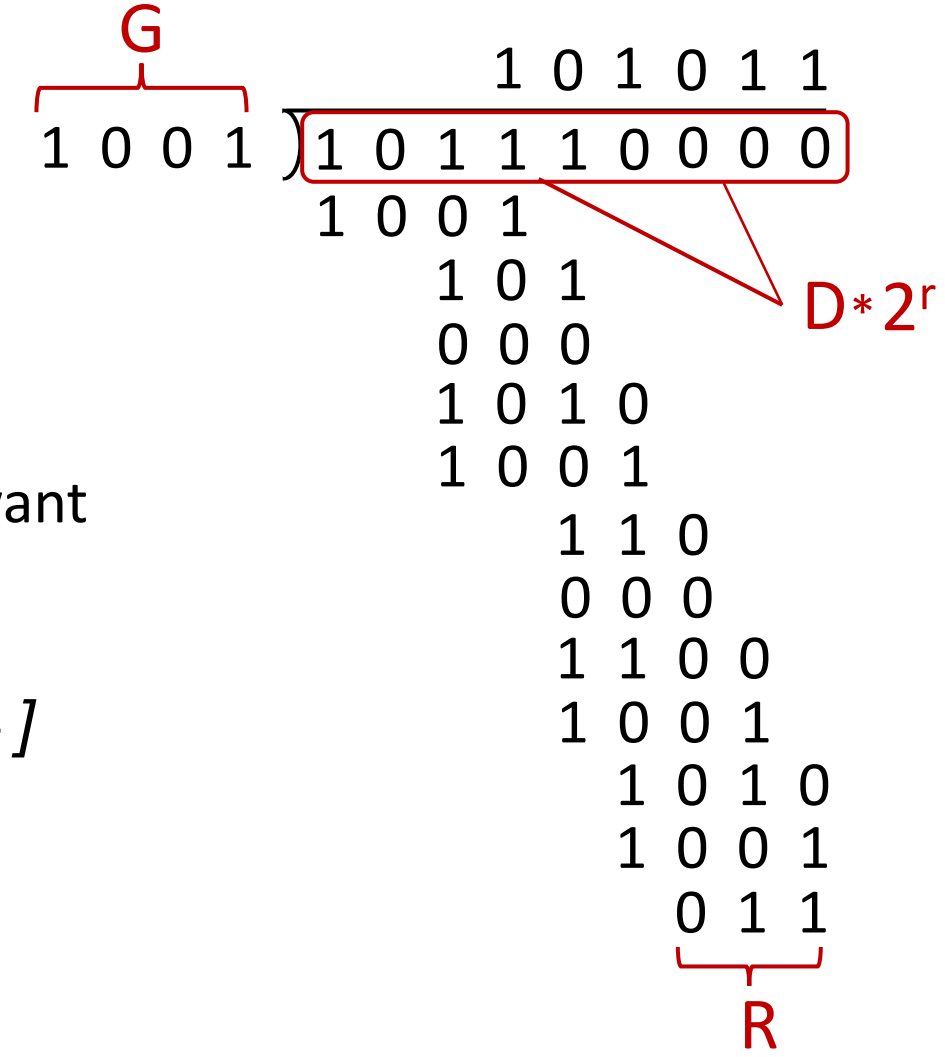
or equivalently:

$D \cdot 2^r = nG \ XOR \ R$

or equivalently:

if we divide $D \cdot 2^r$ by G, want remainder R to satisfy:

$$R = remainder\left[\frac{D \cdot 2^r}{G}\right]$$



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - addressing, ARP
  - Ethernet
  - switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

Class 48 : Multiple Access Protocols : Learning Objectives

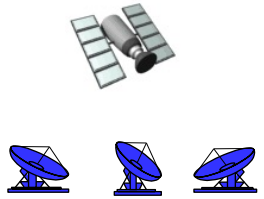
- Multiple Access Protocols-Taxonomy
- Carrier Sense Multiple Access
- CSMA/CD

Multiple access links protocols

shared wire (e.g., cabled Ethernet)

shared radio: 4G/5G

shared radio: WiFi



shared radio: satellite

humans at a cocktail party (shared air, acoustical)

Two types of “links”:

- point-to-point
  - point-to-point link between Ethernet switch, host
  - PPP for dial-up access
- broadcast (shared wire or medium)
  - old-fashioned Ethernet
  - upstream HFC in cable-based access network
  - 802.11 wireless LAN, 4G/4G. satellite

Multiple access protocols

- Single shared broadcast channel
- Two or more simultaneous transmissions by nodes: interference
  - *collision* if node receives two or more signals at the same time

Multiple access protocol

- Distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
- Communication about channel sharing must use channel itself!
  - no out-of-band channel for coordination

An ideal Multiple access protocol

Given: multiple access channel (MAC) of rate *R* bps

desiderata:

1. when one node wants to transmit, it can send at rate *R*.
2. when M nodes want to transmit, each can send at average rate *R/M*
3. fully decentralized:
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. simple

MAC protocols : Taxonomy

Three broad classes:

- channel partitioning
  - divide channel into smaller “pieces” (time slots, frequency, code)
  - allocate piece to node for exclusive use
- *random access*
  - channel not divided, allow collisions
  - “recover” from collisions
- “taking turns”
  - nodes take turns, but nodes with more to send can take longer turns

CSMA (Carrier Sense Multiple Access)

Simple CSMA: listen before transmit:

- if channel sensed idle: transmit entire frame
- if channel sensed busy: defer transmission

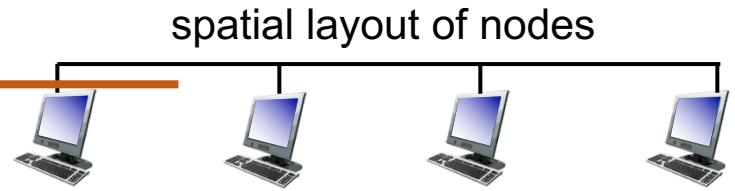
- Human analogy: don't interrupt others!

CSMA/CD: CSMA with *collision detection*

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- collision detection easy in wired, difficult with wireless

- human analogy: the polite conversationalist

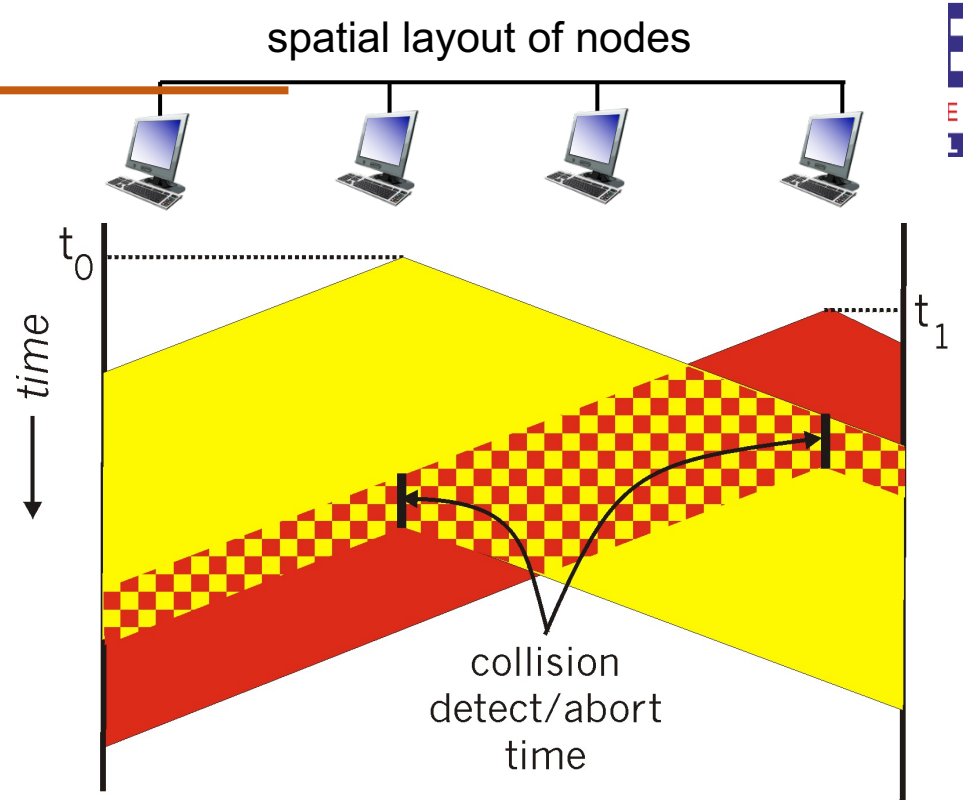
CSMA : Collisions



- Collisions *can* still occur with carrier sensing:
  - Propagation delay means two nodes may not hear each other's just-started transmission
- Collision: entire packet transmission time wasted
  - Distance & propagation delay play role in in determining collision probability

CSMA / CD

- CSMA/CS reduces the amount of time wasted in collisions
  - transmission aborted on collision detection



Ethernet CSMA / CD Algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel:

   if idle: start frame transmission.

   if busy: wait until channel idle, then transmit
3. If NIC transmits entire frame without collision, NIC is done with frame !
4. If NIC detects another transmission while sending: abort, send jam signal
5. After aborting, NIC enters *binary (exponential) backoff:*
   - after *m*th collision, NIC chooses *K* at random from $\{0,1,2, \ldots, 2^m-1\}$. NIC waits $K \cdot 512$ bit times, returns to Step 2
   - more collisions: longer backoff interval

CSMA / CD Efficiency

- T_{prop} = max prop delay between 2 nodes in LAN
- t_{trans} = time to transmit max-size frame

$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

- efficiency goes to 1
  - as t_{prop} goes to 0
  - as t_{trans} goes to infinity
- better performance than ALOHA: and simple, cheap, decentralized!

THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

COMPUTER NETWORKS

Class 49 : Switched LAN : Learning Objectives

- Link layer Addressing
- Address Resolution Protocol

MAC Addresses

- 32-bit IP address:
  - *network-layer* address for interface
  - used for layer 3 (network layer) forwarding
  - e.g.: 128.119.40.136

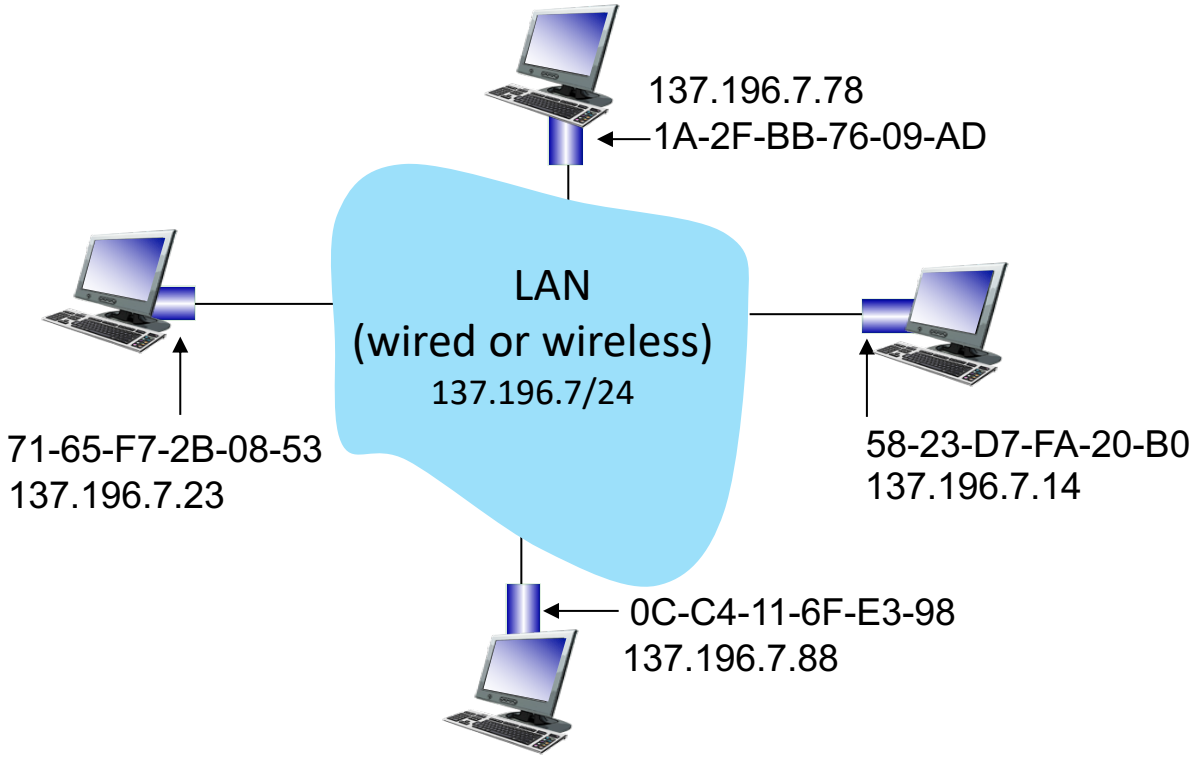
- MAC (or LAN or physical or Ethernet) address:
  - function: used "locally" to get frame from one interface to another physically-connected interface (same subnet, in IP-addressing sense)
  - 48-bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

hexadecimal (base 16) notation (each "numeral" represents 4 bits)

MAC Addresses

Each interface on LAN

- has unique 48-bit MAC address
- has a locally unique 32-bit IP address (as we've seen)

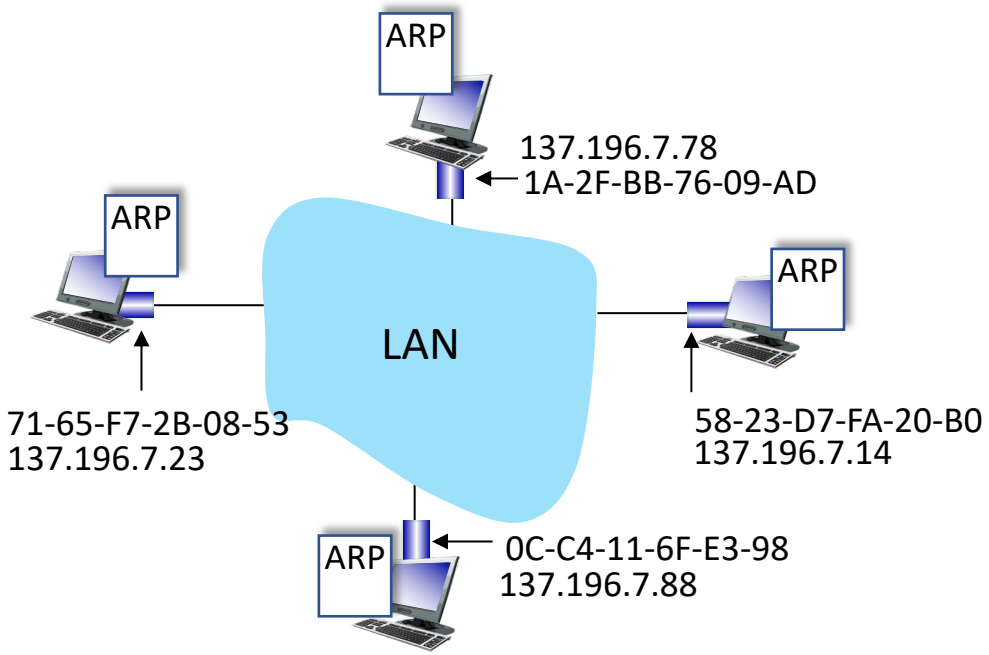


MAC Addresses

- 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 interface from one LAN to another
  - recall IP address *not* portable: 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 in action

Example: A wants to send datagram to B

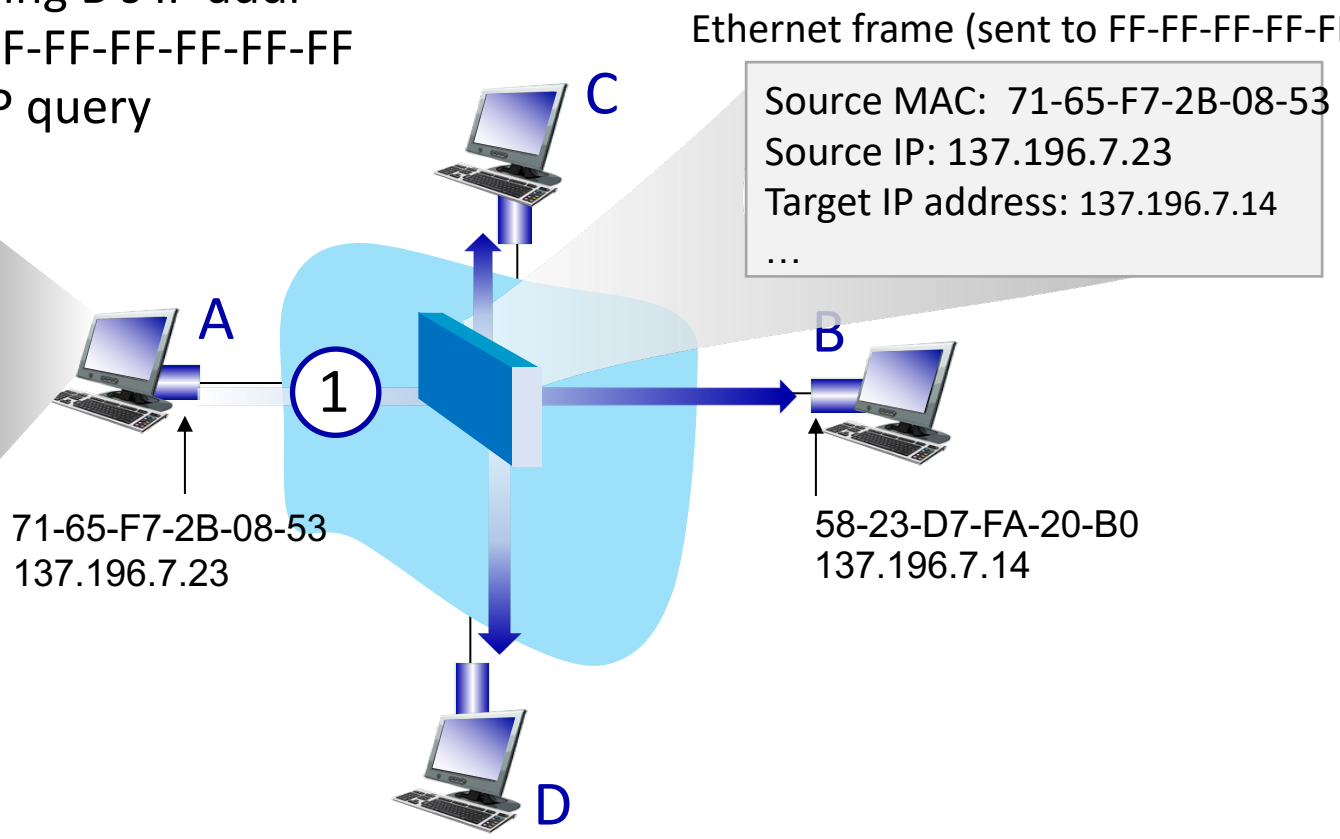
- B's MAC address not in A's ARP table, so A uses ARP to find B's MAC address

A broadcasts ARP query, containing B's IP addr

1
- destination MAC address = FF-FF-FF-FF-FF-FF
- all nodes on LAN receive ARP query

ARP table in A

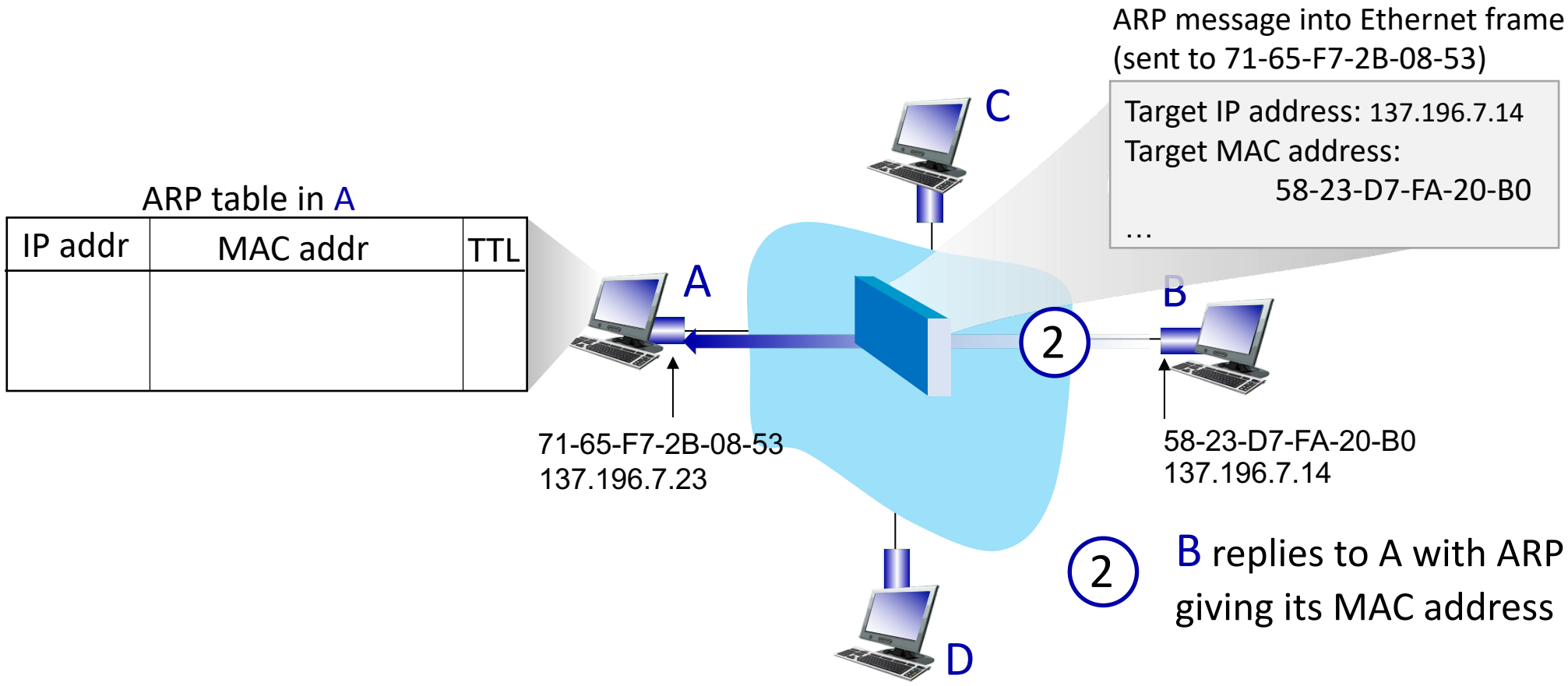
IP addr	MAC addr	TTL



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



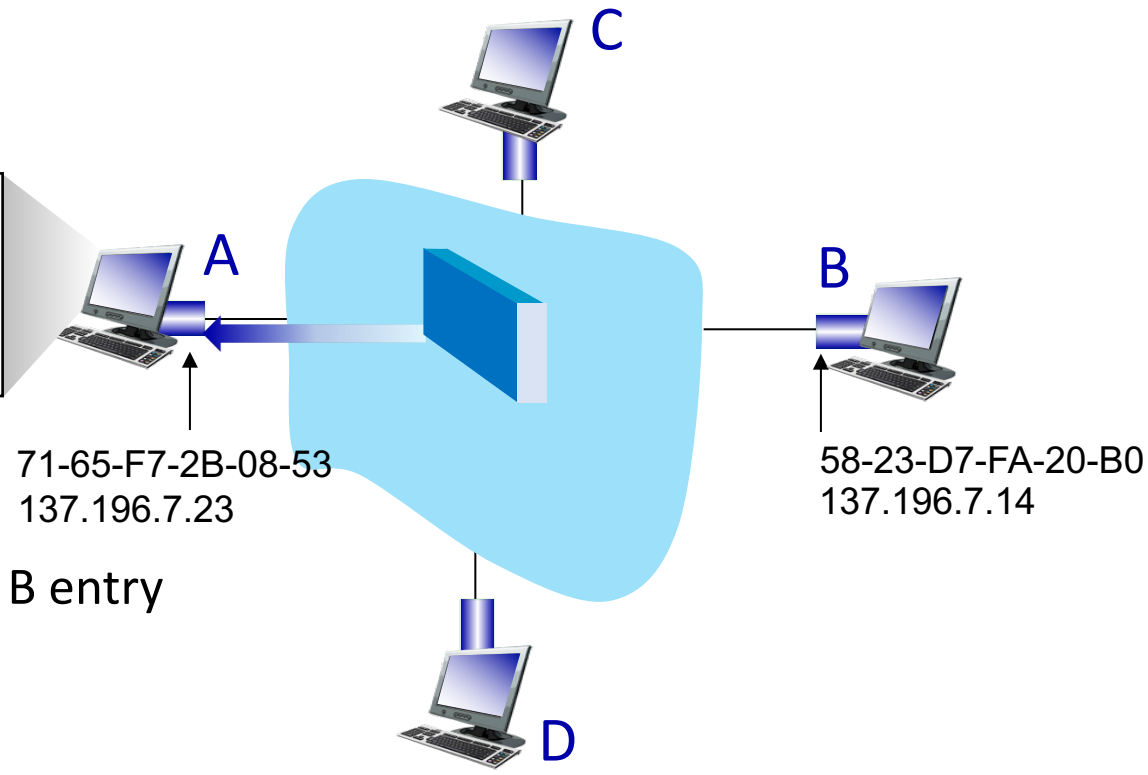
ARP Protocol in action

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

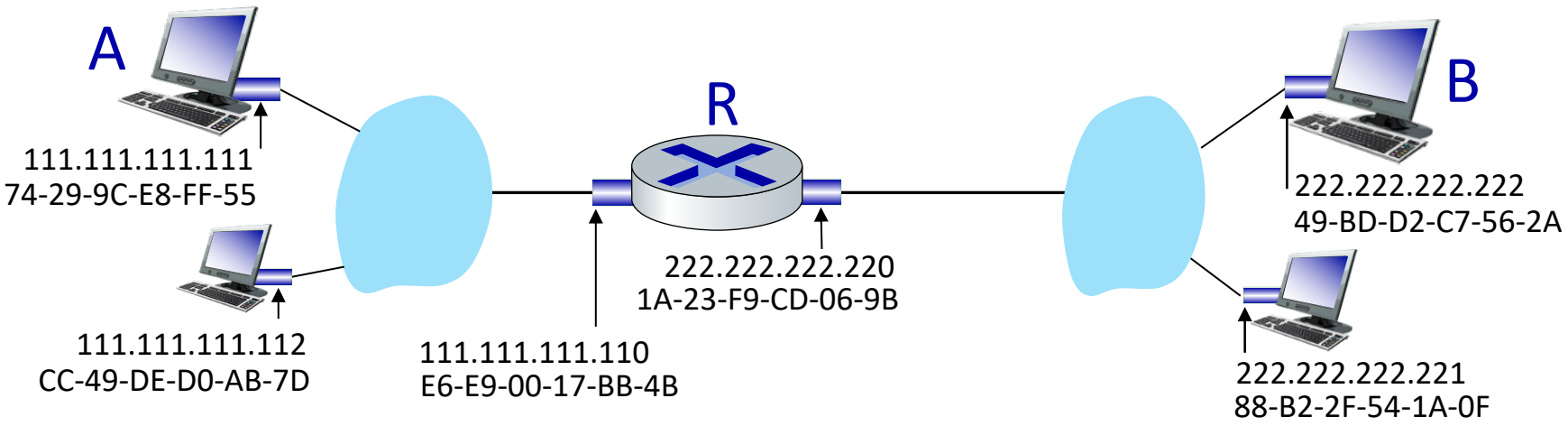


(3) A receives B's reply, adds B entry into its local ARP table

Routing to another Subnet : Addressing

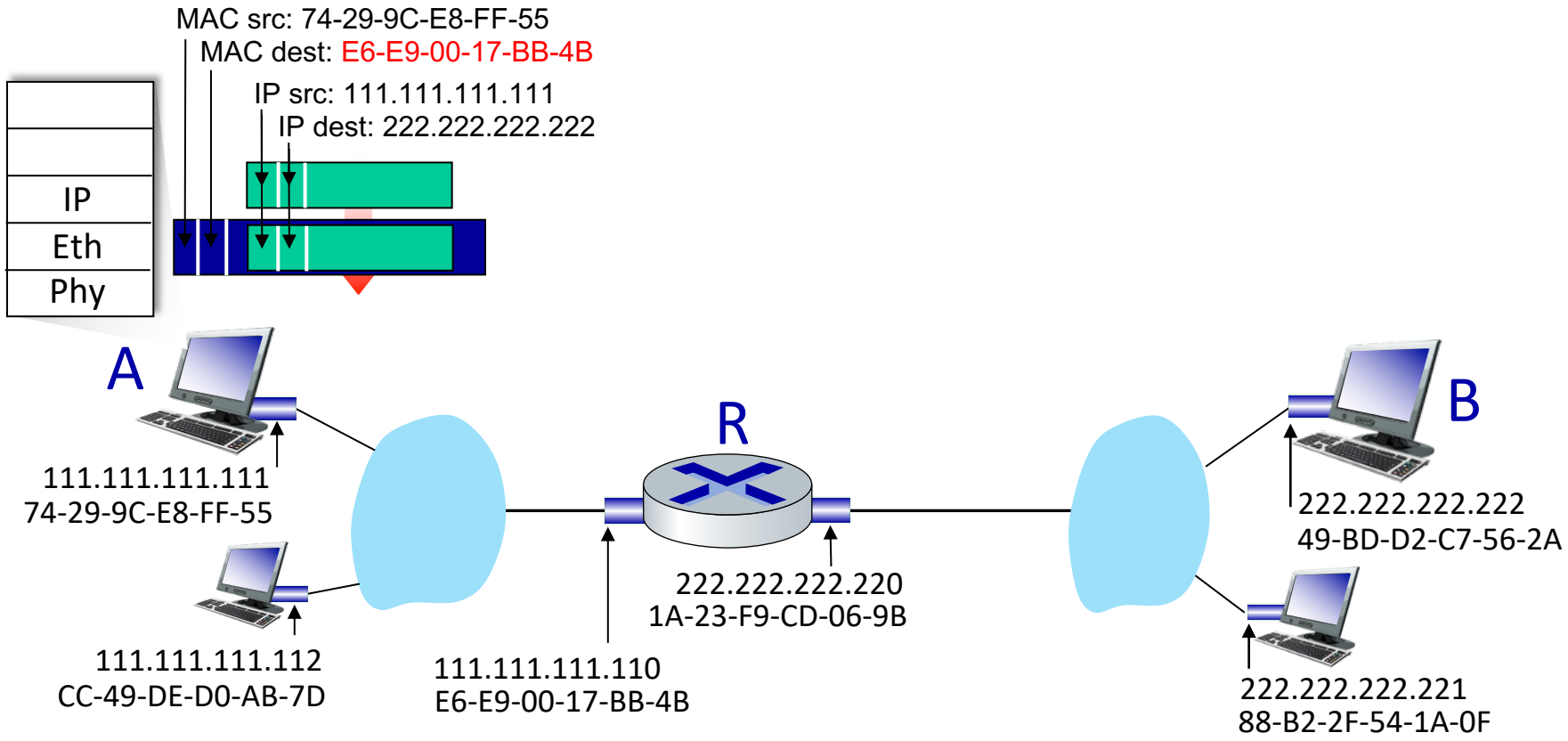
Walkthrough: sending a datagram from *A* to *B* via *R*

- 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 (how?)
  - A knows R's MAC address (how?)



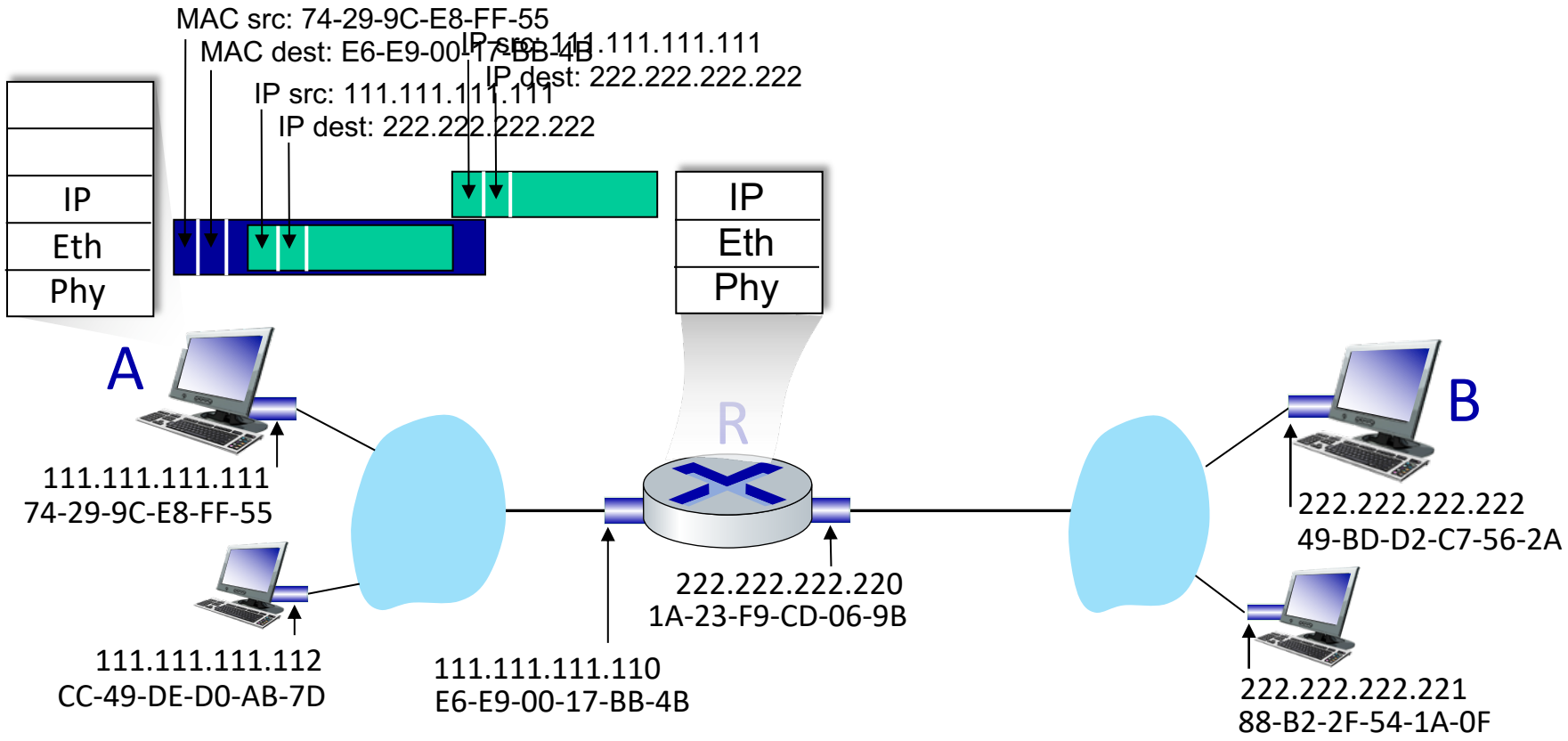
Routing to another Subnet : Addressing

- 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



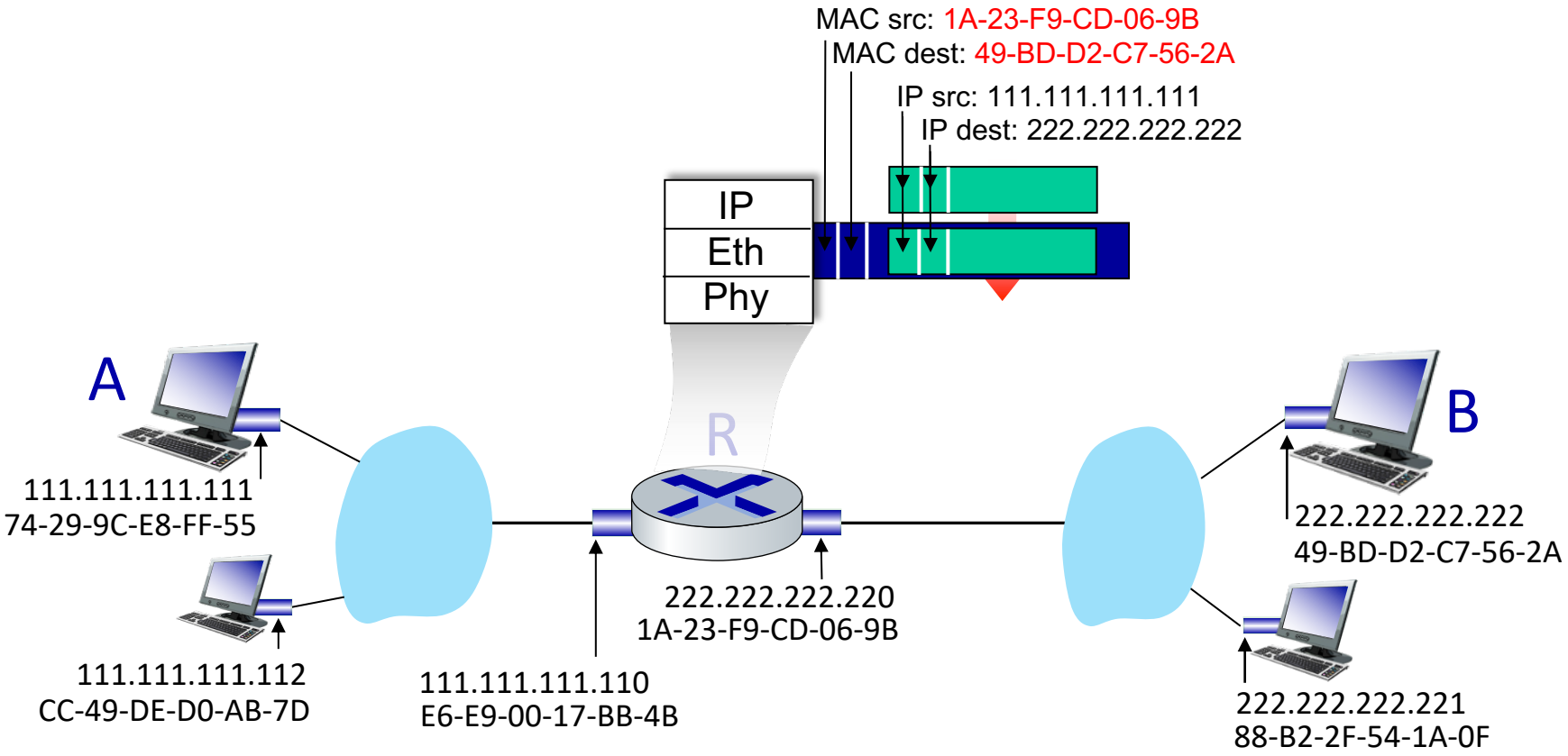
Routing to another Subnet : Addressing

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



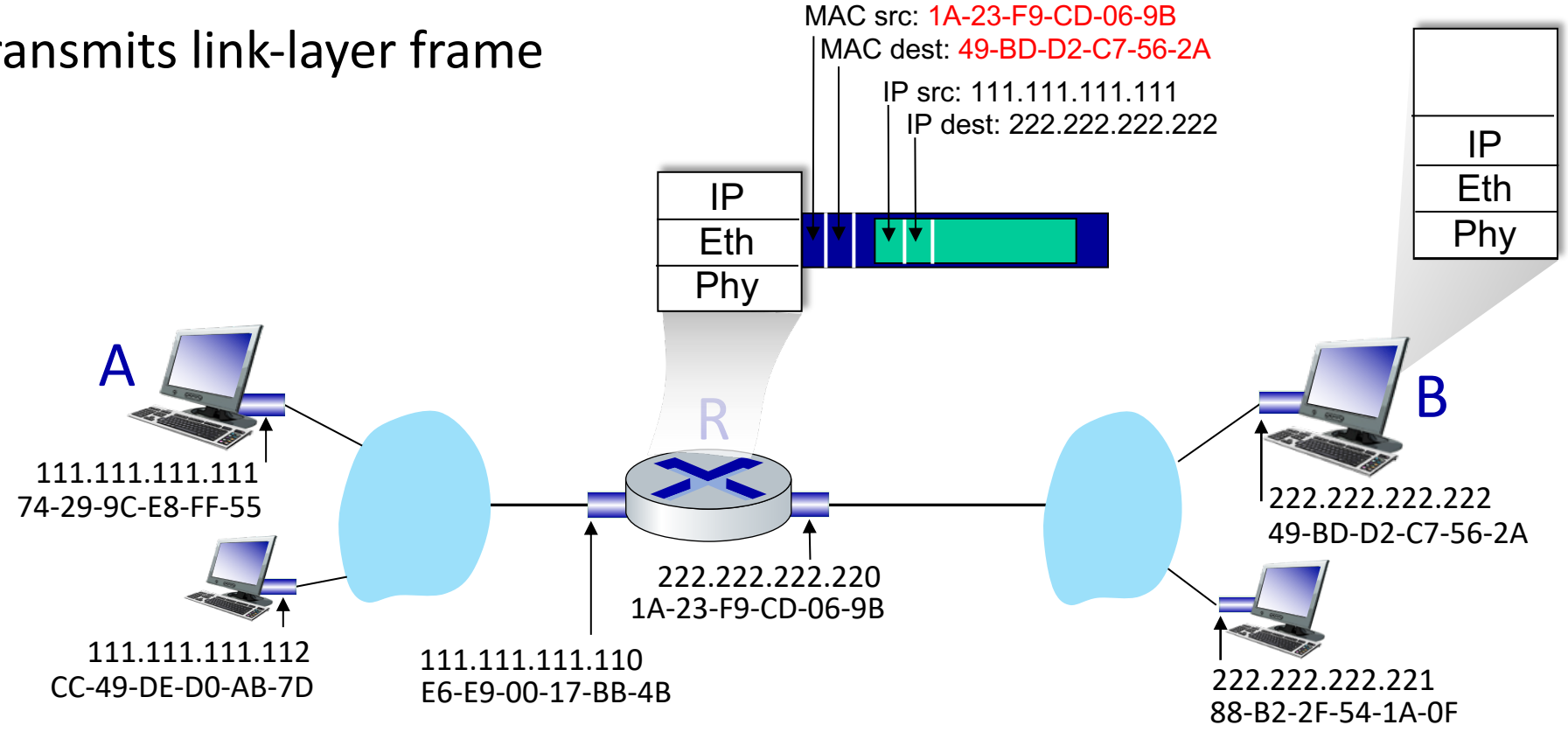
Routing to another Subnet : Addressing

- 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



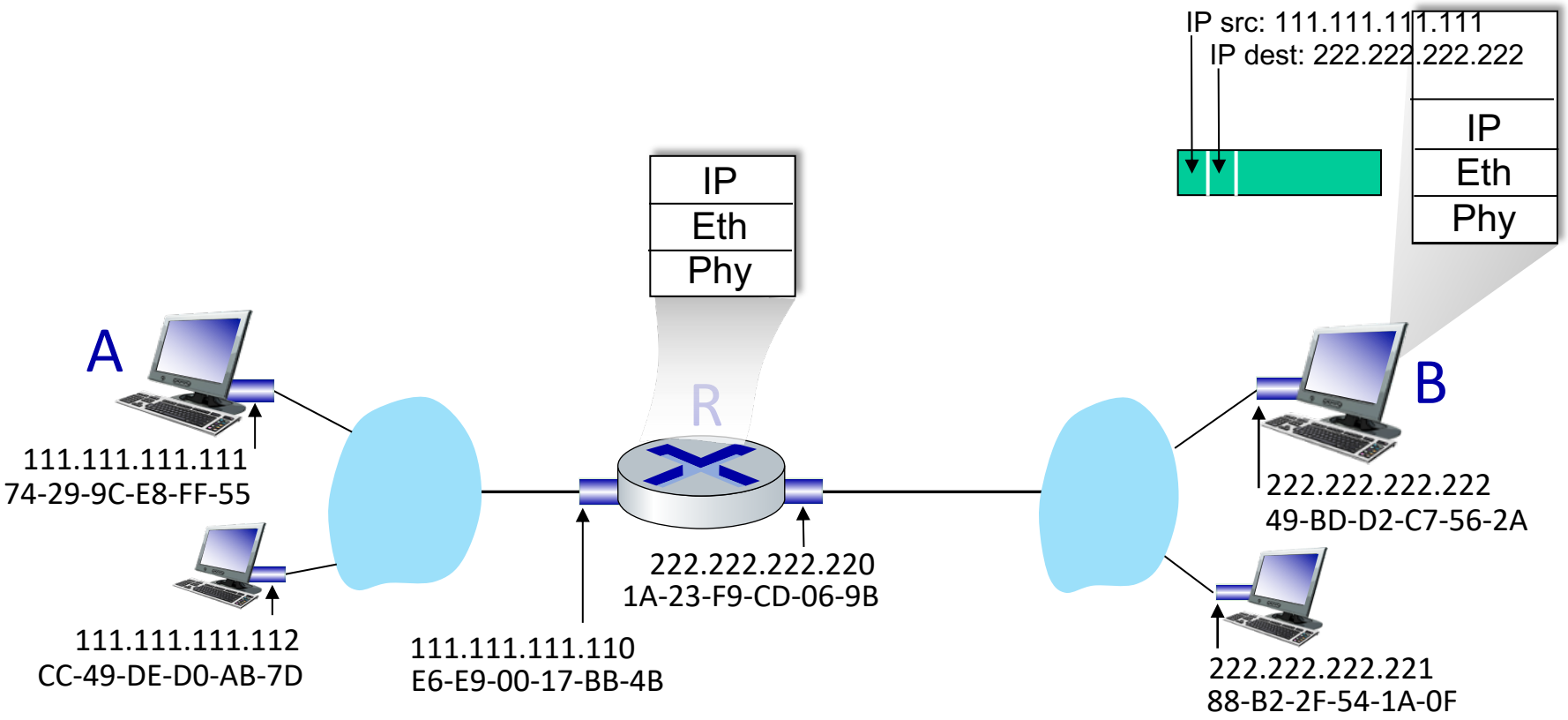
Routing to another Subnet : Addressing

- 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



Routing to another Subnet : Addressing

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



THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

COMPUTER NETWORKS

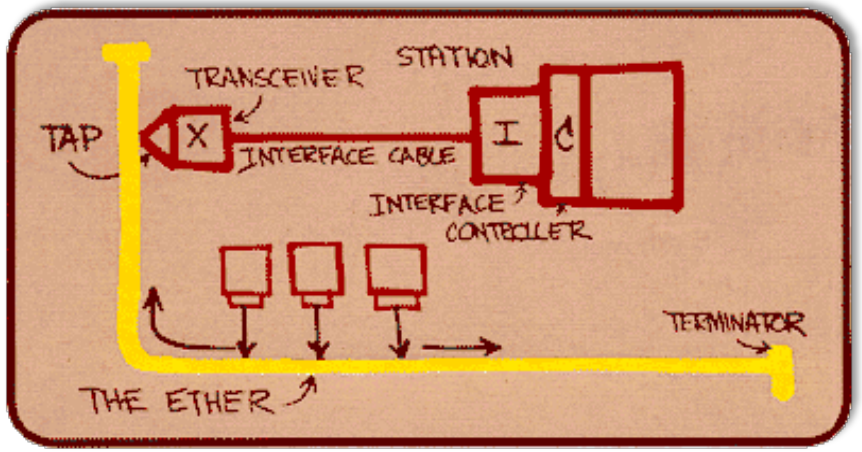
Class 50 : Ethernet : Learning Objectives

- Physical Topology
- Frame Structure

Ethernet

"Dominant" wired LAN technology:

- First widely used LAN technology
- Simpler, cheap
- Kept up with speed race: 10 Mbps – 400 Gbps
- Single chip, multiple speeds (e.g., Broadcom BCM5761)



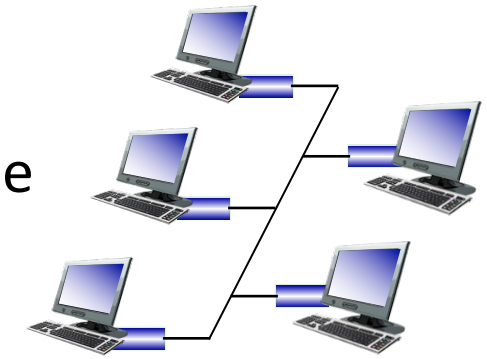
Metcalfe's Ethernet sketch

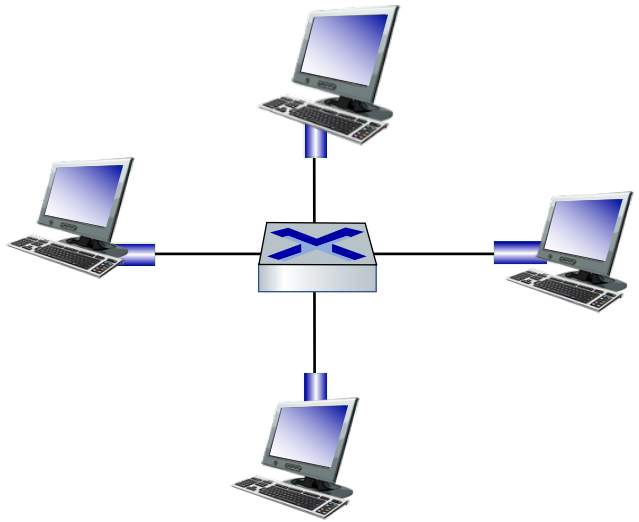
https://www.uspto.gov/learning-and-resources/journeys-innovation/audio-stories/defying-doubters

Ethernet : Physical Topology

- Bus: popular through mid 90s
  - all nodes in same collision domain (can collide with each other)
- Switched: prevails today
  - active link-layer 2 *switch* in center
  - each “spoke” runs a (separate) Ethernet protocol (nodes do not collide with each other)

bus: coaxial cable





switched

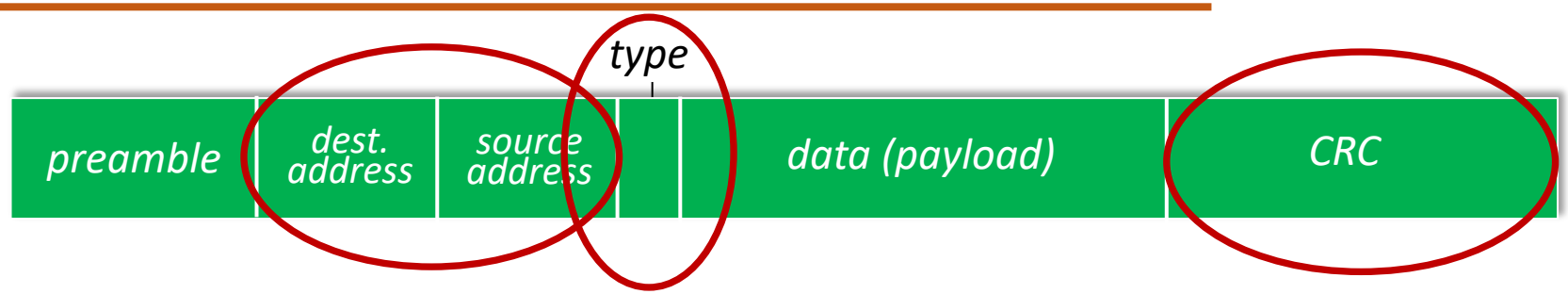
Ethernet Frame Structure

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

Preamble:

- Used to synchronize receiver, sender clock rates
- 7 bytes of 10101010 followed by one byte of 10101011

Ethernet Frame Structure (more)



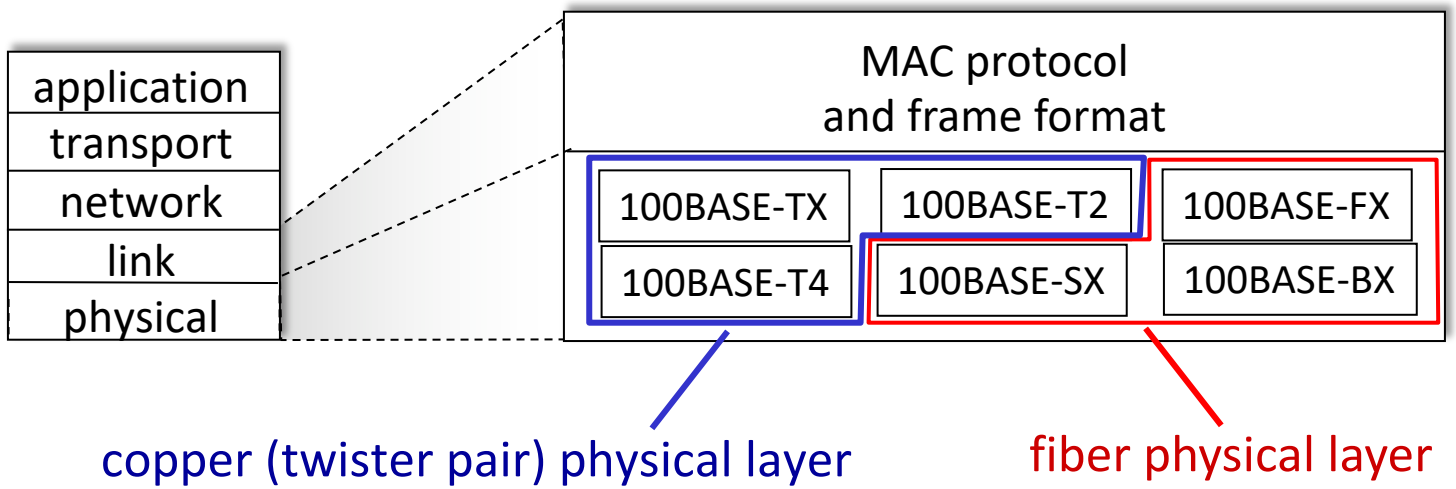
- Addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- Type: indicates higher layer protocol
  - mostly 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

Ethernet : Unreliable Connectionless

- Connectionless: no handshaking between sending and receiving NICs
- Unreliable: receiving NIC doesn't send ACKs or NAKs to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted CSMA/CD with binary backoff

802.3 Ethernet Standards: Link and 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



THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

Class 51 : Link Layer Switches : Learning Objectives

- Multiple Simultaneous Transmissions
- Frame Forwarding and Filtering

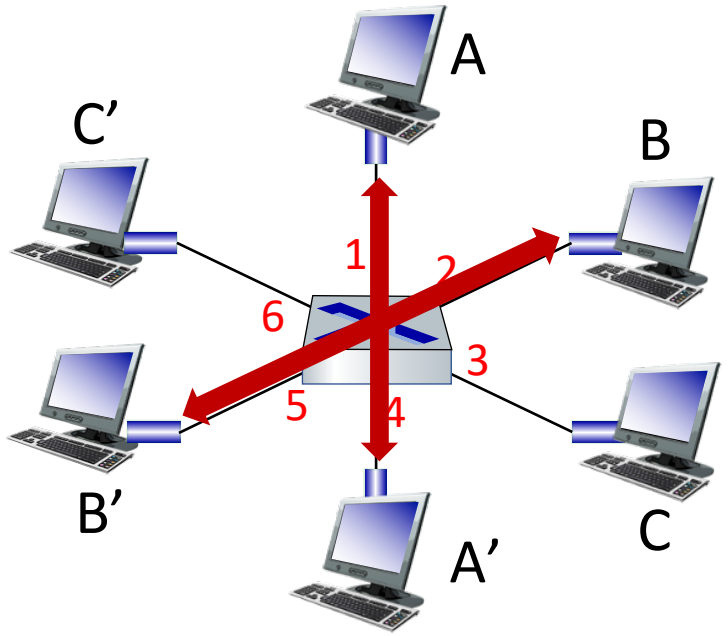
Ethernet switch

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

Switch : Multiple Simultaneous Transmissions

- Hosts have dedicated, direct connection to switch
- Switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain

- Switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions

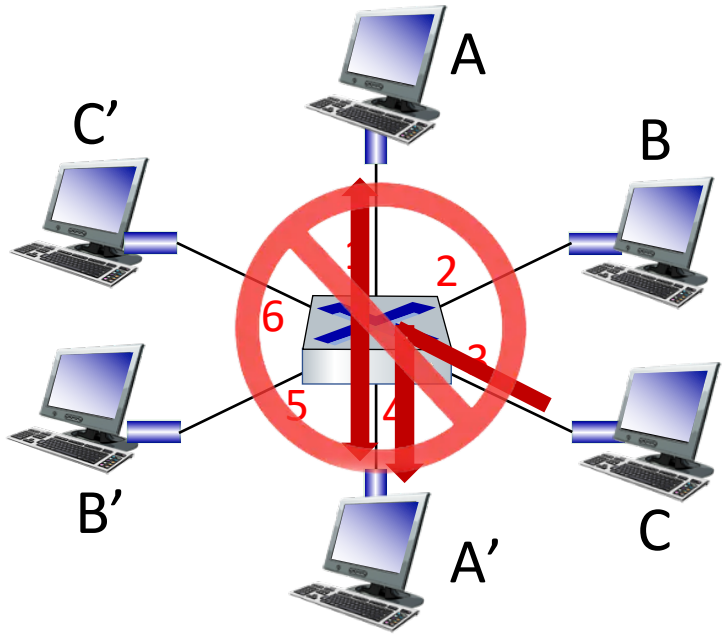


switch with six interfaces (1,2,3,4,5,6)

Switch : Multiple Simultaneous Transmissions

- Hosts have dedicated, direct connection to switch
- Switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - No collisions; full duplex
  - Each link is its own collision domain

- 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

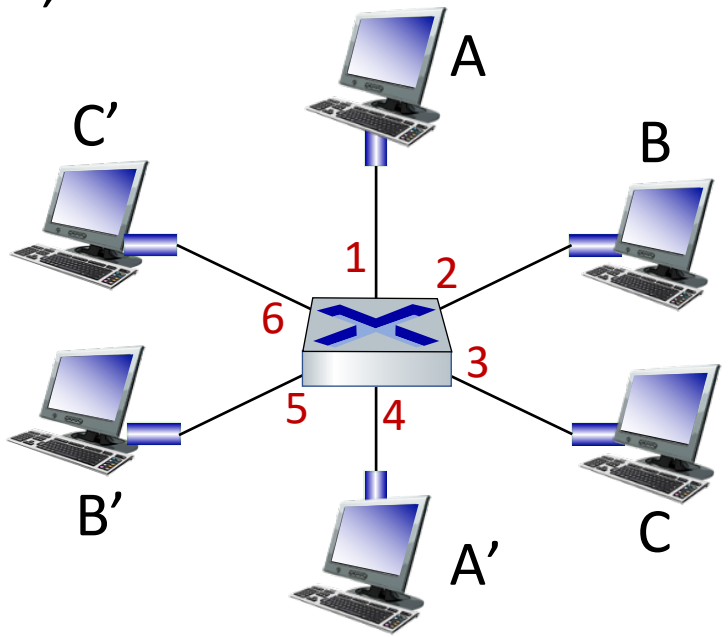
Q: How does switch know A' reachable via interface 4, B' reachable via interface 5?

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

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

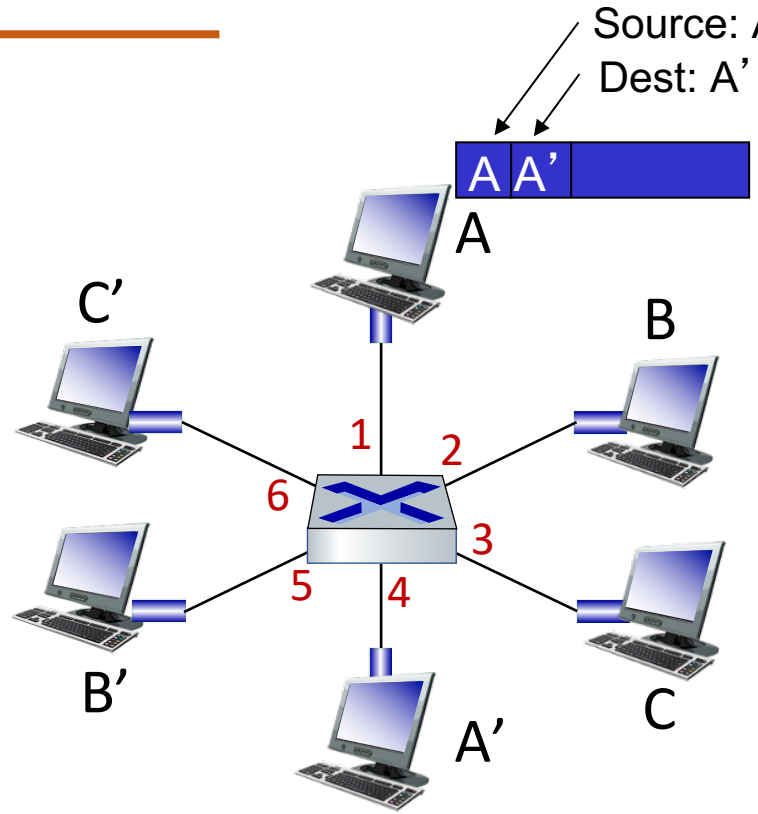
Q: How are entries created, maintained in switch table?

- something like a routing protocol?



Switch : Self - learning

- 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



Switch table (initially empty)

MAC addr	interface	TTL
A	*1*	*60*

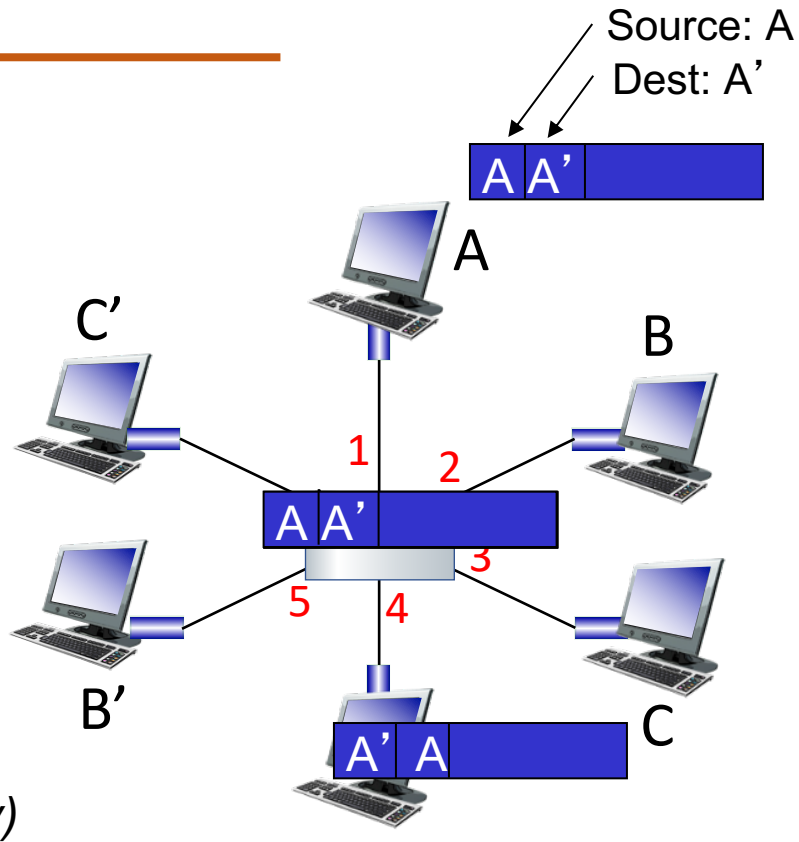
Switch : Frame Filtering / Forwarding

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
   */

Self-learning, Forwarding : Example

- Frame destination, A', location unknown: Flood
- Destination A location known: Selectively send on just one link

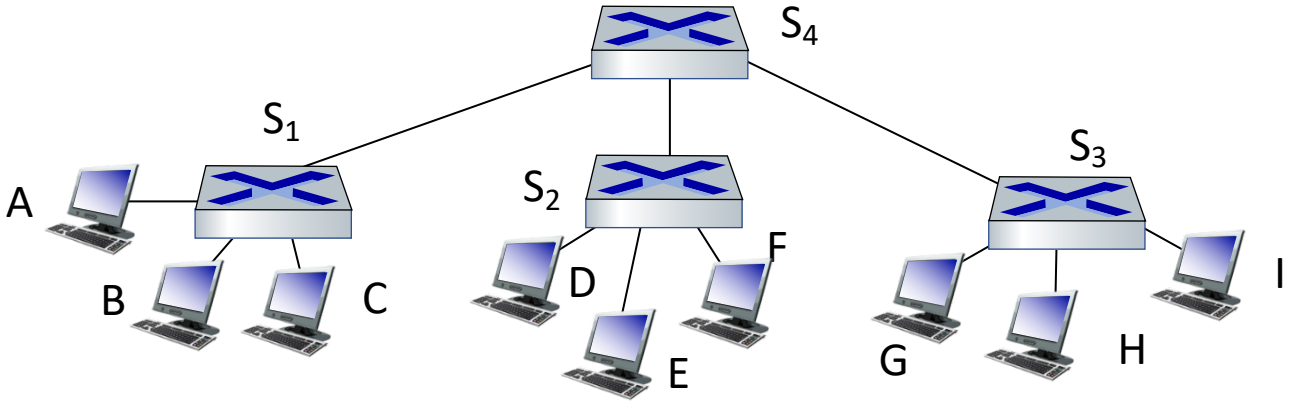


MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

Interconnecting Switches

Self-learning switches can be connected together:

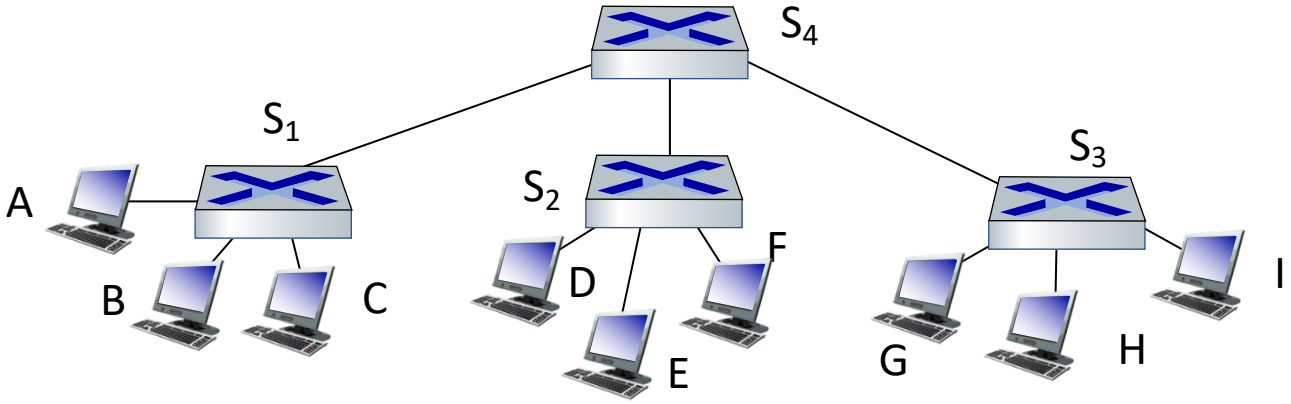


Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

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

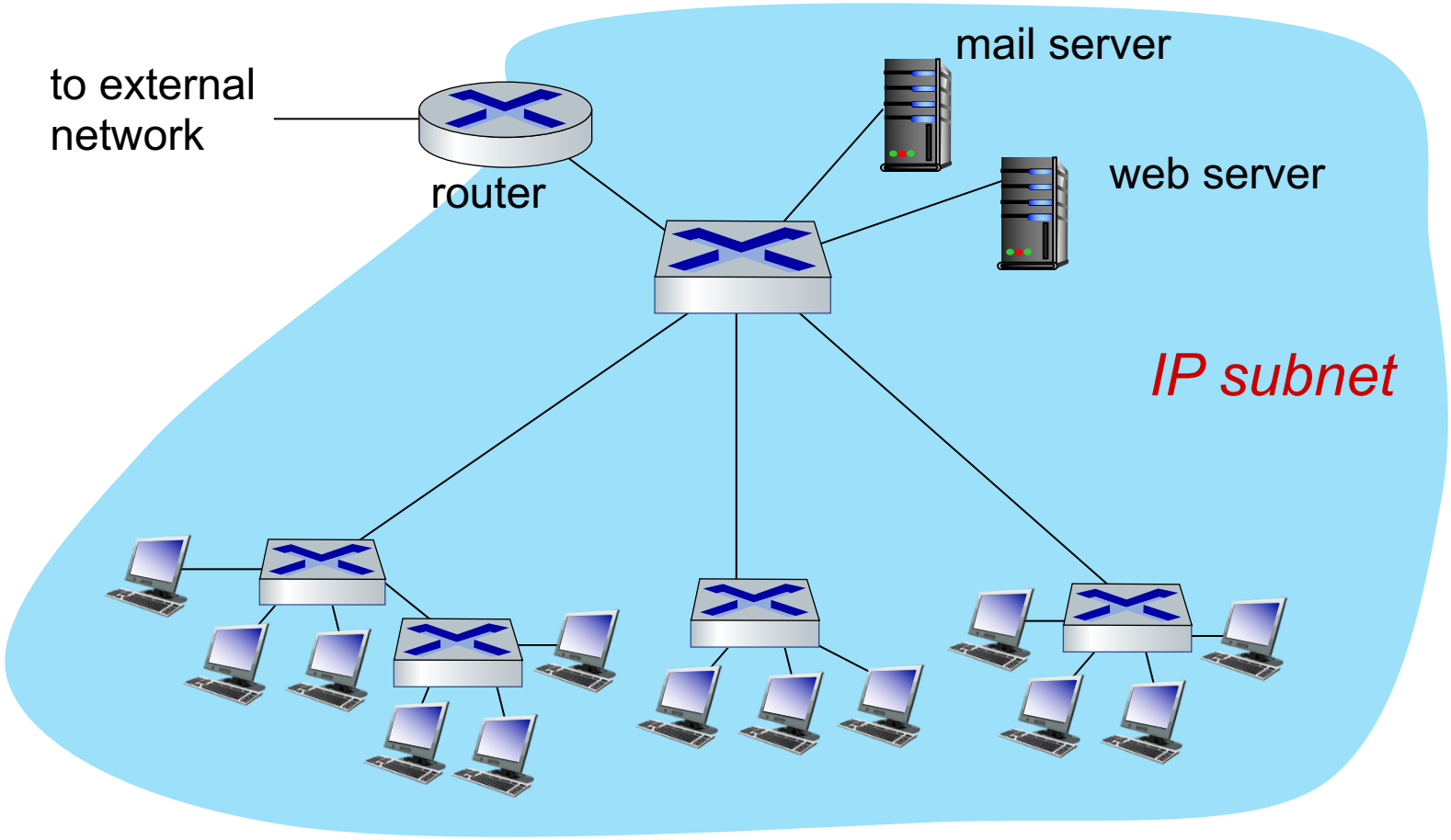
Self-learning Multi-switch Example

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

Small Institutional Network



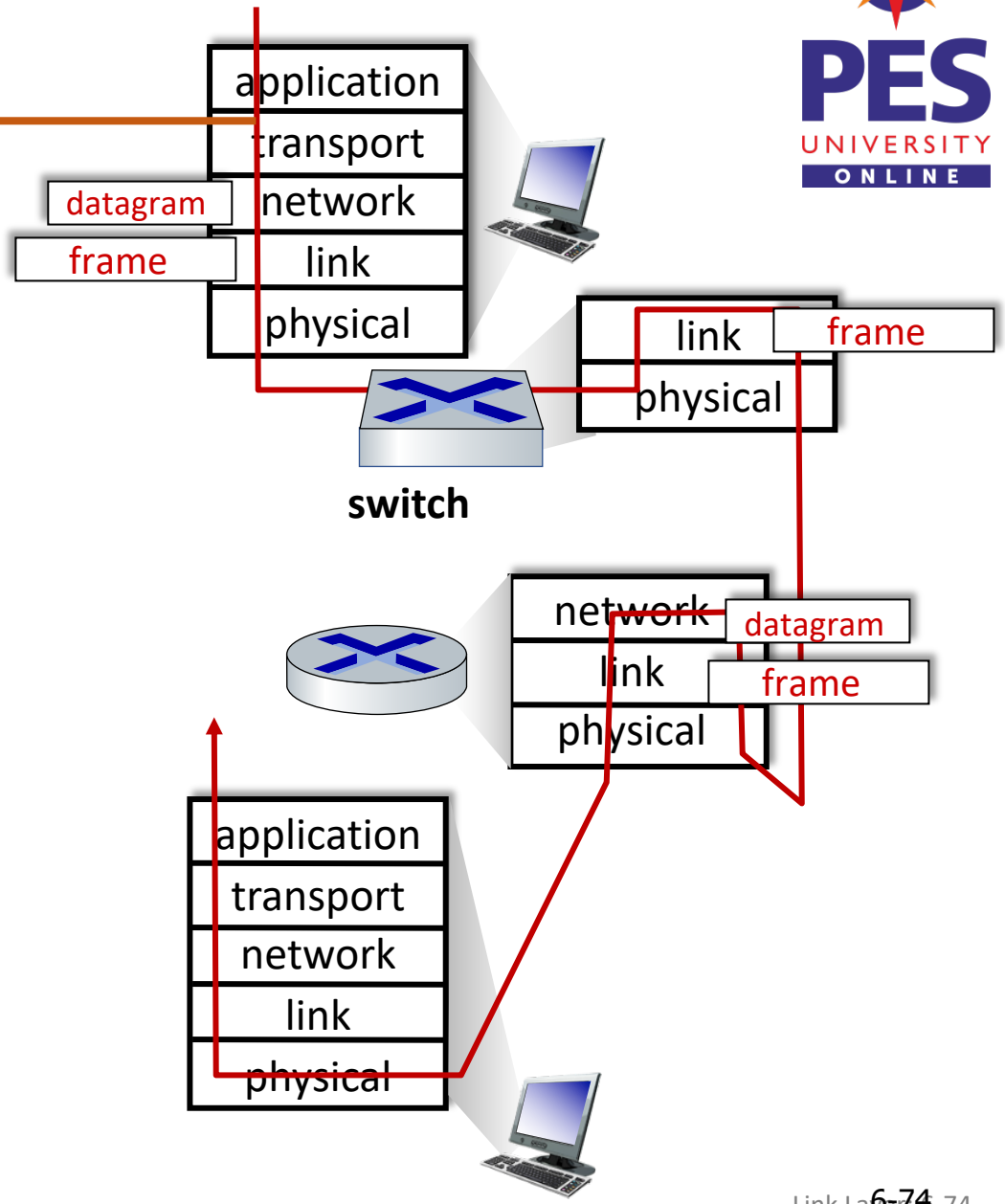
Switches Vs Routers

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



THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request
- Physical layer
- Wireless LANs: IEEE 802.11

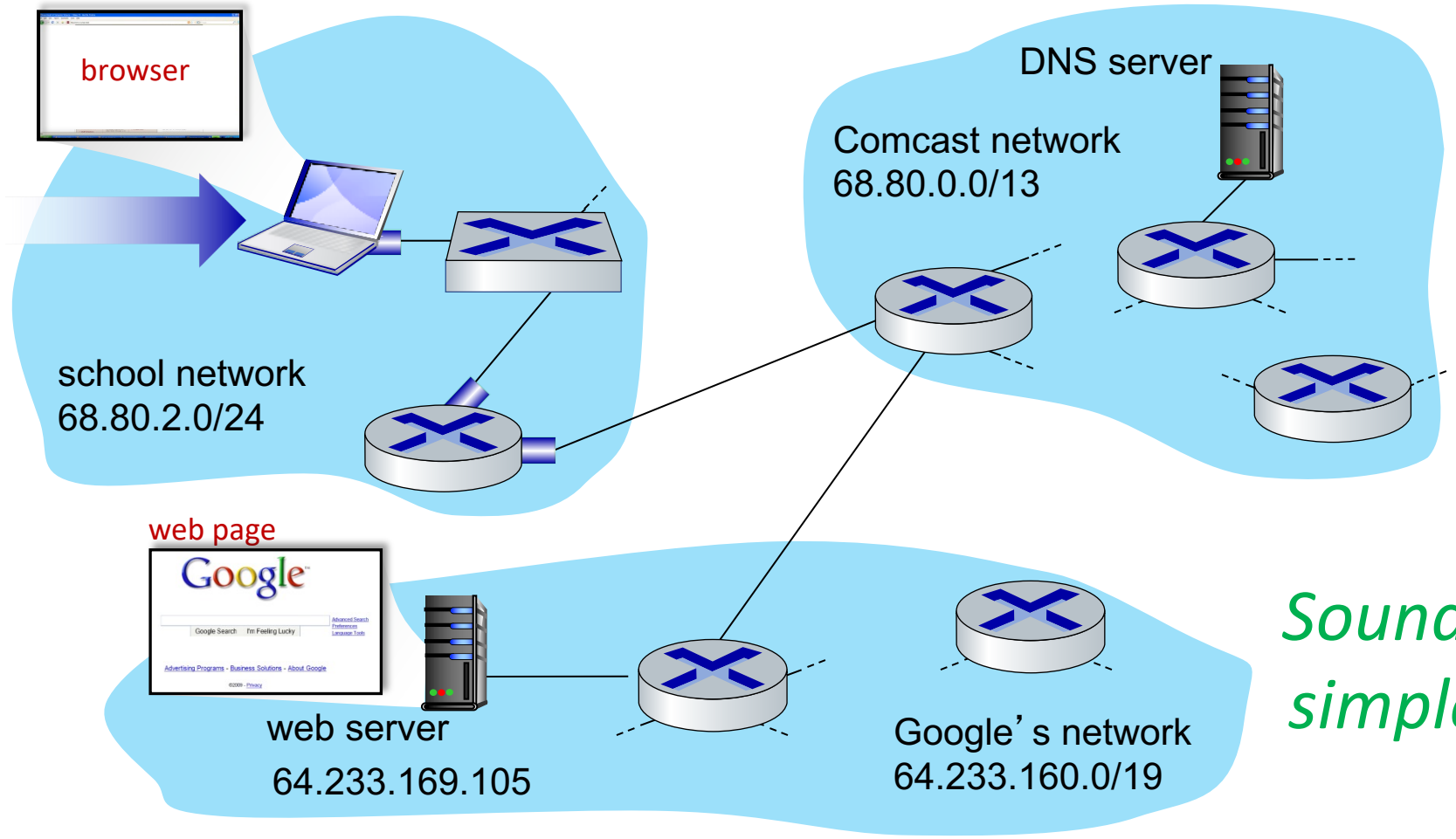
Class 52 : A day in the life of a web request : Learning Objectives

- Synthesis of web request..

Synthesis : A day in the life of a web request

- Our journey down the protocol stack is now complete!
  - application, transport, network, link
- Putting-it-all-together: synthesis!
  - *Goal:* identify, review, understand protocols (at all layers) involved in seemingly simple scenario: requesting www page
  - *Scenario:* student attaches laptop to campus network, requests/receives www.google.com

A day in the life of a web request

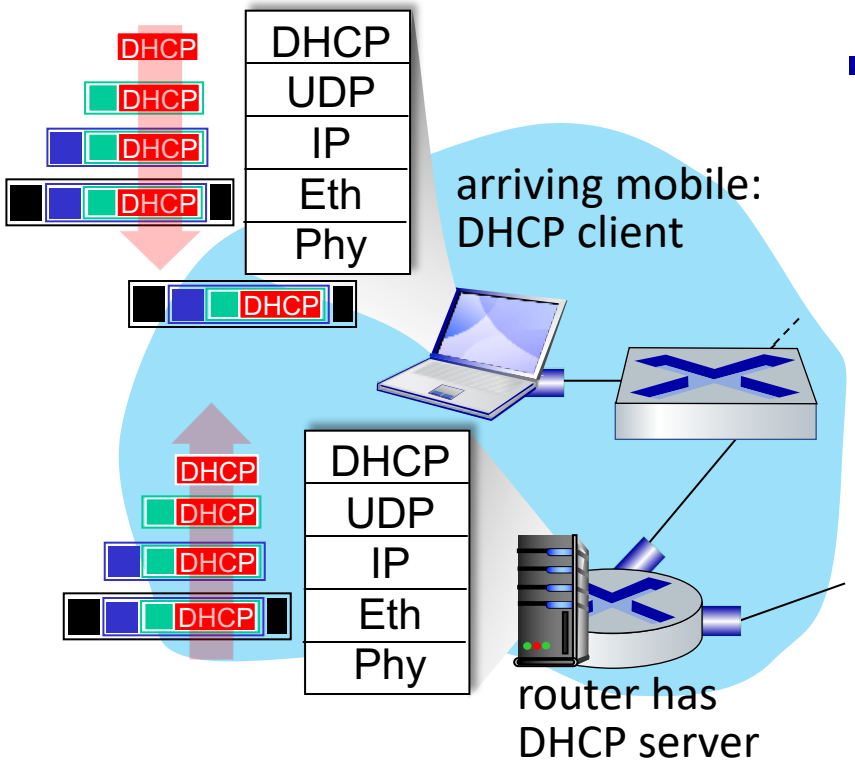


Scenario:

- Arriving mobile client attaches to network …
- Requests web page: www.google.com

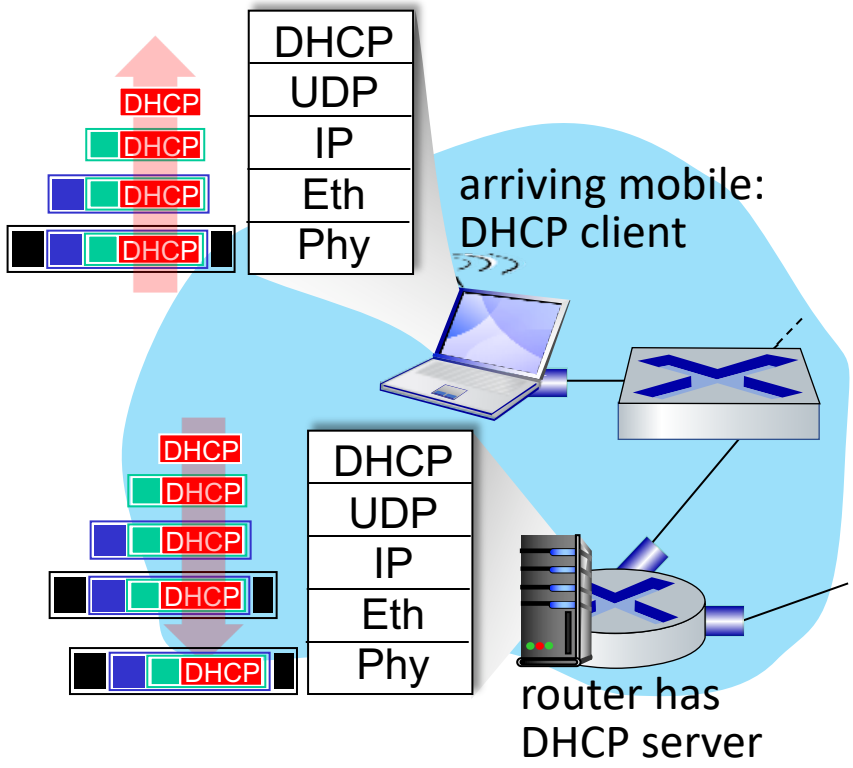
Sounds simple!

A day in the life of a web request



- Connecting laptop needs to get its own IP address, addr of first-hop router, addr of DNS server: use DHCP
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.3 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

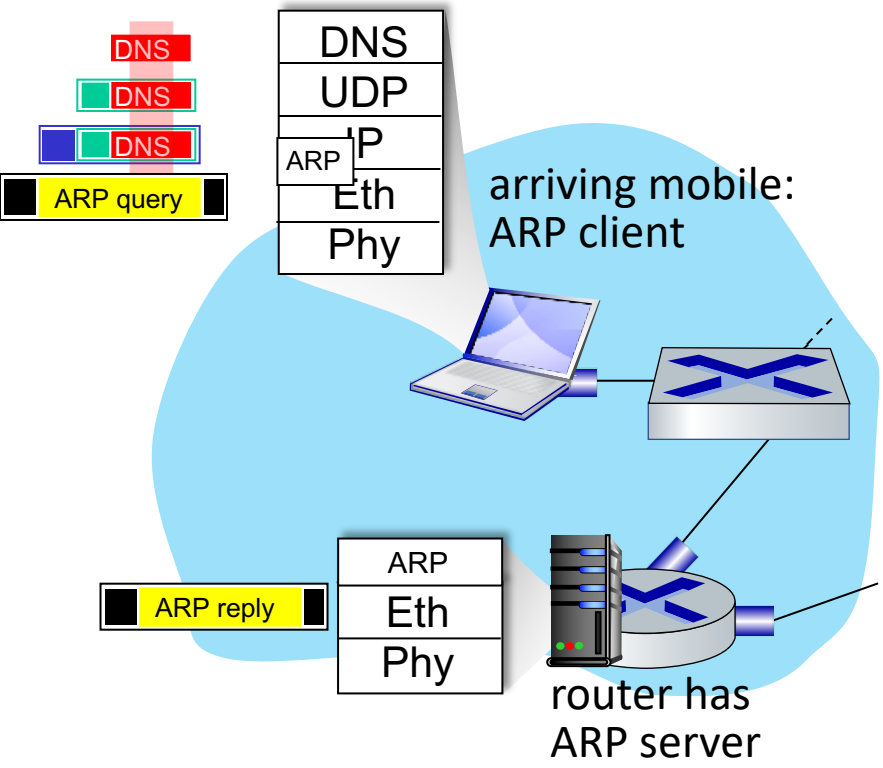
A day in the life : Connecting to the Internet



- DHCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- Encapsulation at DHCP server, frame forwarded (switch learning) through LAN, demultiplexing at client
- DHCP client receives DHCP ACK reply

Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

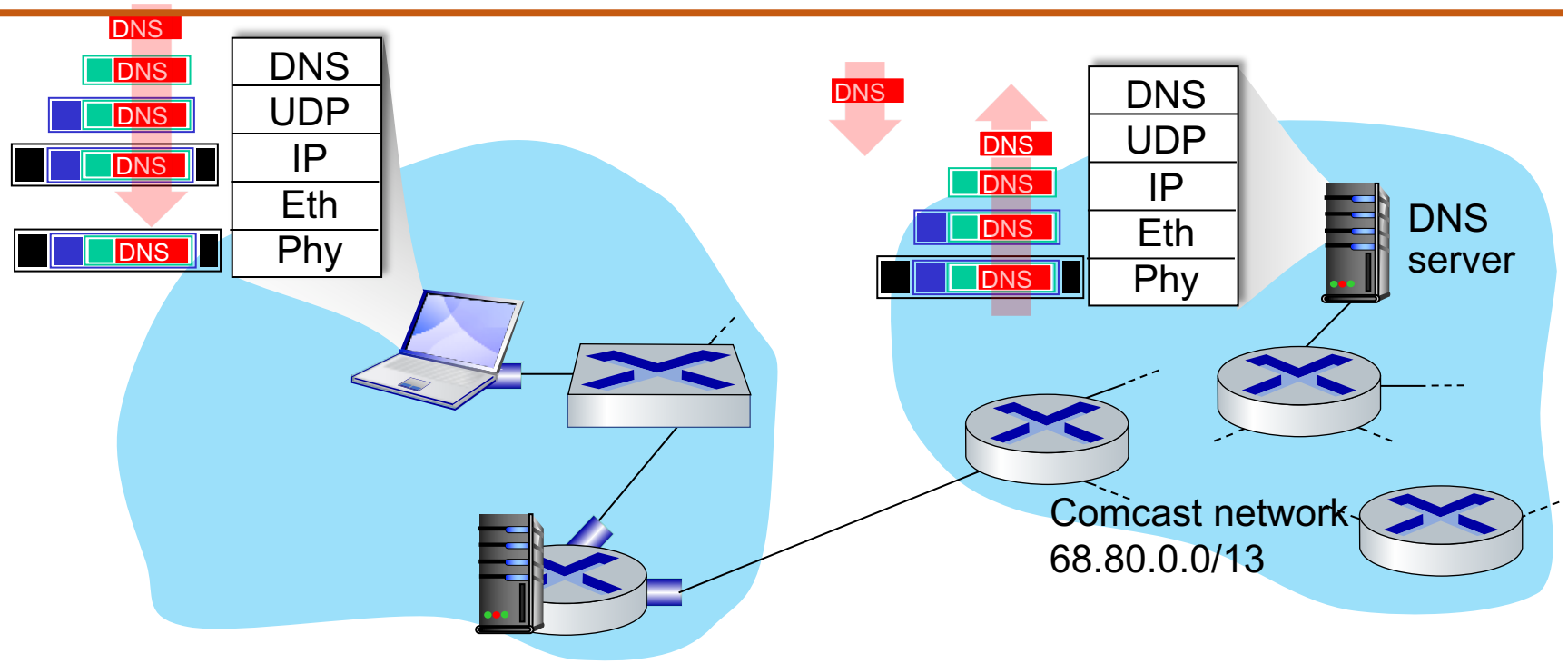
A day in the life…. ARP (Before DNS, Before HTTP)



- Before sending HTTP request, need IP address of www.google.com: DNS
- DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: ARP
- ARP query broadcast, received by router, which replies with ARP reply giving MAC address of router interface

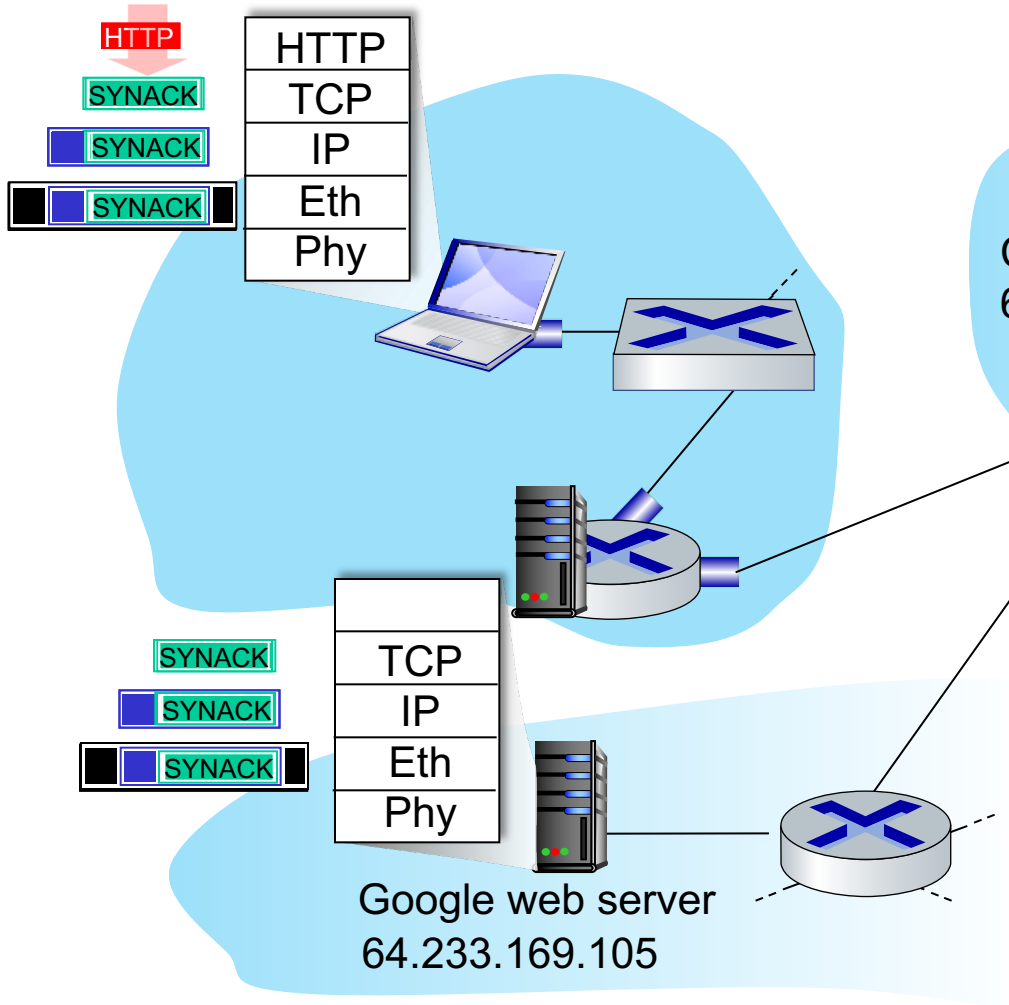
- Client now knows MAC address of first hop router, so can now send frame containing DNS query

A day in the life…. Using DNS



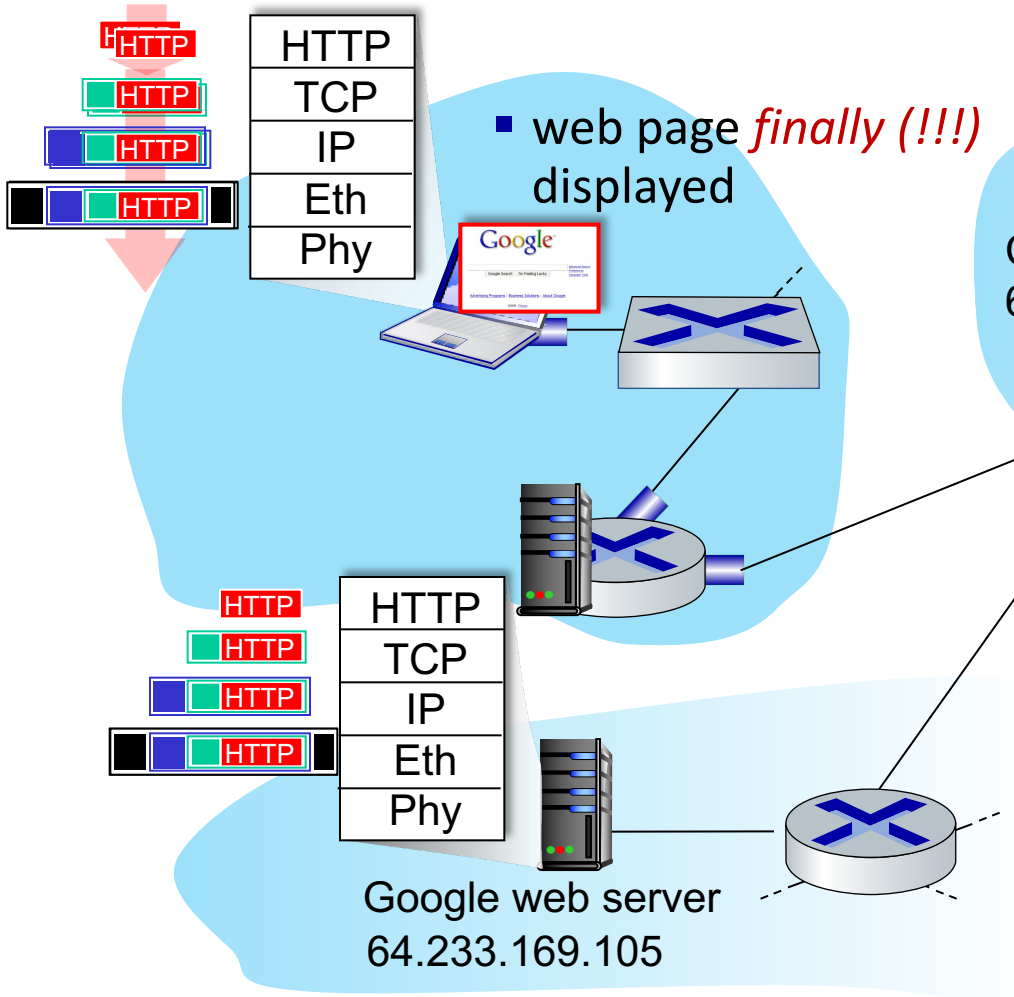
- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router
- IP datagram forwarded from campus network into Comcast network, routed (tables created by RIP, OSPF, IS-IS and/or BGP routing protocols) to DNS server
- Demuxed to DNS
- DNS replies to client with IP address of www.google.com

A day in the life…. TCP Connection carrying HTTP



- To send HTTP request, client first opens TCP socket to web server
- TCP SYN segment (step 1 in TCP 3-way handshake) inter-domain routed to web server
- Web server responds with TCP SYNACK (step 2 in TCP 3-way handshake)
- TCP connection established!

A day in the life…. HTTP Request / Reply



- HTTP request sent into TCP socket
- IP datagram containing HTTP request routed to www.google.com
- Web server responds with HTTP reply (containing web page)
- IP datagram containing HTTP reply routed back to client

THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request

- Physical layer
  - Purpose, Signals to Packets
  - Analog Vs Digital Signals
  - Transmission Media
- Wireless LANs: IEEE 802.11

COMPUTER NETWORKS

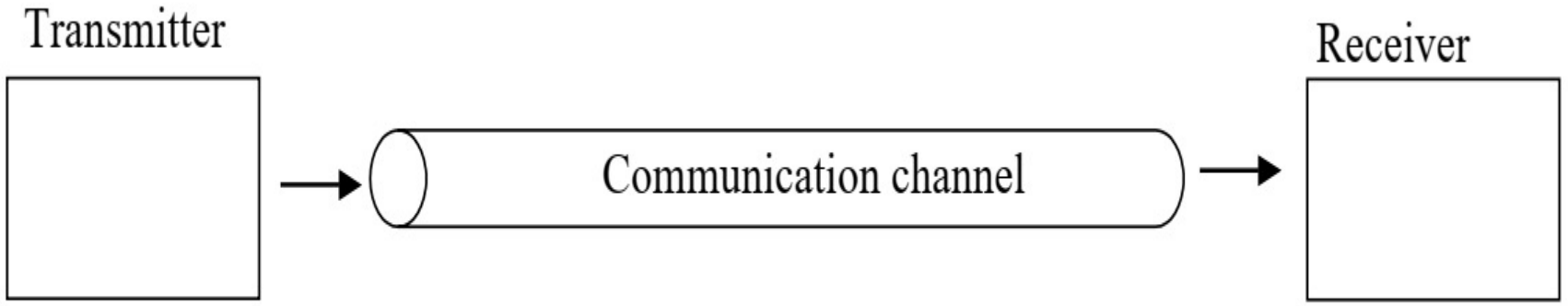
Class 53 : Intro to Physical layer : Learning Objectives

- Purpose
- Signals to Packets

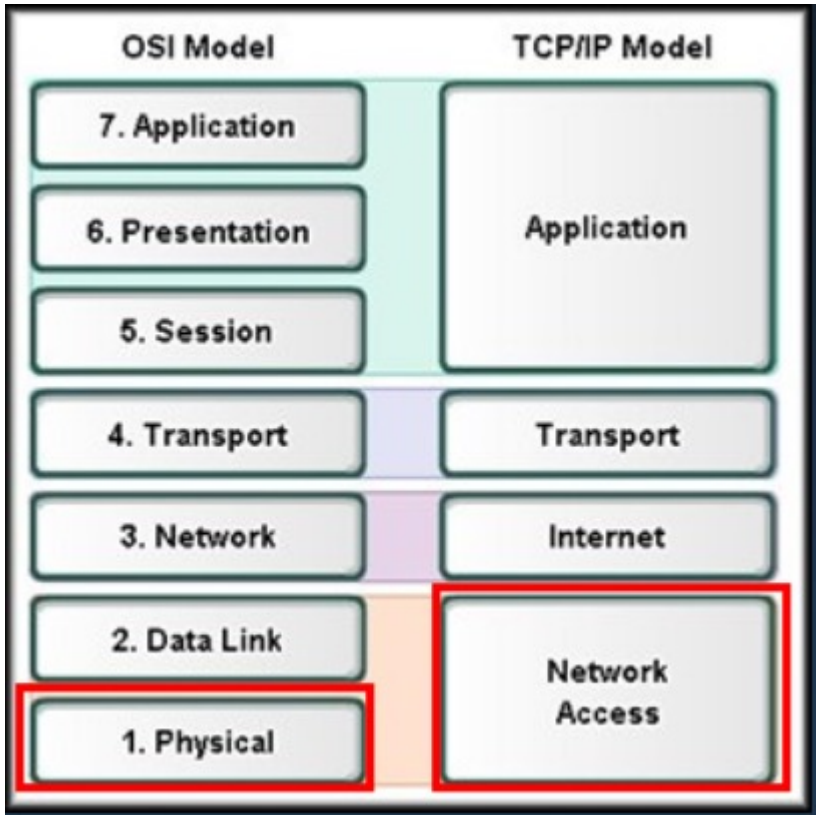
Physical layer

The Physical layer consists of hardware, in the form of

- electronic circuitry,
- media, and
- connectors.



Physical Layer



Purpose:

- *Primary Purpose:*
  - *Representation of the bits of a frame on the media in the form of signals*
- The physical media and associated connectors
- Encoding of data and control information
- Transmitter and receiver circuitry on the network devices

Each medium has a unique method of representing bits (signaling):

Physical Layer

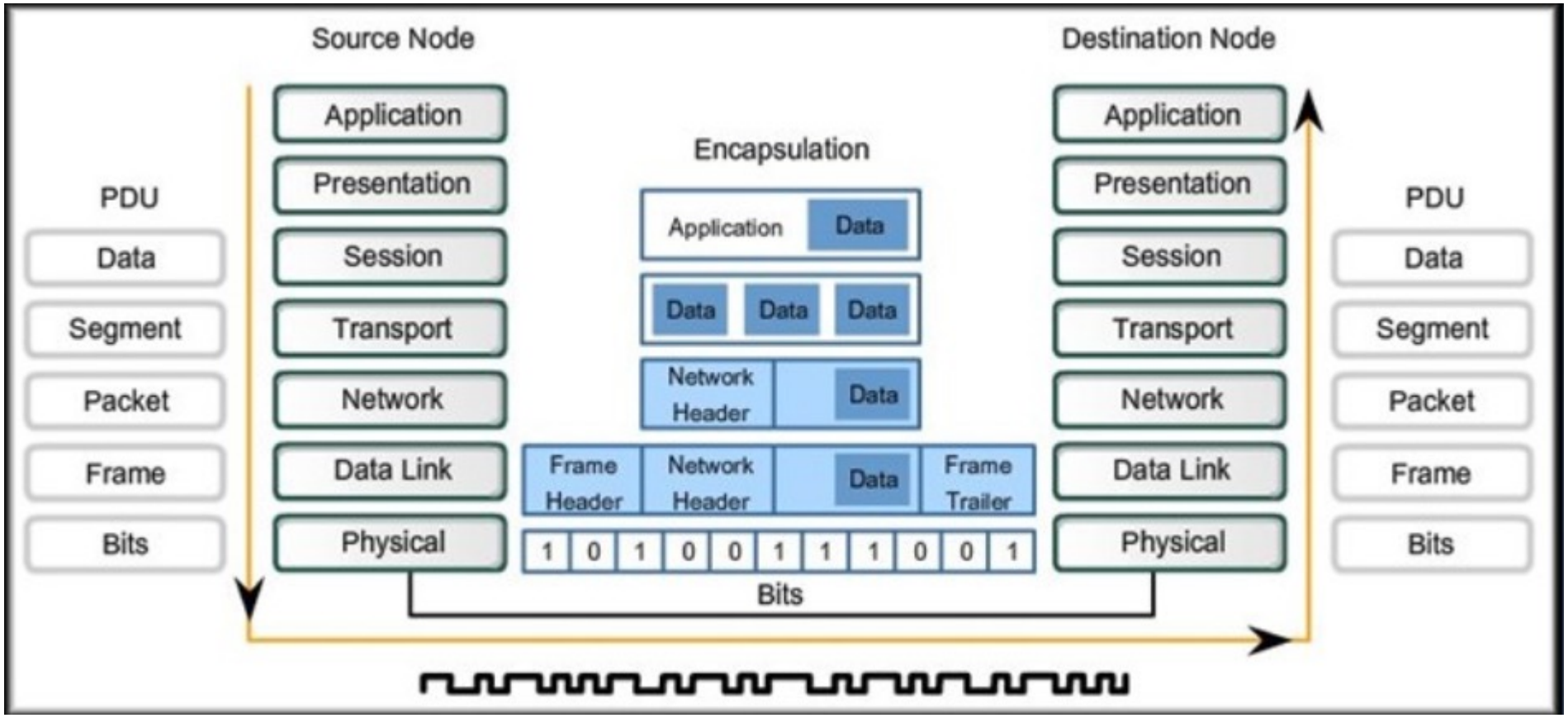
Hardware components such as

- network adapters (NICs),
- interfaces and connectors,
- cable materials
- cable designs

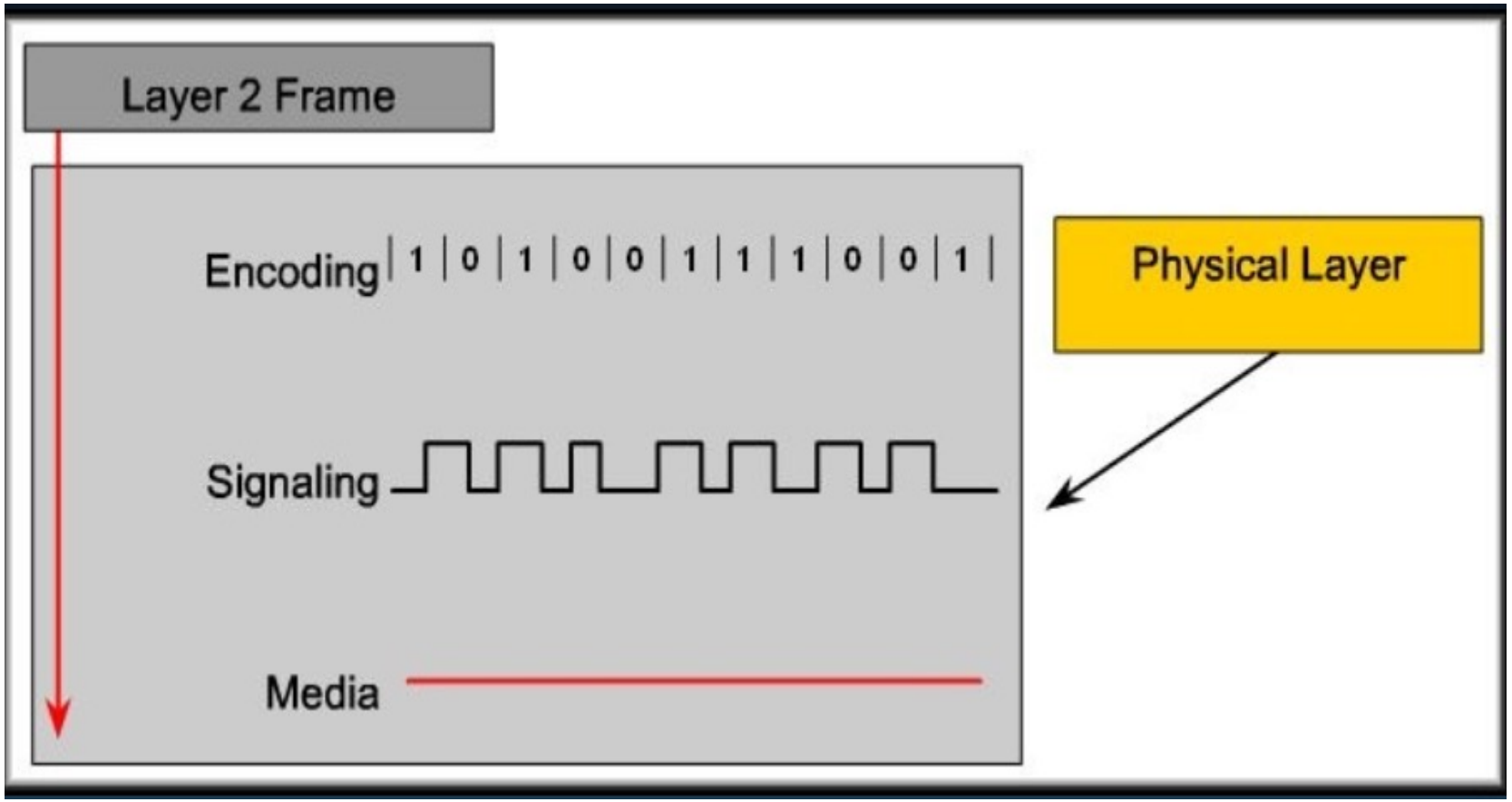
Determine

- Physical and electrical properties of the media
- Mechanical properties (materials, dimensions, pinouts) of the connectors
- Bit representation by the signals (encoding)
- Definition of control information signals

Physical Layer



Physical layer Fundamental Principles



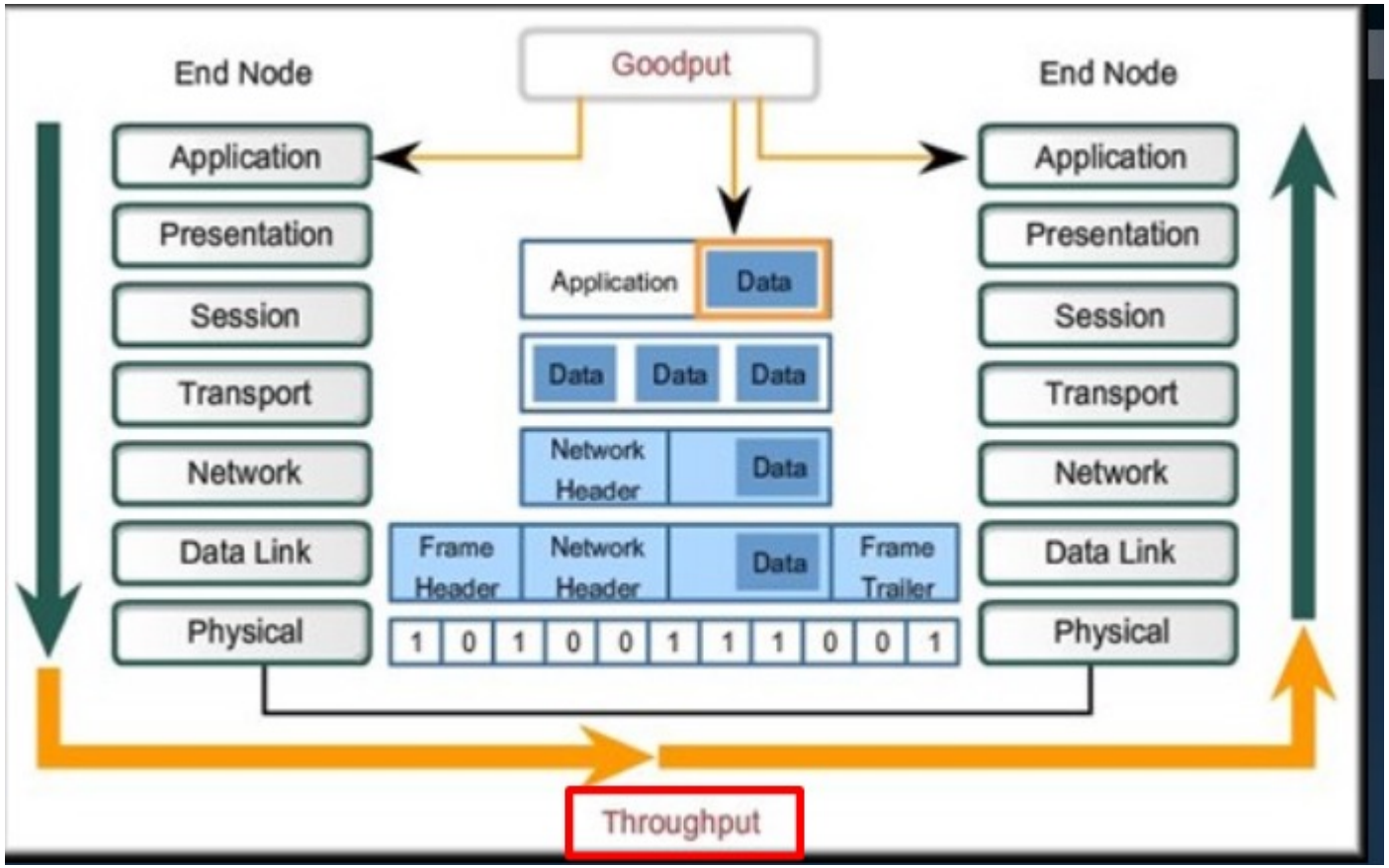
- The physical components
- Data encoding
- Signaling

Physical Signaling and Encoding : Representing Bits

Signaling Bits for the Media

- *All communication from the human network becomes binary digits, which are transported across the physical media*
  - Transmission occurs as a stream of bits sent one at a time
  - Each of the bits in the frame represented as a signal
  - Each signal has a specific amount of time to occupy the media
    - This is referred to as its bit time

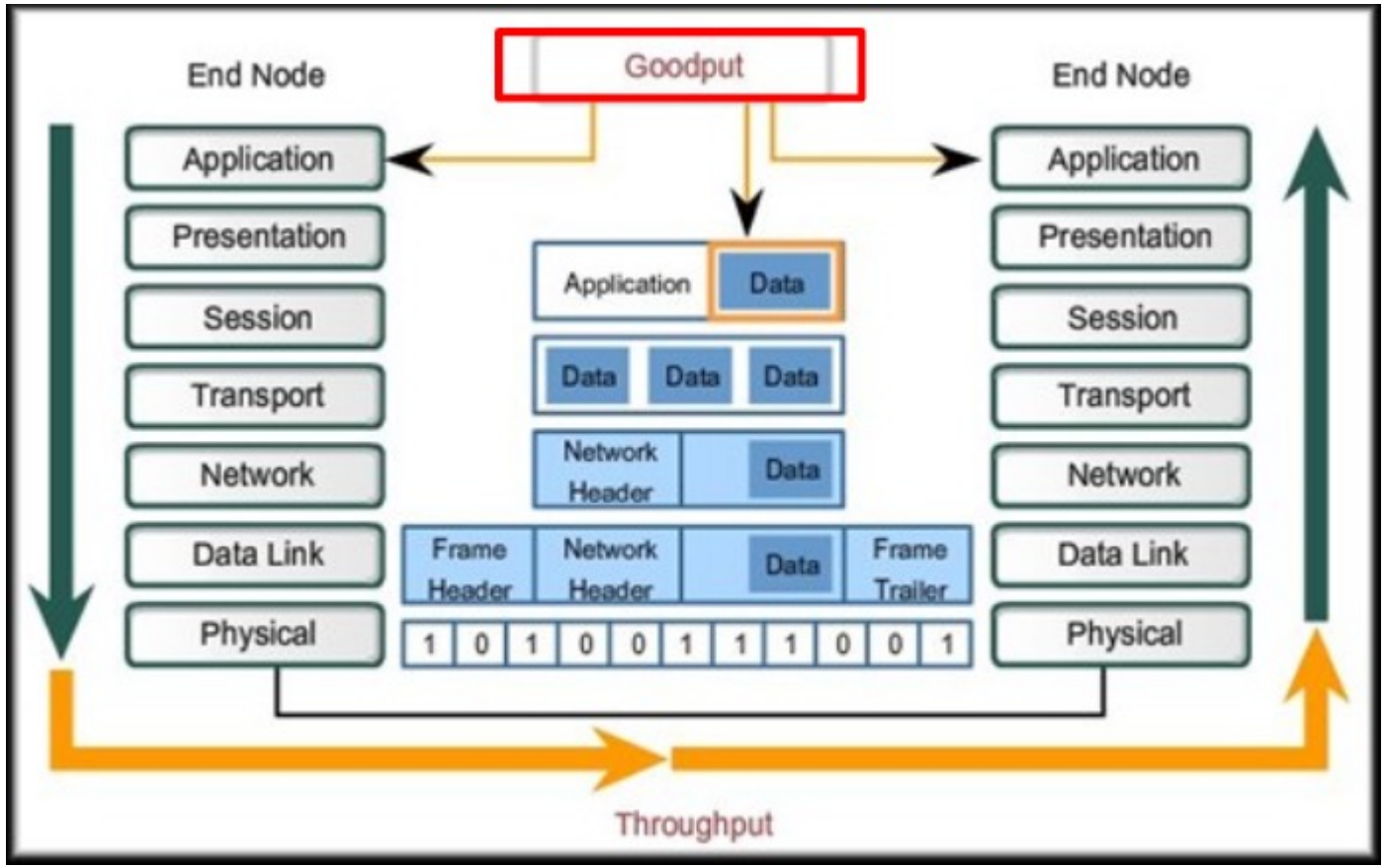
Data Carrying Capacity



Bandwidth(Theoretical)

- The capacity of a medium to carry data in a given amount of time
- Takes into account the physical properties of the medium and the signaling method

Data Carrying Capacity



Throughput(Practical):

- Transfer rate of data over the medium
- Factors that affect: Amount and type of traffic, number of devices

Goodput(Qualitative):

- Transfer rate of actual usable data bits
- Throughput less the data protocol overhead, error corrections and retransmissions

THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request

- Physical layer
  - Purpose, Signals to Packets
  - Analog Vs Digital Signals
  - Transmission Media
- Wireless LANs: IEEE 802.11

COMPUTER NETWORKS

Class 54 : Physical layer : Learning Objectives

- Analog Vs Digital Signals
- Transmission Media

Analog Vs Digital Signals

- If data is to be transmitted, then it must be transformed to electromagnetic signals.
  - Analog signals - infinite number of values in a range;
  - Digital signals can have only a limited number of values.
- Data can be analog or digital.
  - Analog data - information that is continuous;
    - Analog data example: voice temperature captured by analog sensor
  - Digital data - information that has discrete states.

Transmission Media

- Transmission medium-the physical path between transmitter and receiver.
- Repeaters or amplifiers may be used to extend the length of the medium.
- Communication of electromagnetic waves is *guided* or *unguided.*
  - *Guided media* : waves are guided along a physical path (e.g, twisted pair, coaxial cable and optical fiber).
  - *Unguided media*: means for transmitting but not guiding electromagnetic waves (e.g., the atmosphere and outer space).

Types of Physical Transmission Media

- Twisted pair
- Coaxial cable
- Optical fiber
- Wireless communications

Types of Physical Transmission Media

Specification	Media	Maximum Segment Length	Connector
10BASE-T	CAT 3,4 or 5 UTP (4 pair)	100m	RJ-45
100BASE-TX	CAT 5 UTP (2 pair)	100m	RJ-45
100BASE-FX	62.5/125 multimode fiber	2km	
1000BASE-CX	STP	25m	RJ-45
1000BASE-T	CAT 5 UTP (4 pair)	100m	RJ-45
1000BASE-SX	62.5/50 multimode fiber	62.5 – 275m 50 – 550m	
1000BASE-LX	62.5/50 multimode 9-micron single-mode fiber	62.5/50 – 550m 9 –10 km	
1000BASE-ZX	9-micron single-mode fiber	70km	
10GBASE-ZR	9-micron single-mode fiber	80km	

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

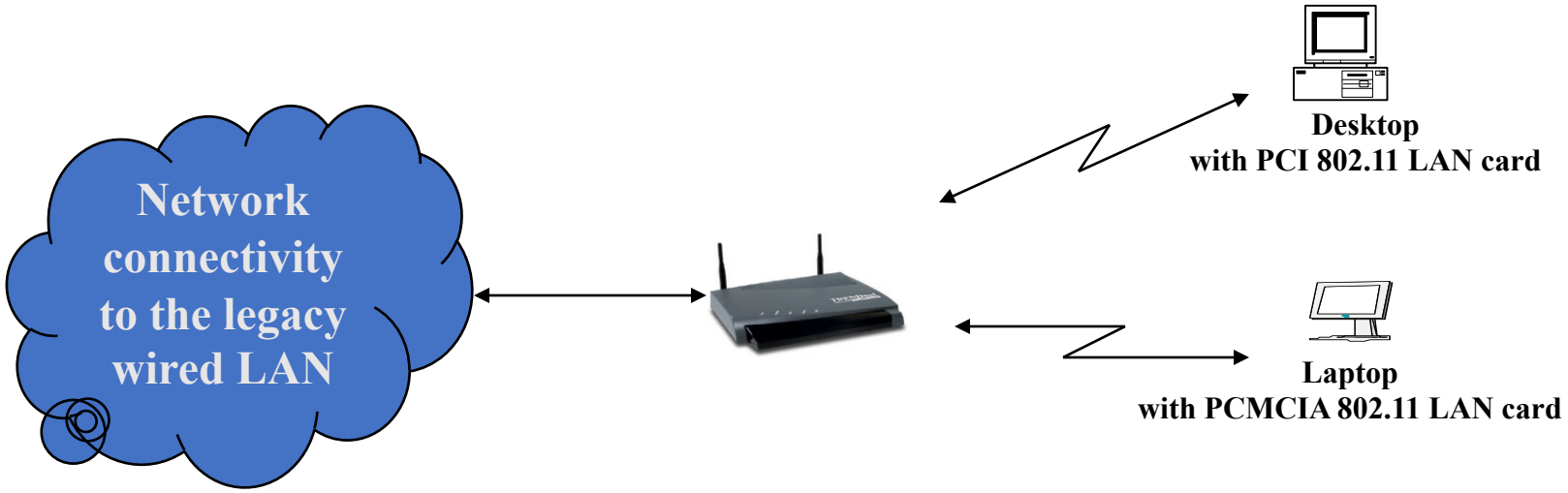
Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request
- Physical layer
  - Purpose, Signals to Packets
  - Analog Vs Digital Signals
  - Transmission Media
- Wireless LANs: IEEE 802.11

Class 55 : IEEE 802.11- Wireless LAN : Learning Objectives

- Why, What- Wireless LAN
- 802.11 Architecture

Wireless LAN



- Provides network connectivity over wireless media
- An Access Point (AP) is installed to act as Bridge between Wireless and Wired Network
- The AP is connected to wired network and is equipped with antennae to provide wireless connectivity

Wireless LAN

- Range (Distance between Access Point and WLAN client) depends on
  - structural hindrances and
  - RF gain of the antenna at the Access Point
- To service larger areas, multiple APs may be installed with a 20-30% overlap
- A client is always associated with one AP and when the client moves closer to another AP, it associates with the new AP (Hand-Off)

IEEE 802.11- Wireless LAN

IEEE 802.11 defines

- MAC protocol and
- Physical medium specification

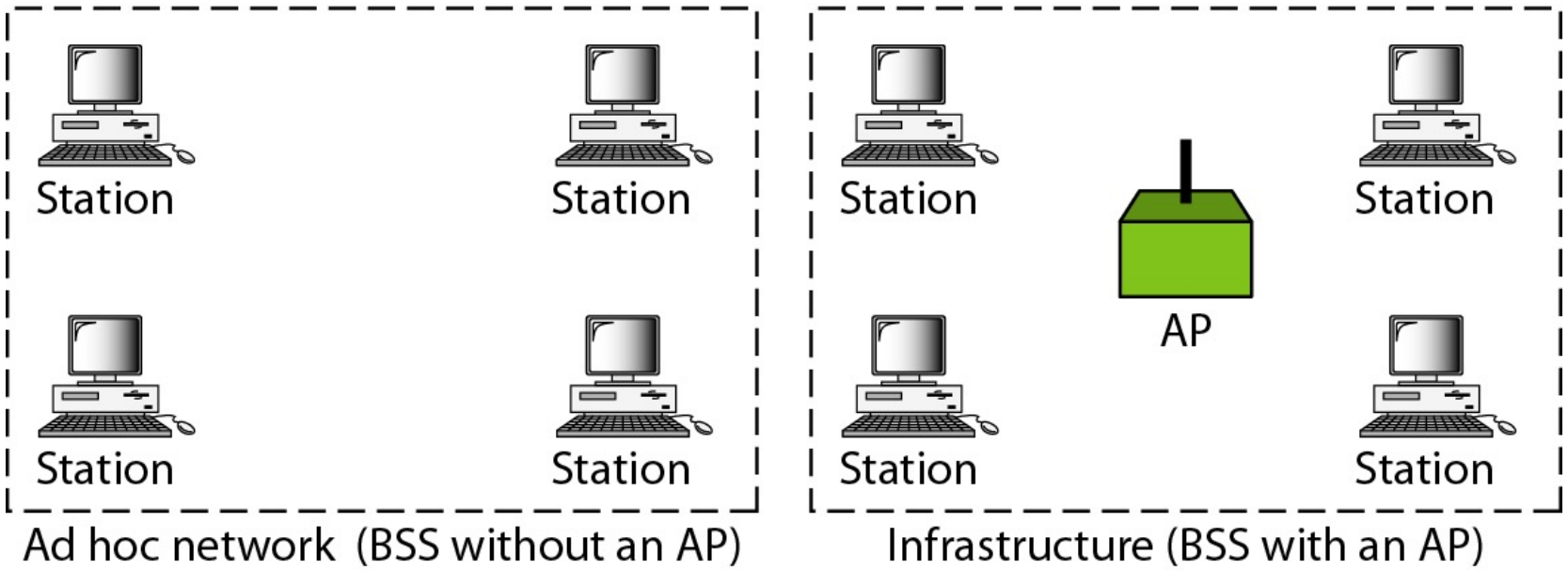
for wireless LANs

IEEE 802.11- Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution System (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

Basic Service Set

BSS: Basic service set
AP: Access point



May be isolated or connect to backbone distribution system (DS) through access point (AP)

- AP functions as bridge

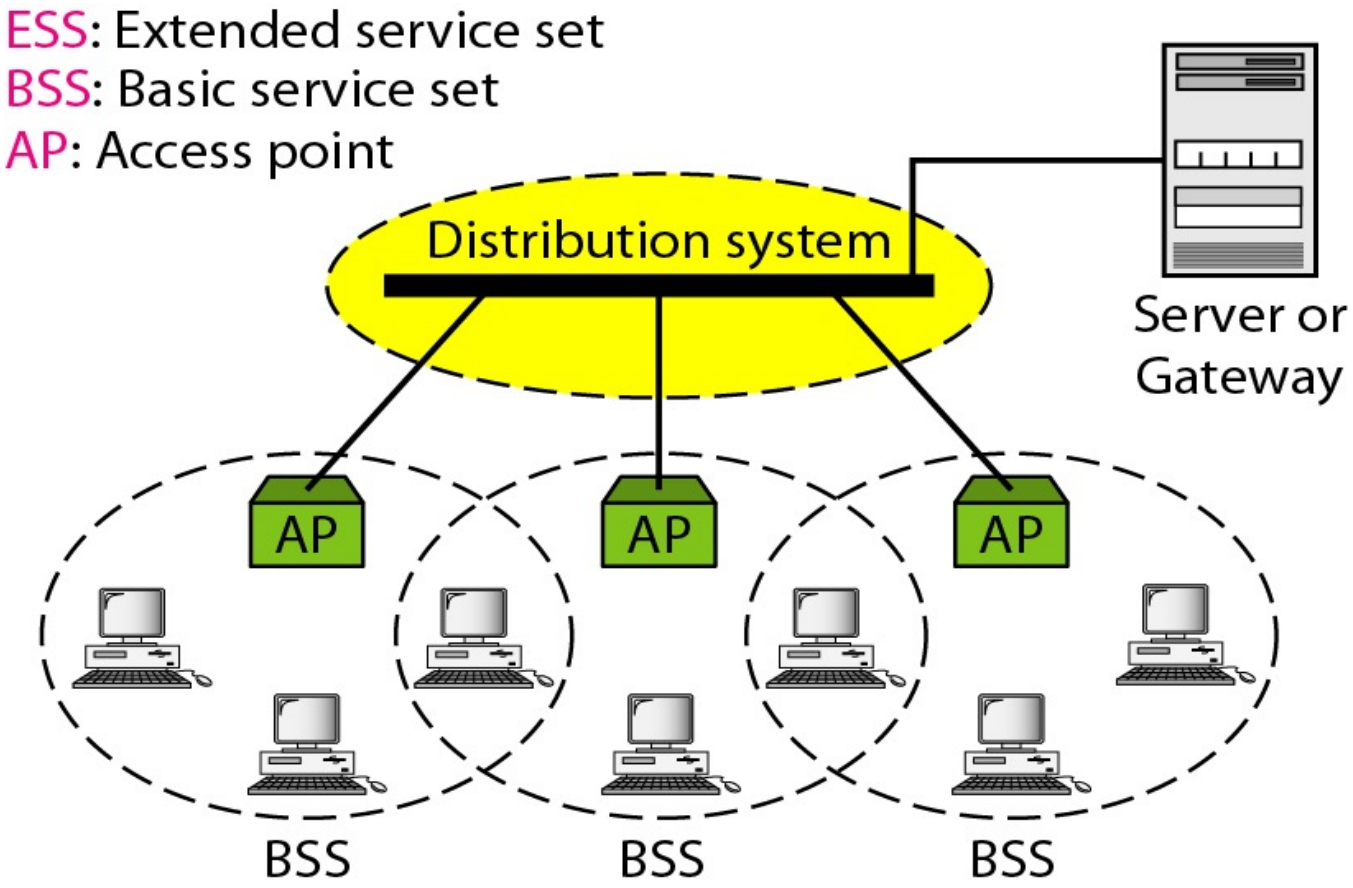
BSS- Smallest building block

- Number of stations
- Same MAC protocol
- Competing for access to same shared wireless medium

IEEE 802.11

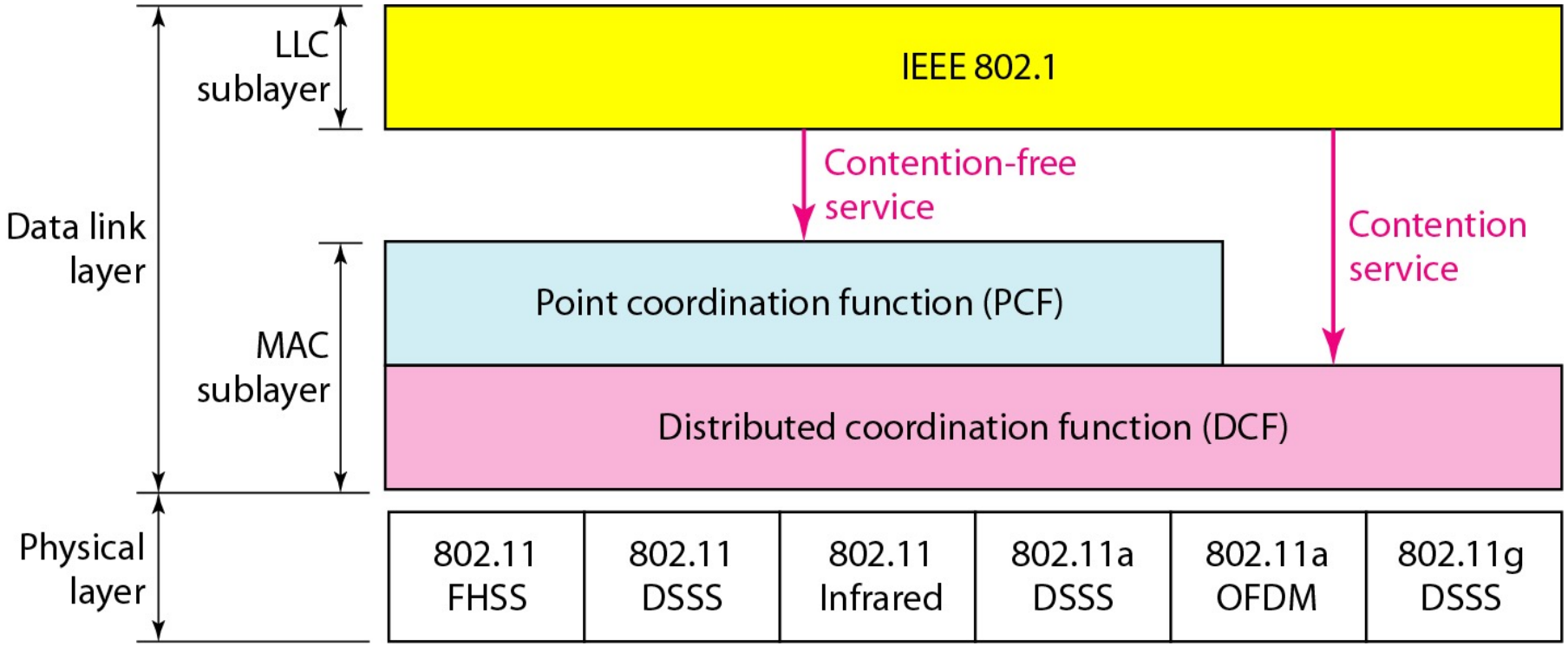
- MAC protocol may be distributed or controlled by central coordination function in AP
- BSS generally corresponds to cell
- Distributed System can be switch, wired network, or wireless network

Extended Service Set



An Access Point (AP) broadcasts is SSID (service set identifier) roughly every 100 ms and at 1 Mbps (to accommodate the slowest client)

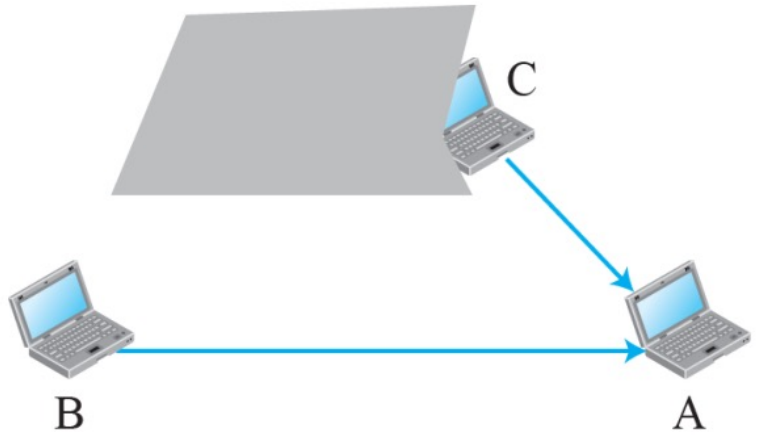
IEEE 802.11 Architecture



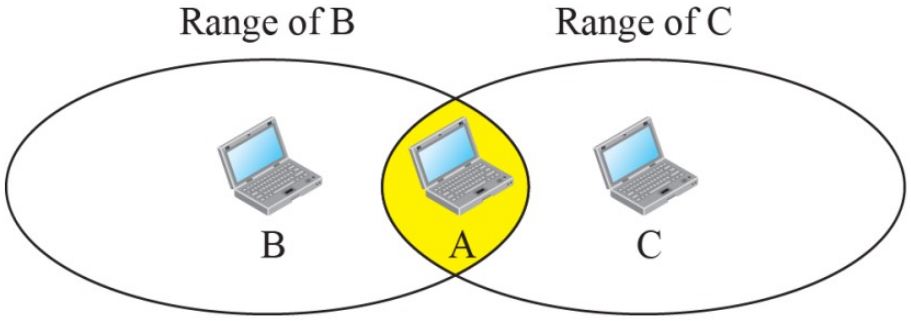
FHSS - frequency hopping spread spectrum
DSSS - direct sequence spread spectrum
OFDM - orthogonal frequency division multiplexing

Access Control

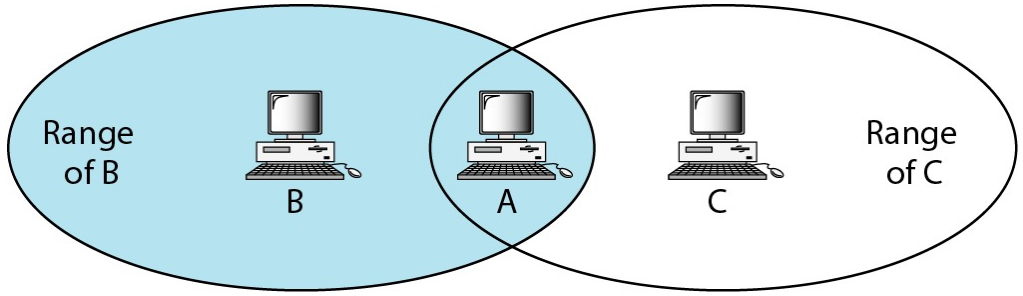
- How a wireless host can get access to the shared medium (air)?
- The CSMA/CD algorithm does not work in wireless LANs for such reasons:
  - Send and receiving signal power
  - The hidden station problem prevents collision detection



b. Stations B and C are hidden from each other.

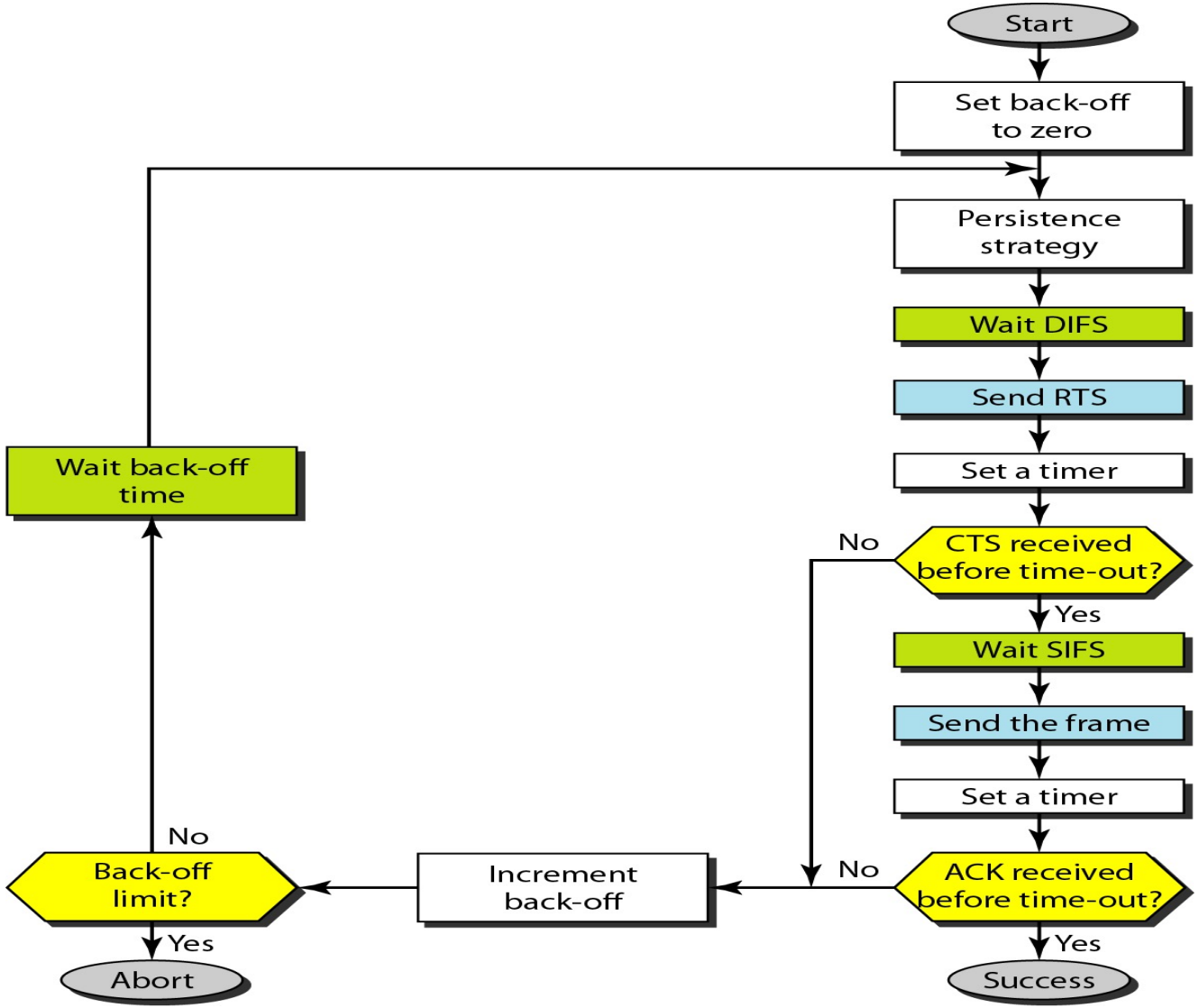


a. Stations B and C are not in each other's range.



B and C are hidden from each other with respect to A.

CSMA/CA

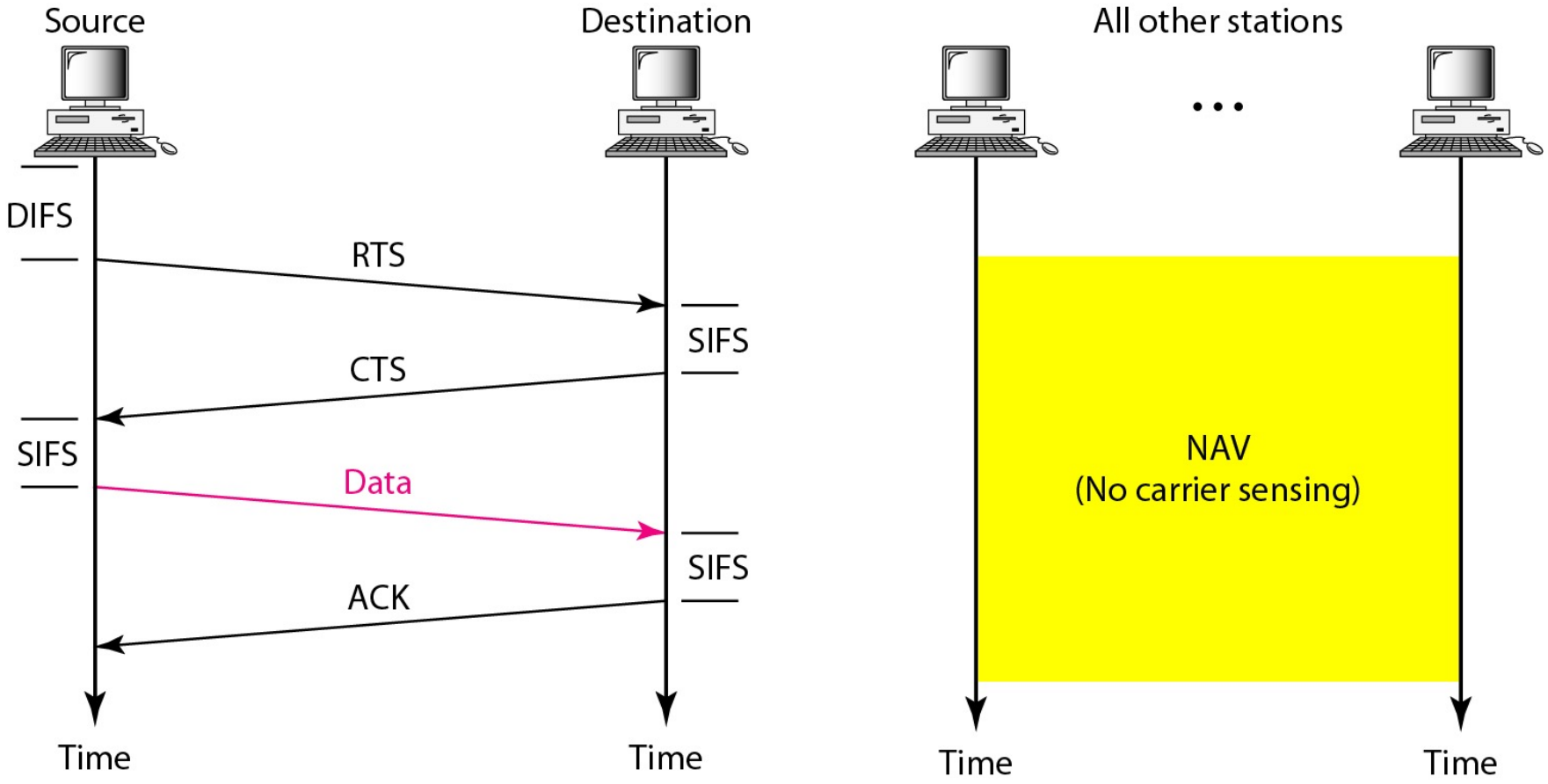


DIFS: distributed interframe space

SIFS: short interframe space

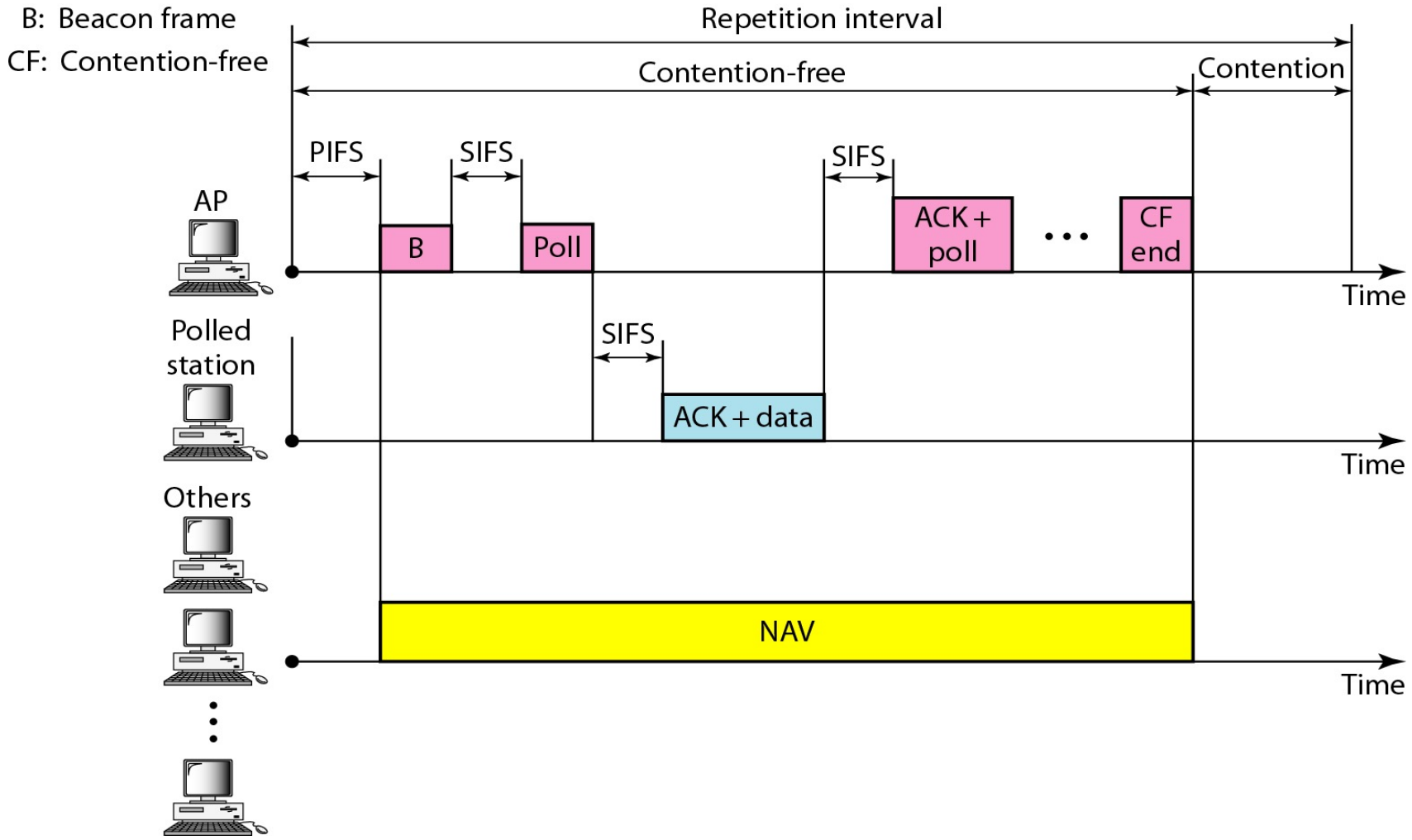
CSMA/CA

The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.



When a station sends its RTS, it includes a time of how long it needs the medium. Other stations then set their NAV timer to this time so they don't transmit.
DIFS: Distributed interframe space; SIFS: short interframe space

Example of Repetition Interval



THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu

COMPUTER NETWORKS

Ashwini M Joshi

Department of Computer Science and Engineering

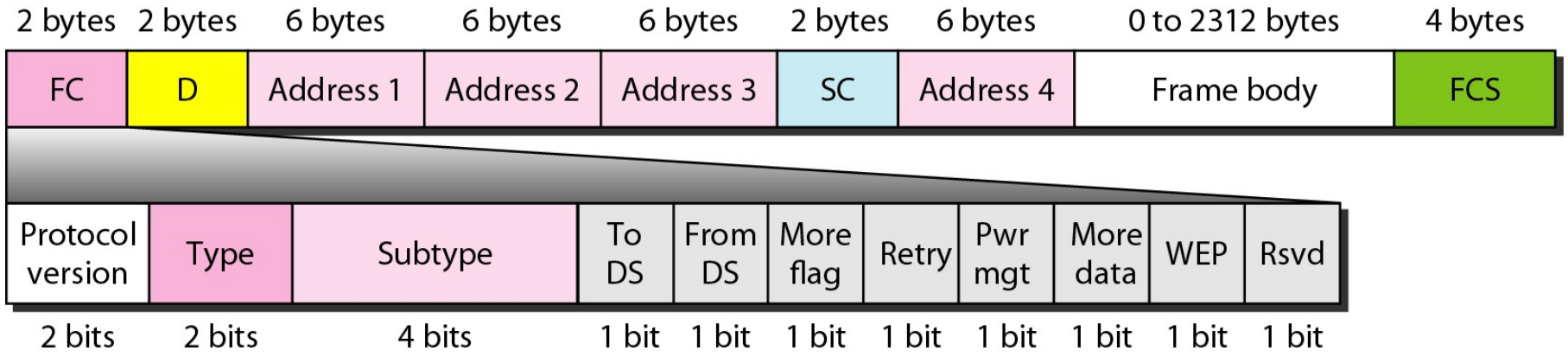
Unit – 5 Link Layer and LAN Roadmap

- Introduction
- Error detection, correction
- Multiple access protocols
- LANs
  - Addressing, ARP
  - Ethernet
  - Switches
- A day in the life of a web request
- Physical layer
  - Purpose, Signals to Packets
  - Analog Vs Digital Signals
  - Transmission Media
- Wireless LANs: IEEE 802.11

Class 56 : IEEE 802.11- Wireless LAN : Learning Objectives

- Frame Format
- Addressing Mechanism

Frame Format

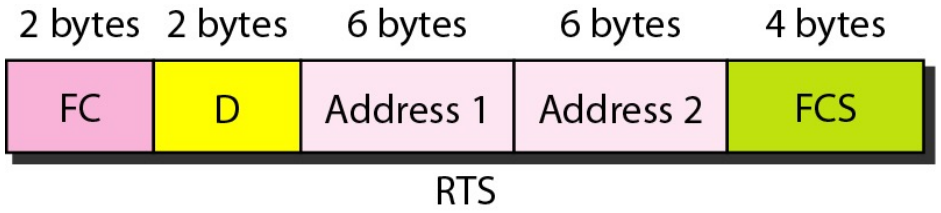


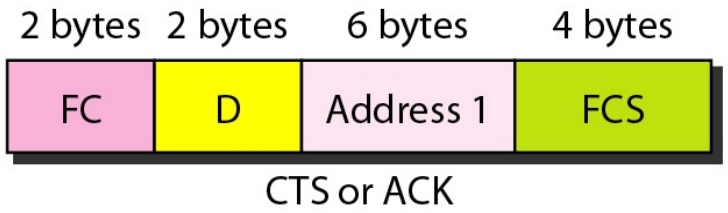
FC: Frame Control
D: duration of the transmission that is used to set the value of NAV
SC: sequence control: defines the sequence number of the frame to be used in flow control

Sub fields in FC field

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

Control Frames





FC: Frame Control
D: duration of the transmission that is used to set the value of NAV

Frames Types

1. Management - used for initial communication between stations and access points

2. Control - used for accessing the channel (RTS) and acknowledging frames (CTS or ACK)

3. Data - used for carrying data and control information

Values of subfields in control frames

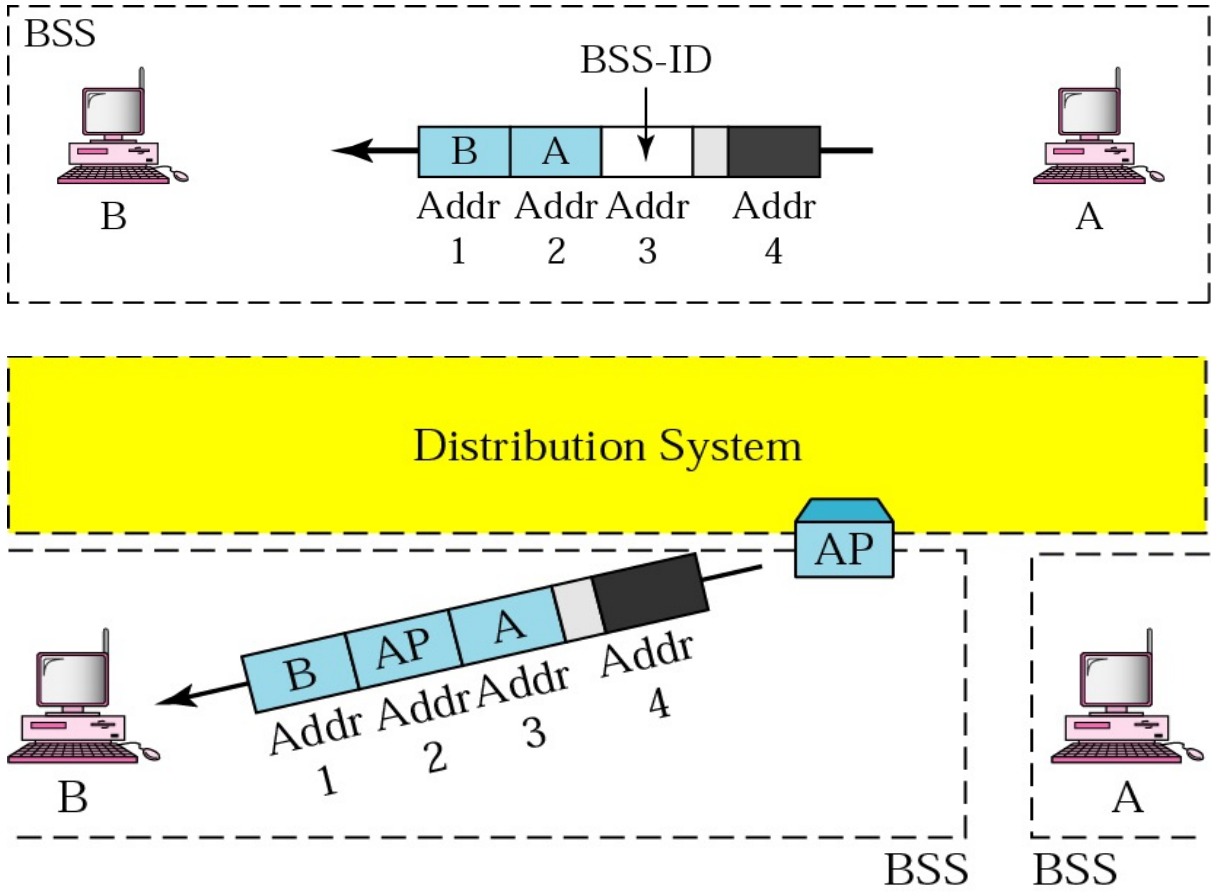
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Addresses

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Note:
Address 1 is always address of next device
Address 2 is always address of previous device
Address 3 is address of final destination if not defined by Address 1
Address 4 is address of original source if not defined by Address 2

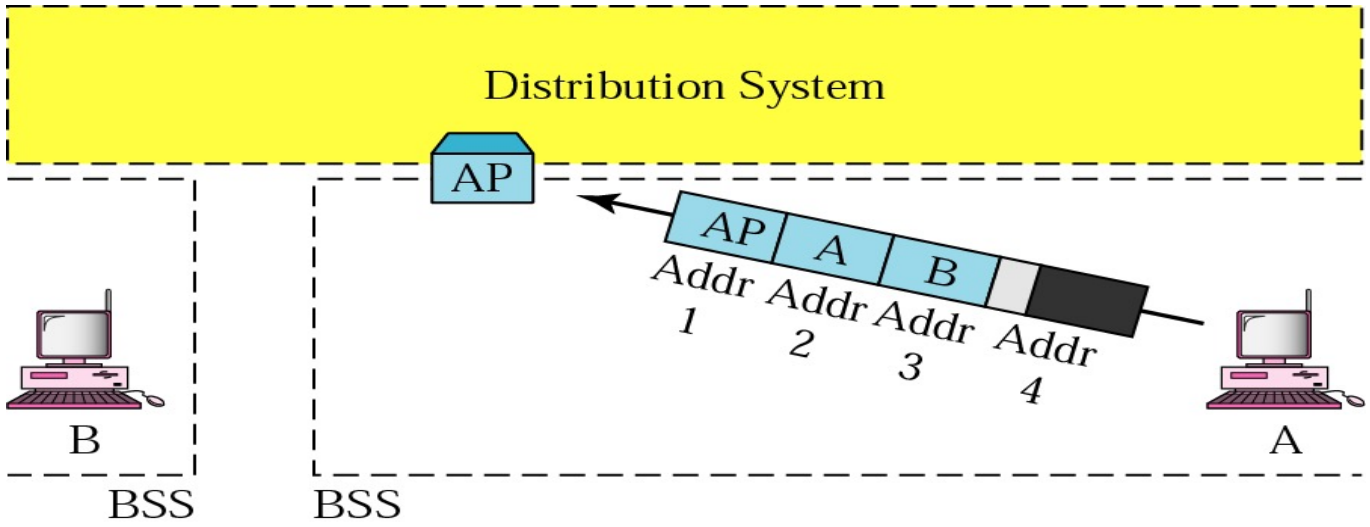
Addressing Mechanism



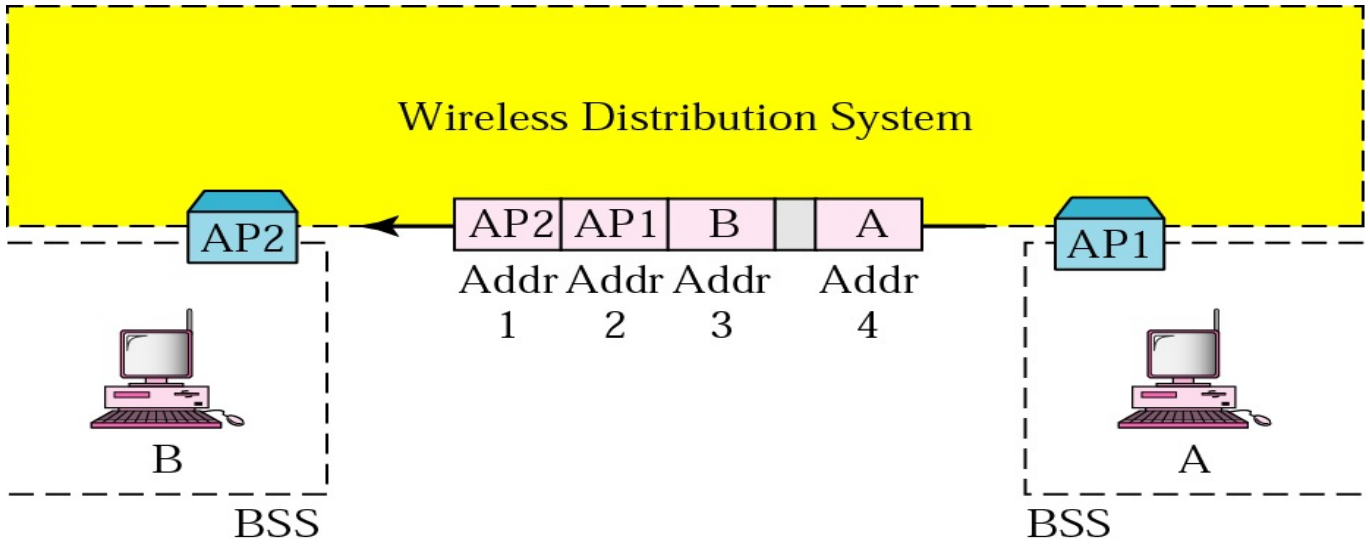
Case 1:
Frame is going directly from one client to another.
No intervening distribution system.
To DS = 0, From DS = 0

Case 2:
To DS = 0, From DS = 1 - frame is coming from a DS (Access
Point)

Addressing Mechanism



To DS = 1, From DS = 0 - frame is going to a DS (or AP)



To DS = 1 and From DS = 1

Physical layer

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Summary

- Principles behind data link layer services:
  - Error detection, correction
  - Sharing a broadcast channel: multiple access
  - Link layer addressing
- Instantiation, implementation of various link layer technologies
  - Ethernet
  - switched LANS
- Synthesis: a day in the life of a web request
- Intro to Physical layer and Wireless LAN

Summary

- Journey down protocol stack *complete*
- Solid understanding of networking principles, practice!
- ….. could stop here …. but *more* interesting topics!
  - deep understanding of wireless
  - security

THANK YOU

Ashwini M Joshi
Department of Computer Science and Engineering

ashwinimjoshi@pes.edu