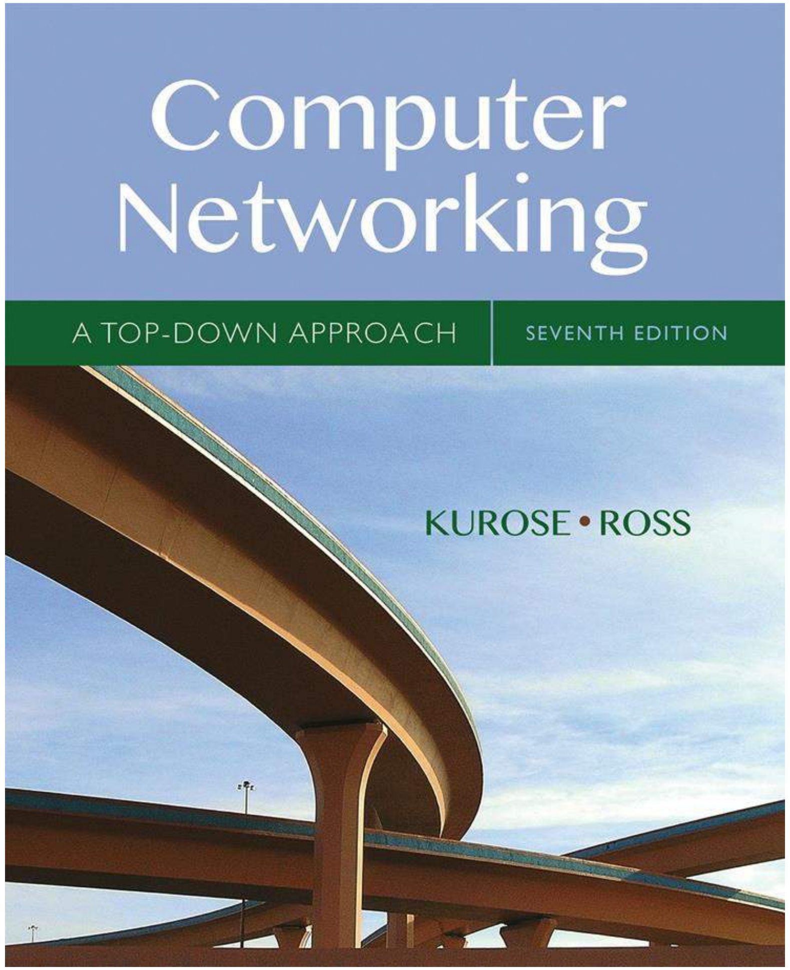
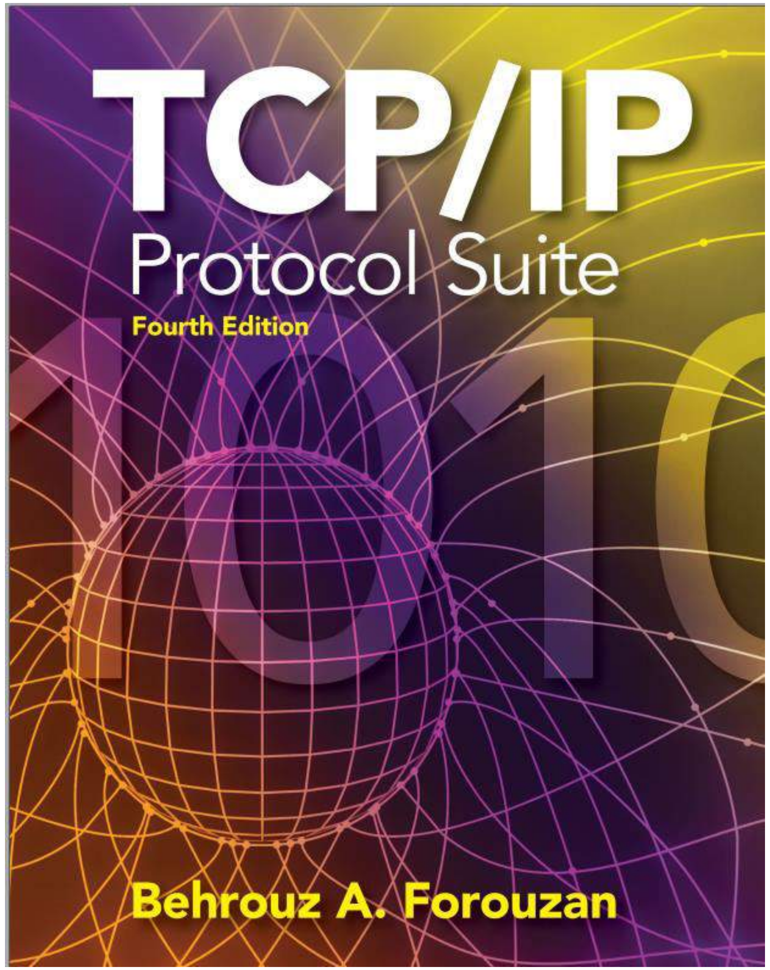
COMPUTER NETWORKS

S Nagasundari
Department of Computer Science and Engineering

Text Book





Slides adapted from

Computer Networking: A Top-Down Approach
Jim Kurose, Keith Ross
Pearson, 2017, 8th Ed.

TCP/IP protocol suite ,
Behrouz A. Forouzan.,4th Ed.

COMPUTER NETWORKS

Link Layer and LAN

S Nagasundari
Department of Computer Science and Engineering

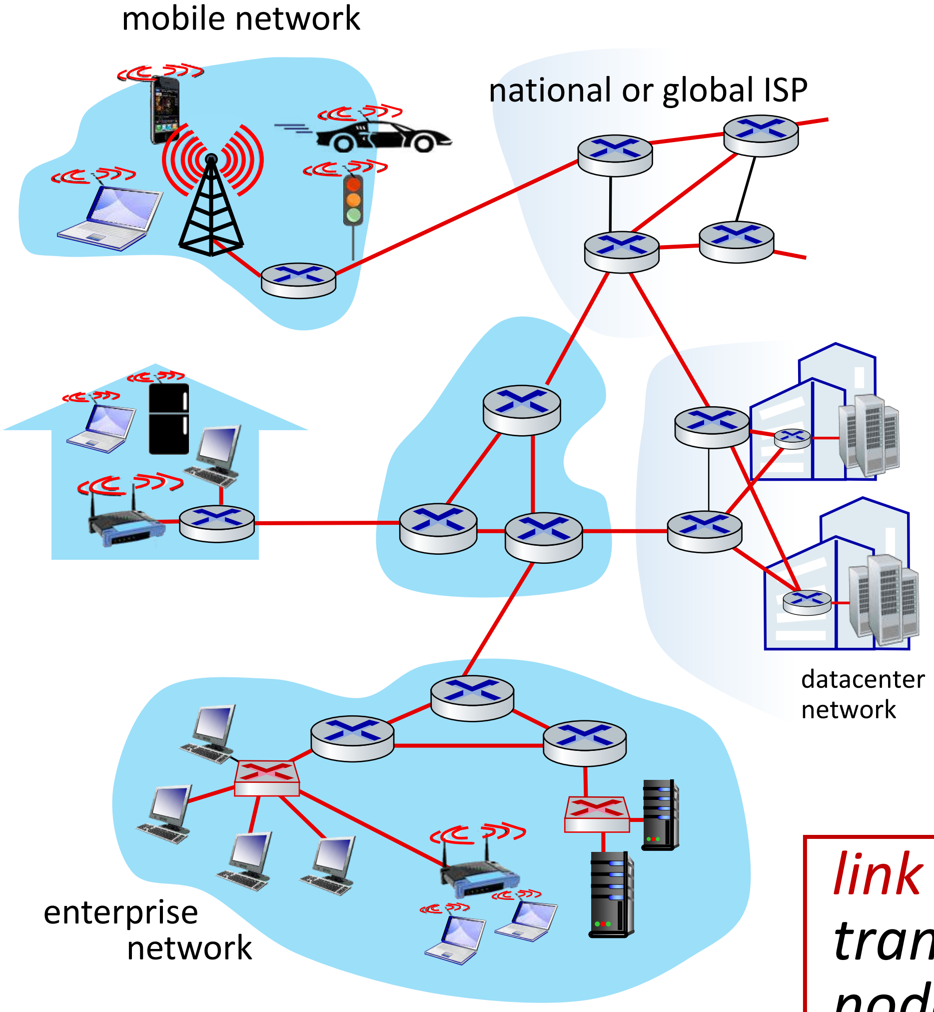
Unit – 5 Link Layer and LAN Roadmap

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

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

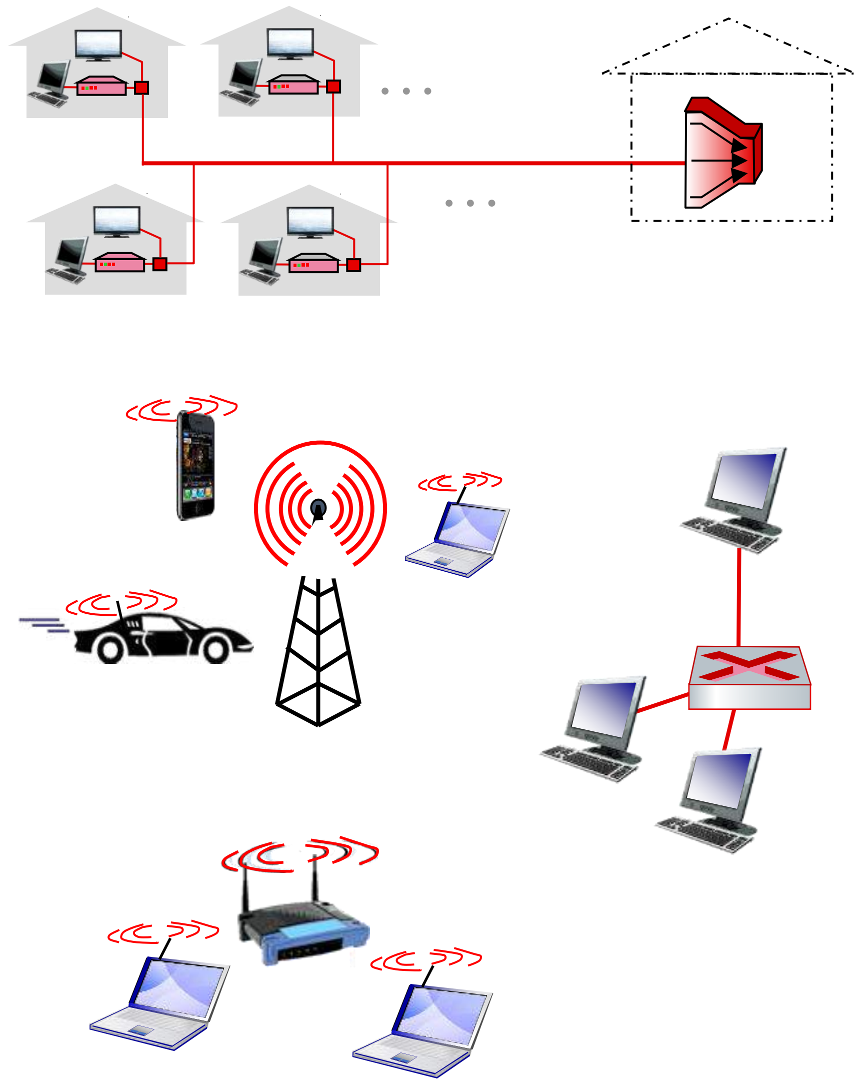
Link layer : context

- 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

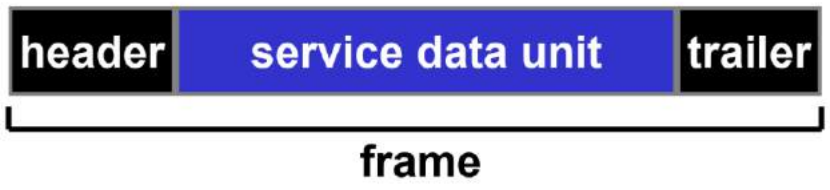
transportation analogy:

- trip from Mysore to Jaipur
  - Car: Mysore to Bangalore
  - plane: Bangalore to Delhi
  - train: Delhi to Jaipur
- tourist = datagram
- transport segment = communication link
- transportation mode = link-layer protocol
- travel agent = routing algorithm

Link layer : services

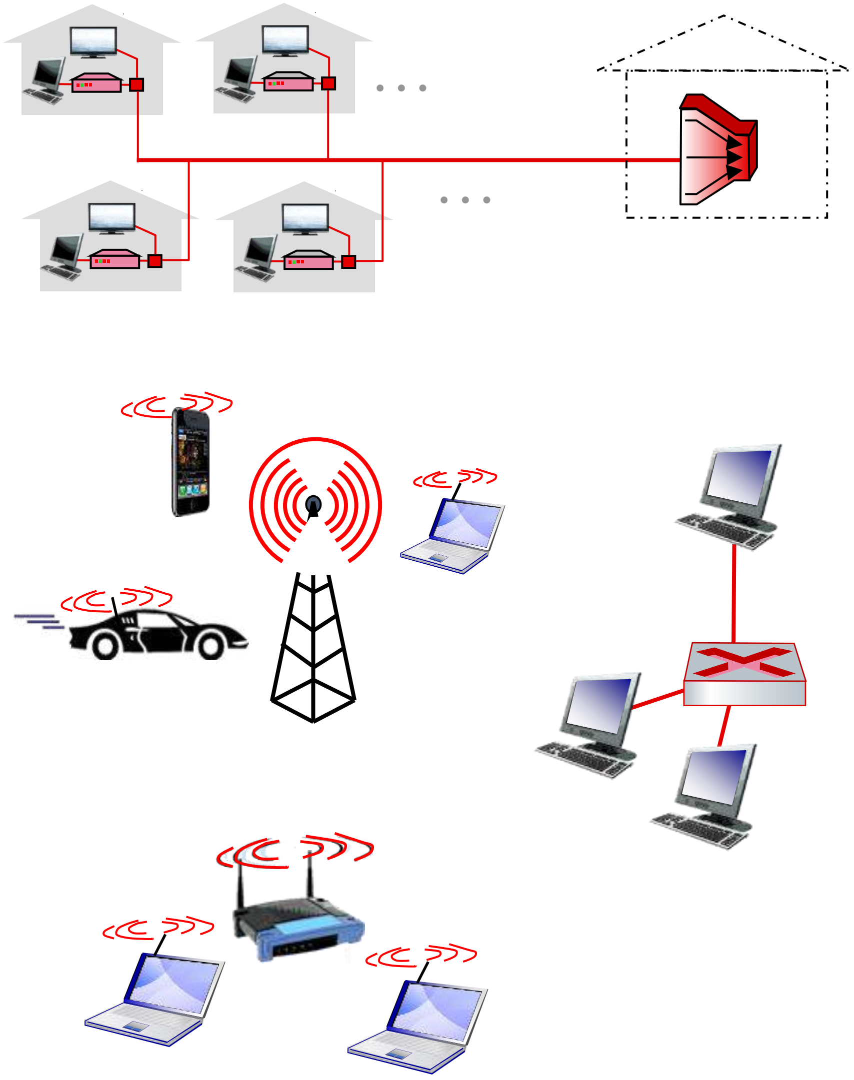


- **Framing:**
  - encapsulate datagram into frame, adding header, trailer



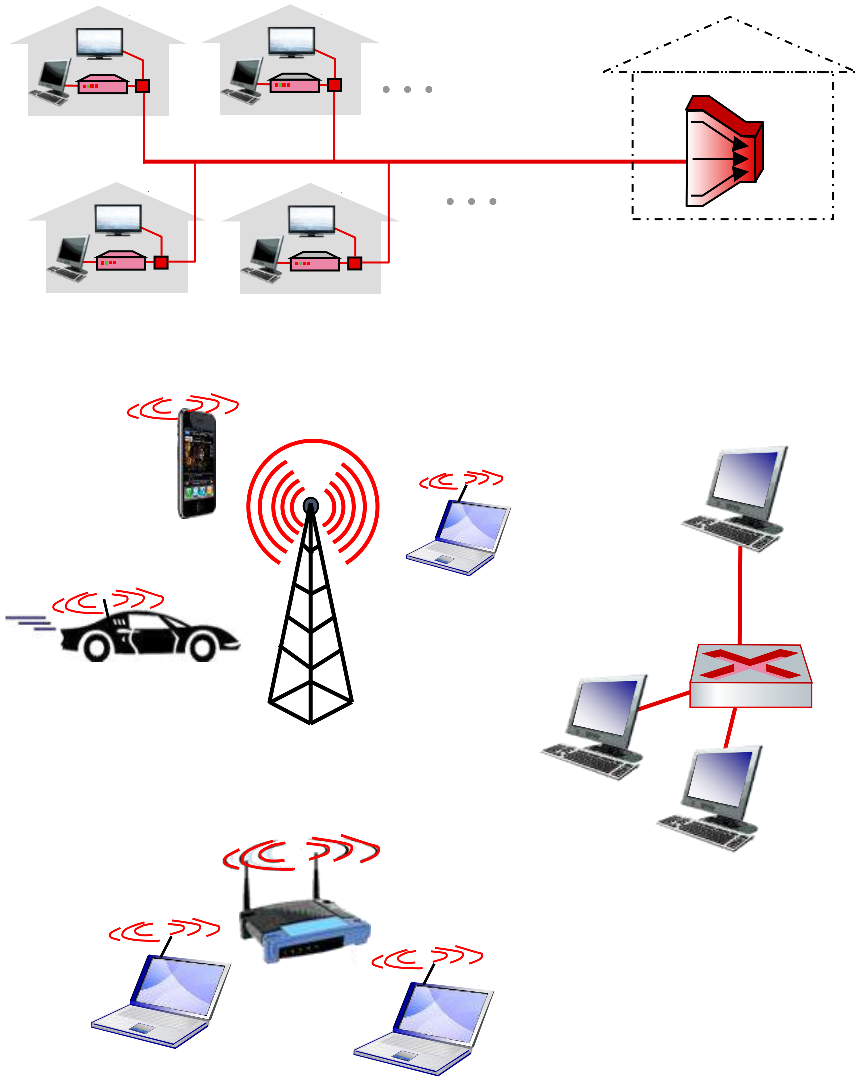
- **Link access:**
  - channel access if shared medium
  - “MAC” addresses in frame headers identify source, destination (different from IP address!)

Link layer : services



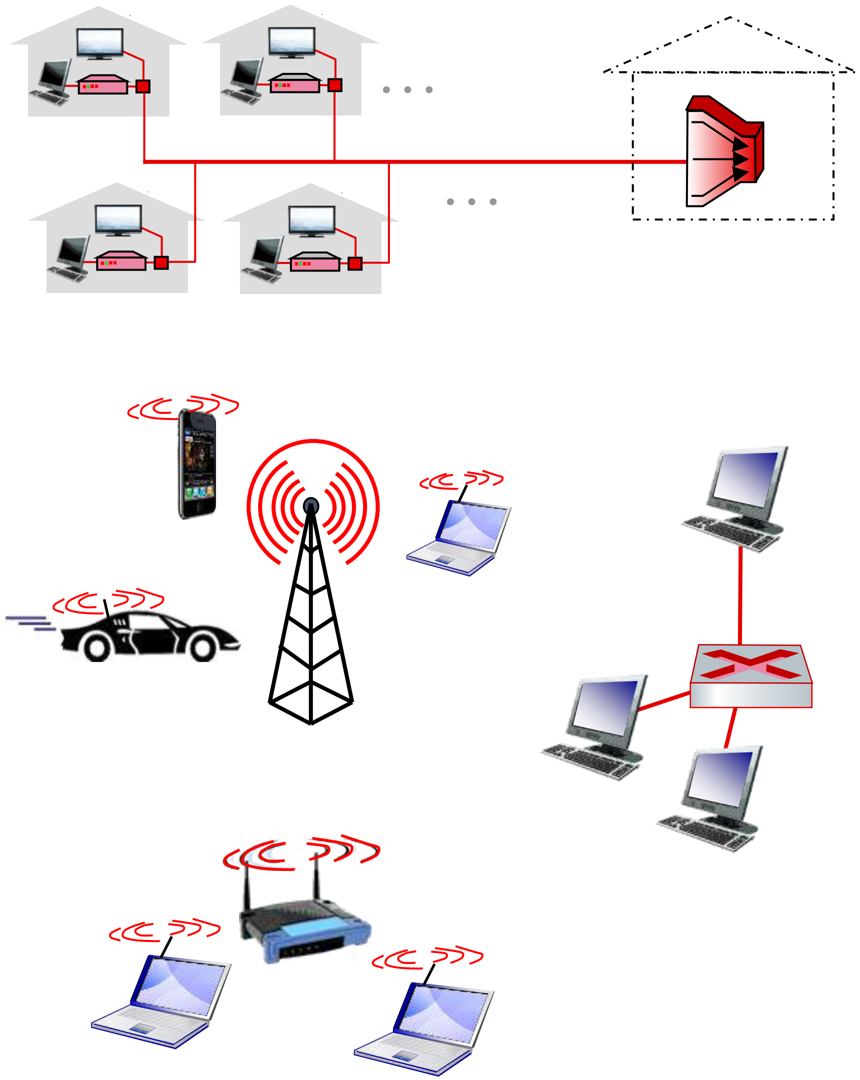
- Reliable delivery between adjacent nodes
  - we already know how to do this!
  - seldom used on low bit-error links
  - wireless links: high error rates
    - *Q:* why both link-level and end-end reliability?

Link layer : services (more)



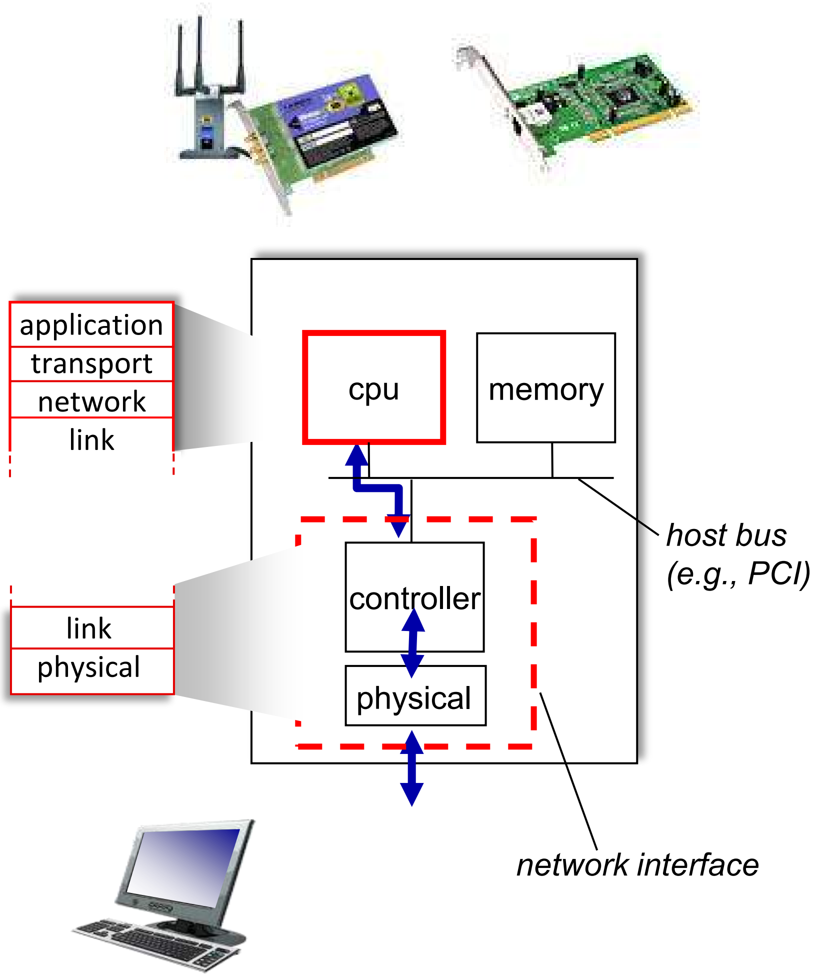
- **Flow control:**
  - pacing between adjacent sending and receiving nodes
- **Error detection:**
  - errors caused by signal attenuation, noise.
  - receiver detects errors, signals retransmission, or drops frame

Link layer : services (more)



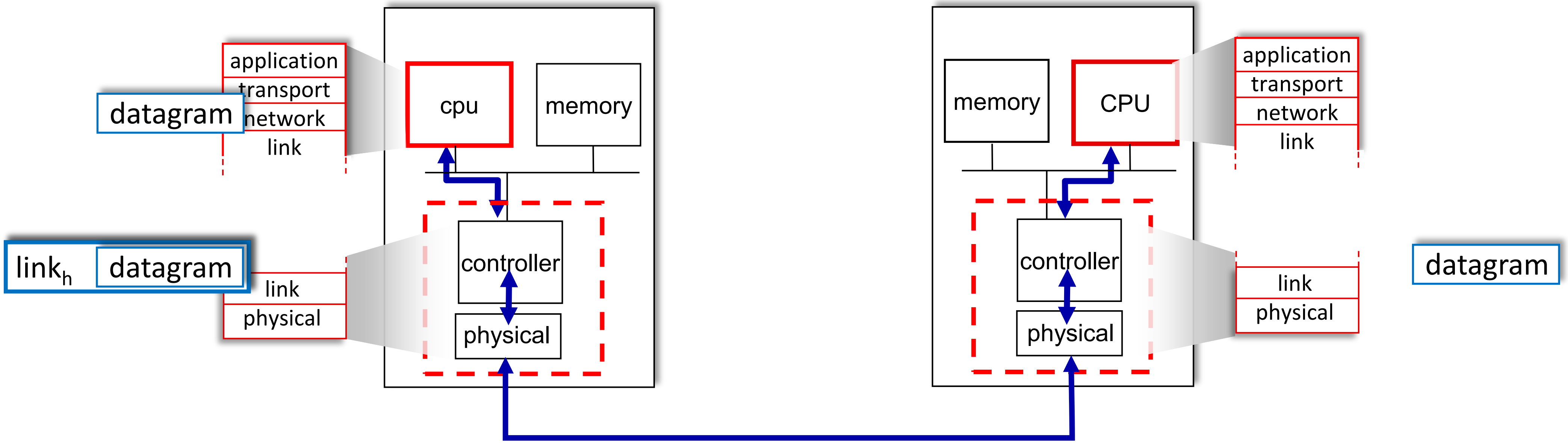
- **Error correction:**
  - receiver identifies *and corrects* bit error(s) without retransmission
- **Half-duplex and Full-duplex:**
  - with half duplex, nodes at both ends of link can transmit, but not at same time

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

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

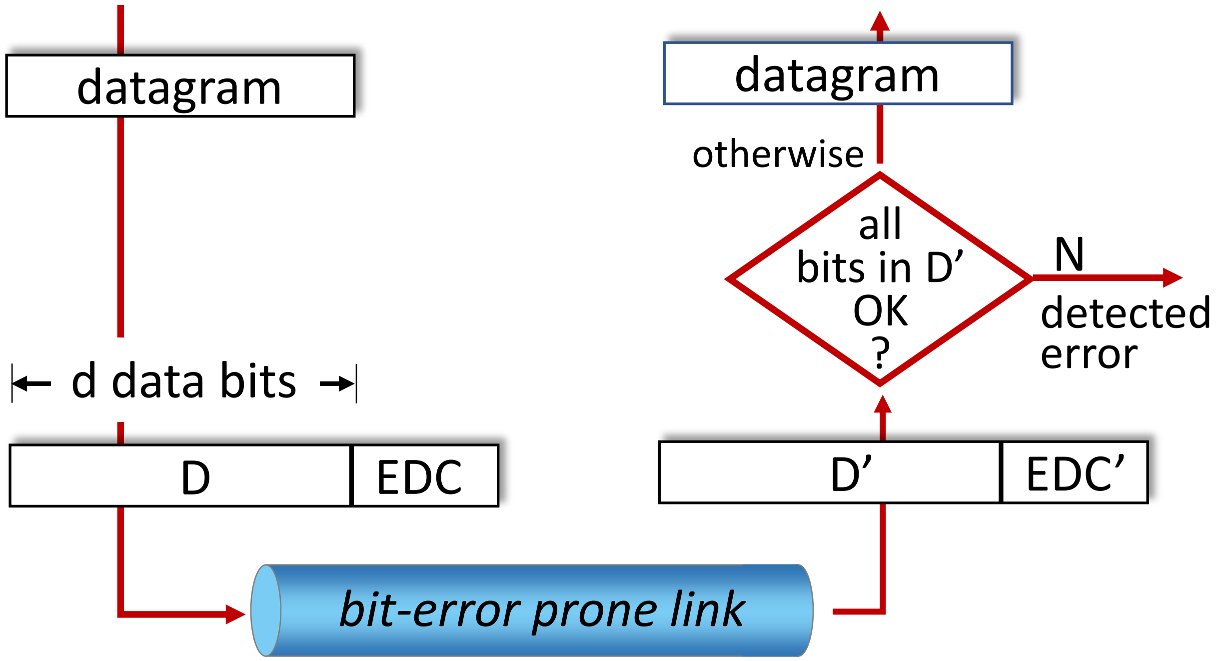
Unit – 5 Link Layer and LAN Roadmap

- 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

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

0111000110101011	1

d data bits — parity bit

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

Two-dimensional bit parity:

- detect *and correct* single bit errors

row parity →

column parity ↓

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

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

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:

$$\begin{array}{ccccc|cl}
1 & 0 & 1 & 0 & 1 & 1 & \\
1 & 0 & 1 & 1 & 0 & 0 & \leftarrow \text{parity error} \\
0 & 1 & 1 & 1 & 0 & 1 & \\
\hline
0 & 0 & 1 & 0 & 1 & 0 & \\
 & \uparrow & & & & & \\
 & \text{parity error} & & & & &
\end{array}$$

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)

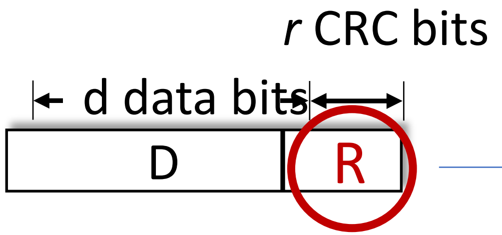
- More powerful error-detection coding
- D: data bits (given, think of these as a binary number)
- G: bit pattern (generator), of *r+1* bits (given)

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)



bit pattern

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

formula for bit pattern

Cyclic Redundancy Check (CRC) : example

We want:

$$D \cdot 2^r \text{ XOR } R = nG$$

or equivalently:

$$D \cdot 2^r = nG \text{ XOR } R$$

or equivalently:

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

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

```
   G                      1 0 1 0 1 1
 1 0 0 1 ) 1 0 1 1 1 0 0 0 0     <- D*2^r
           1 0 0 1
             1 0 1
             0 0 0
             1 0 1 0
             1 0 0 1
               1 1 0
               0 0 0
               1 1 0 0
               1 0 0 1
                 1 0 1 0
                 1 0 0 1
                   0 1 1
                     R
```

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

THANK YOU

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
Department of Computer Science and Engineering

PES UNIVERSITY ONLINE

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 48 : Multiple Access Protocols : Learning Objectives

PES UNIVERSITY ONLINE

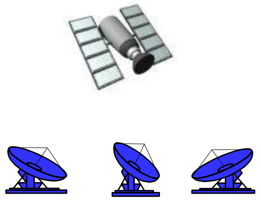
- Multiple Access
- Carrier Sense Multiple Access/Collision Detection

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 problem

How to coordinate the access of multiple sending and receiving nodes to a shared broadcast channel

- Broadcast channels are often used in
  - LANs,
  - Networks that are geographically concentrated in a single building (or on a corporate or university campus).

- Can I say Television as an example for Broadcasting??
  - Traditional television-one-way broadcast
  - While nodes on a computer network- broadcast channel can both send and receive

Human Protocols for sharing Broadcast channel

- Give everyone a chance to speak.
- Don’t speak until you are spoken to.
- Don’t monopolize the conversation.
- Raise your hand if you have a question.
- Don’t interrupt when someone is speaking.
- Don’t fall asleep when someone is talking

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

When multiple nodes are active in Broadcast channel,

- coordinate the transmissions of the active nodes.

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

Desirable characteristics:

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
  - Eg: TDM,FDM,CDMA
- *Random access*
  - channel not divided, allow collisions
  - “recover” from collisions
  - Eg. ALOHA,CSMA deployed in Ethernet
- “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:(Carrier Sensing)

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

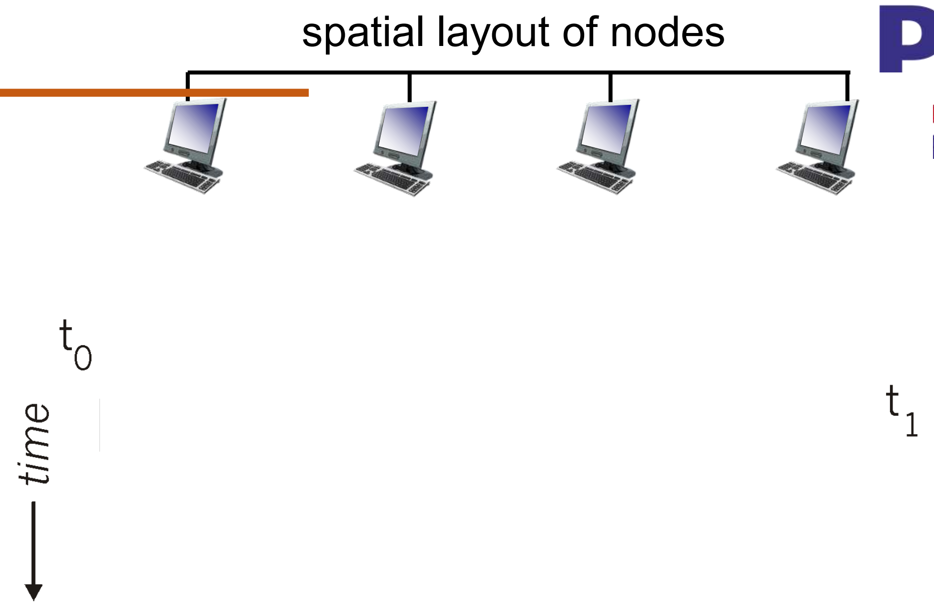
- Human analogy: don't interrupt others!

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

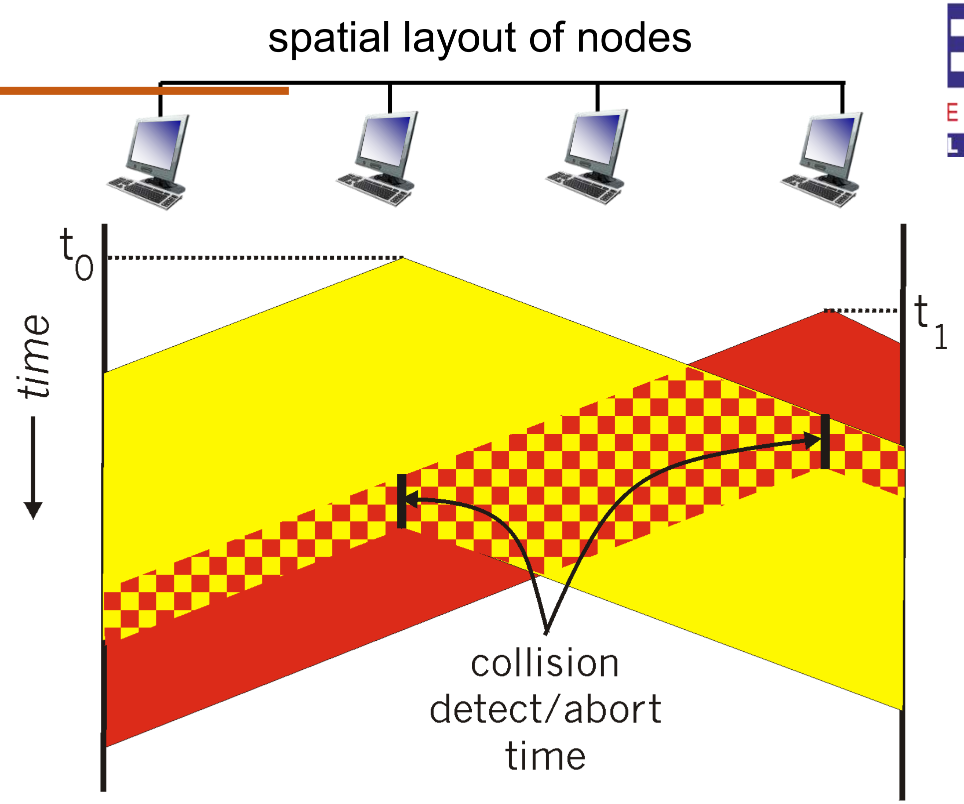
CSMA : Collisions



- 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/CD 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

S Nagasundari
Department of Computer Science and Engineering
nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
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
- Physical layer
- Wireless LANs: IEEE 802.11
- A day in the life of a web request

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

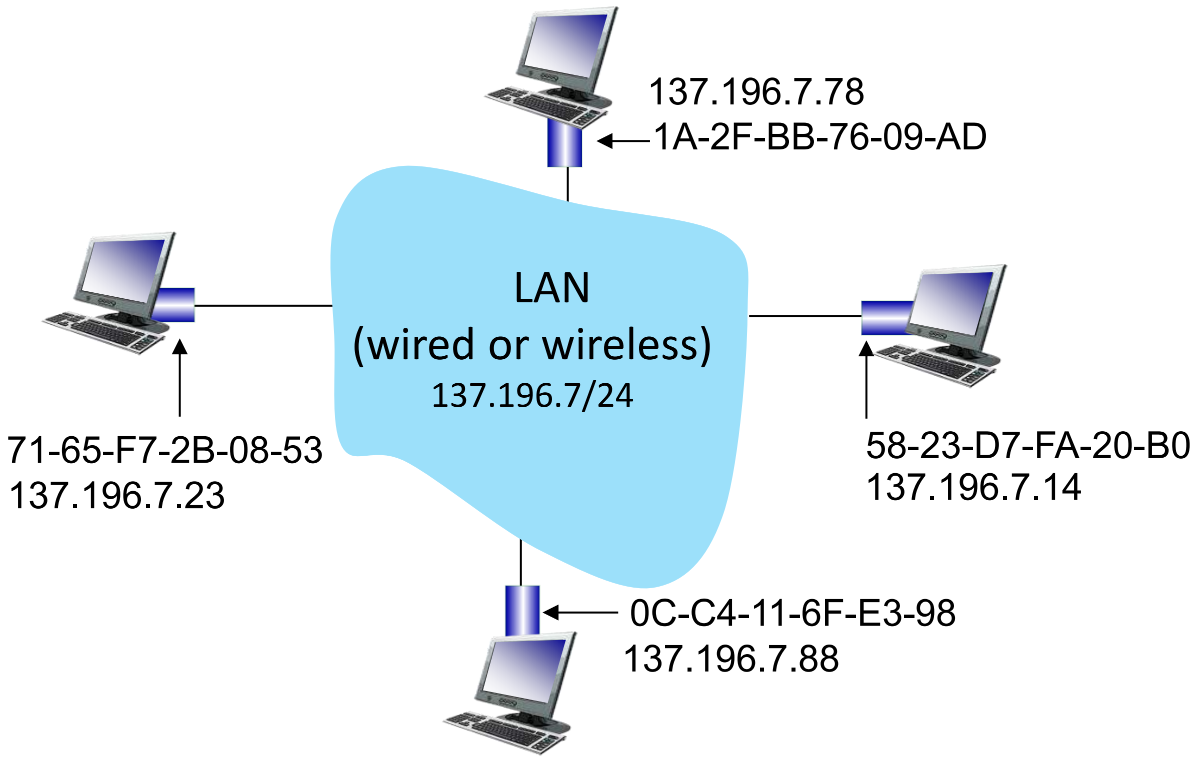
- MAC (or LAN or physical or Ethernet) address:
  - function: used "locally" to get frame from one interface to another physically-connected interface (same subnet, in IP-addressing sense)
  - 48-bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

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)

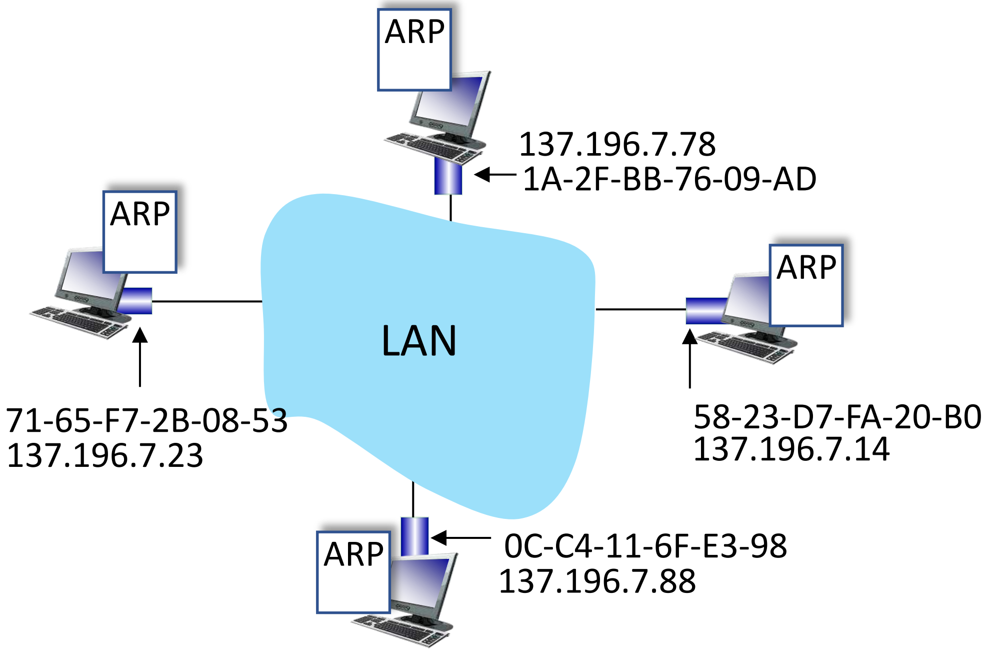


MAC Addresses

- 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

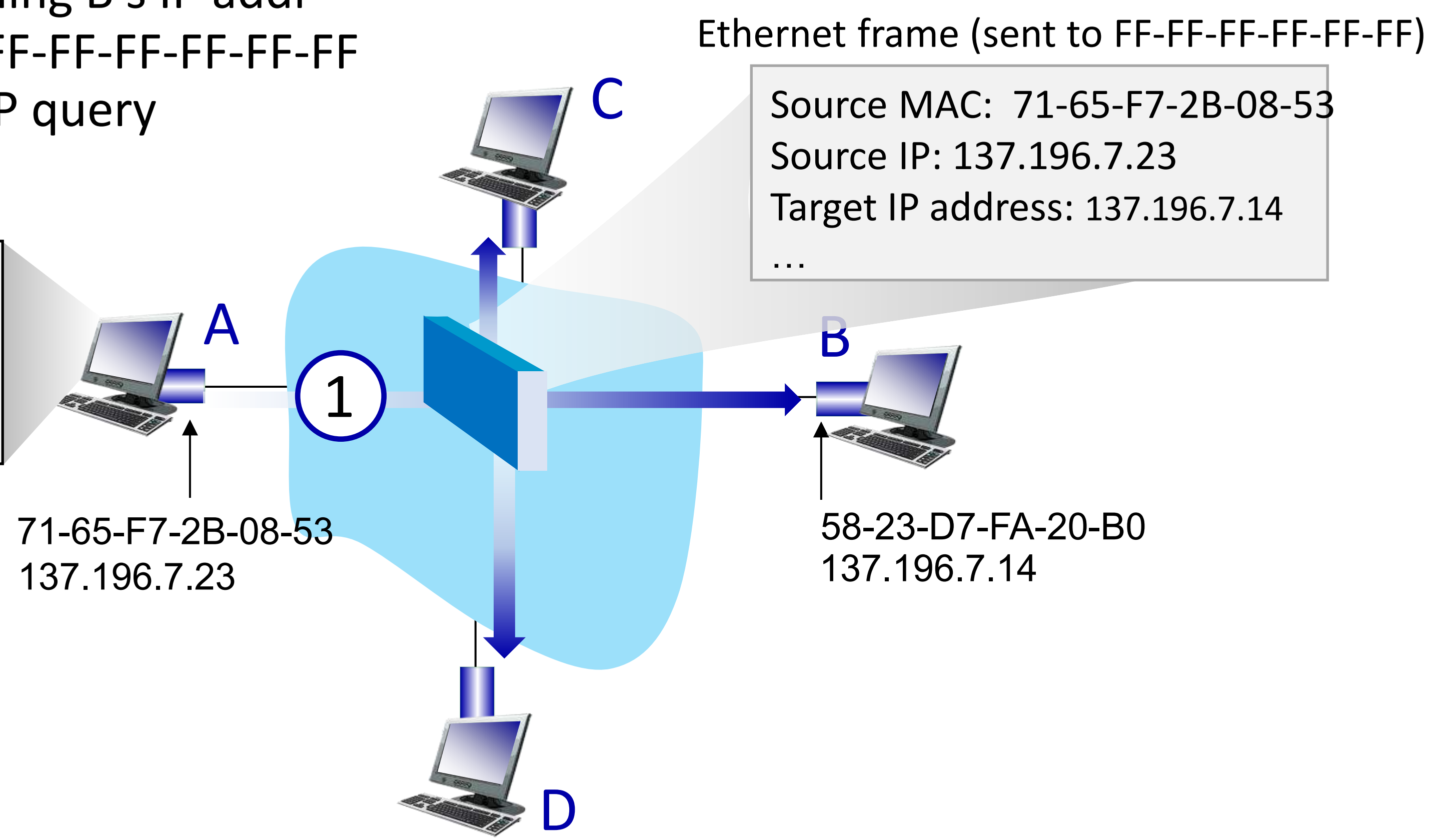
Example: A wants to send datagram to B

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

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

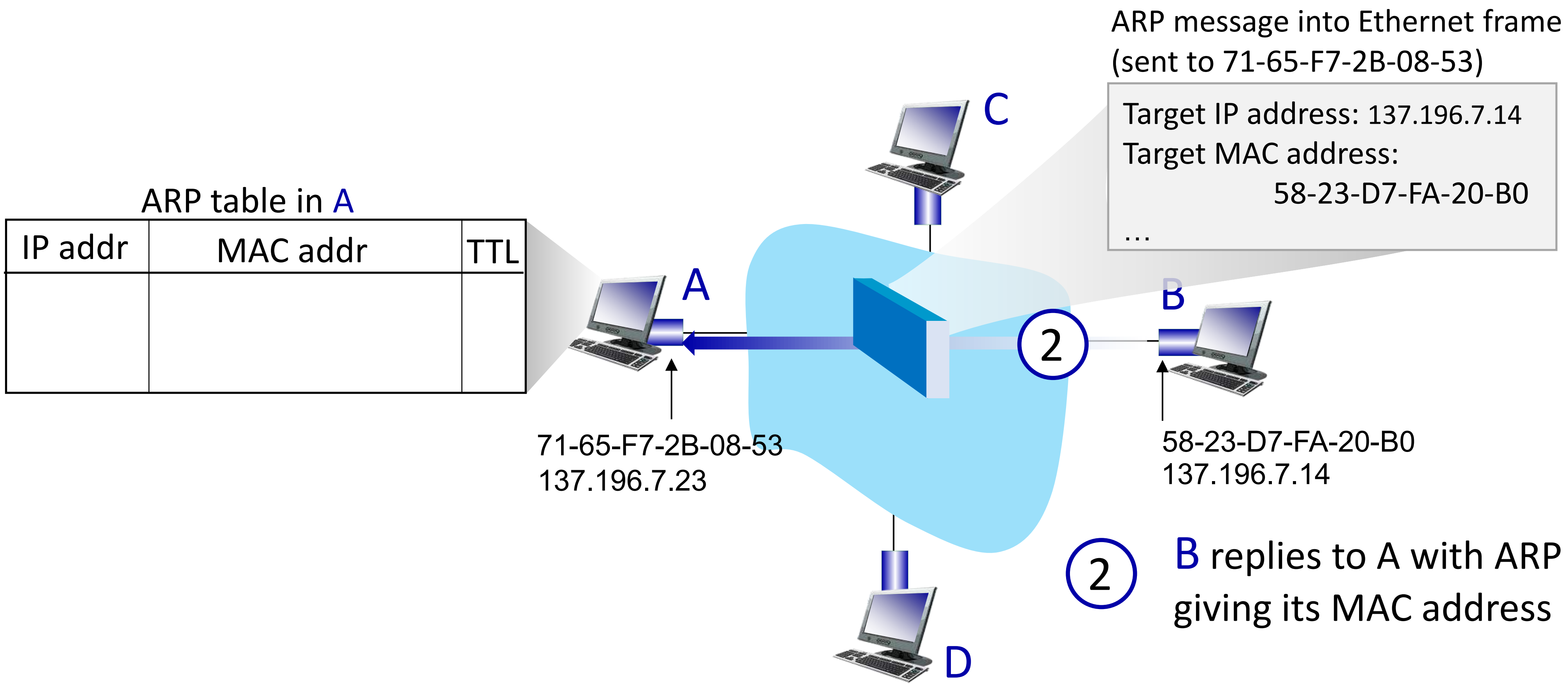
IP addr	MAC addr	TTL



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



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

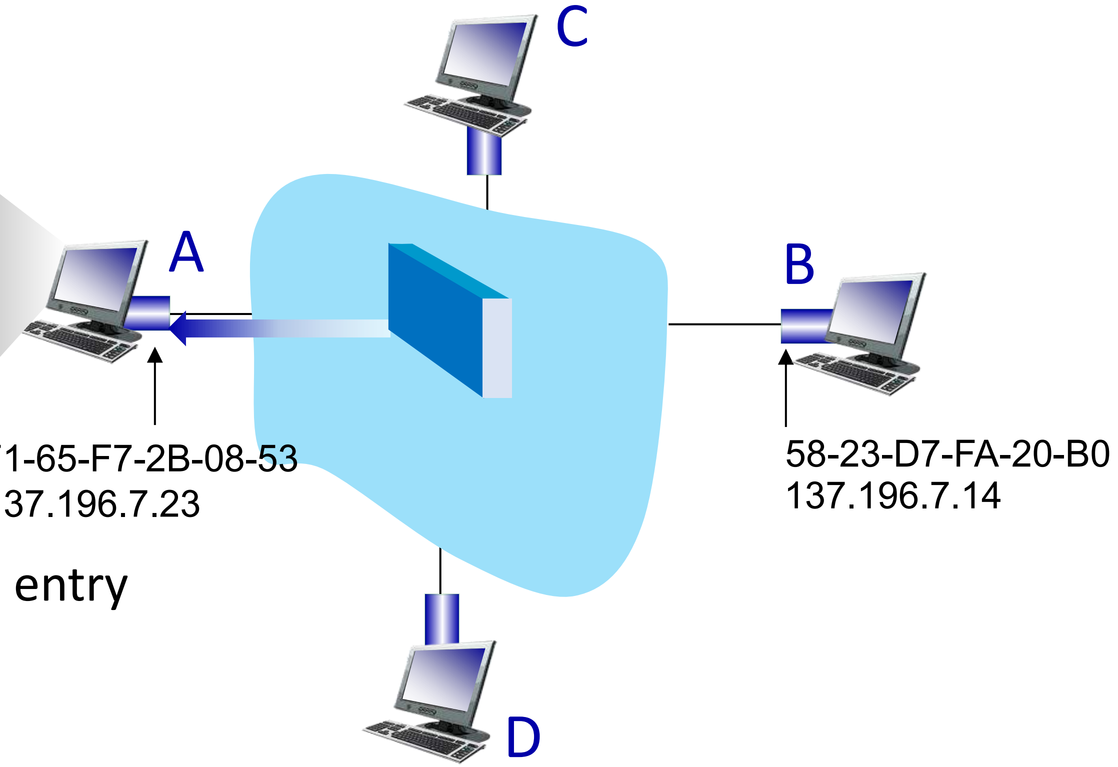
ARP Protocol in action

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

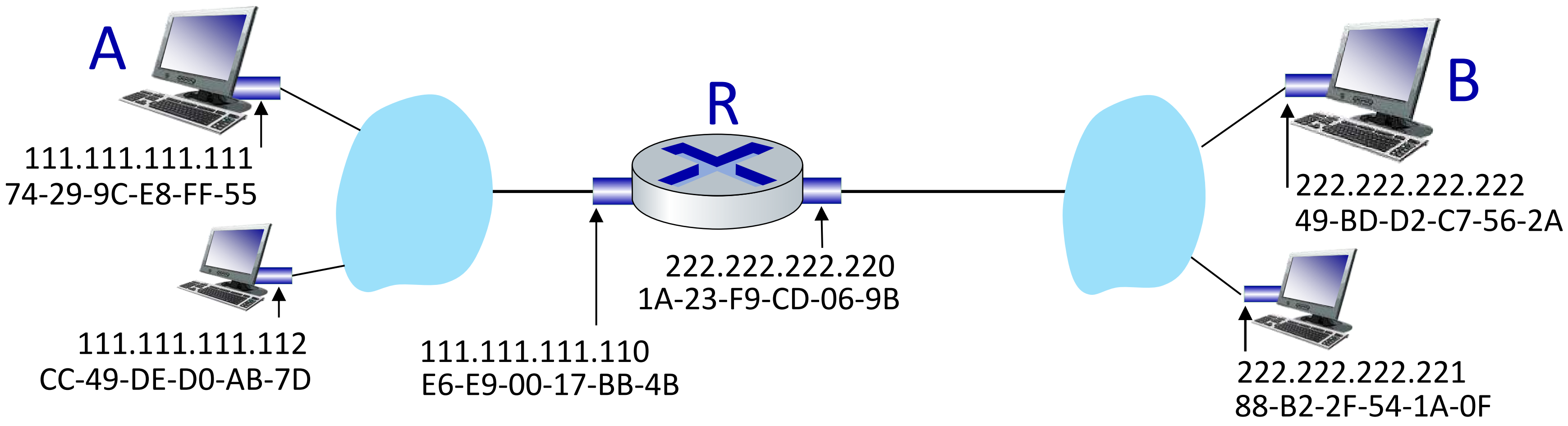


3 A receives B's reply, adds B entry into its local ARP table

Routing to another Subnet : Addressing

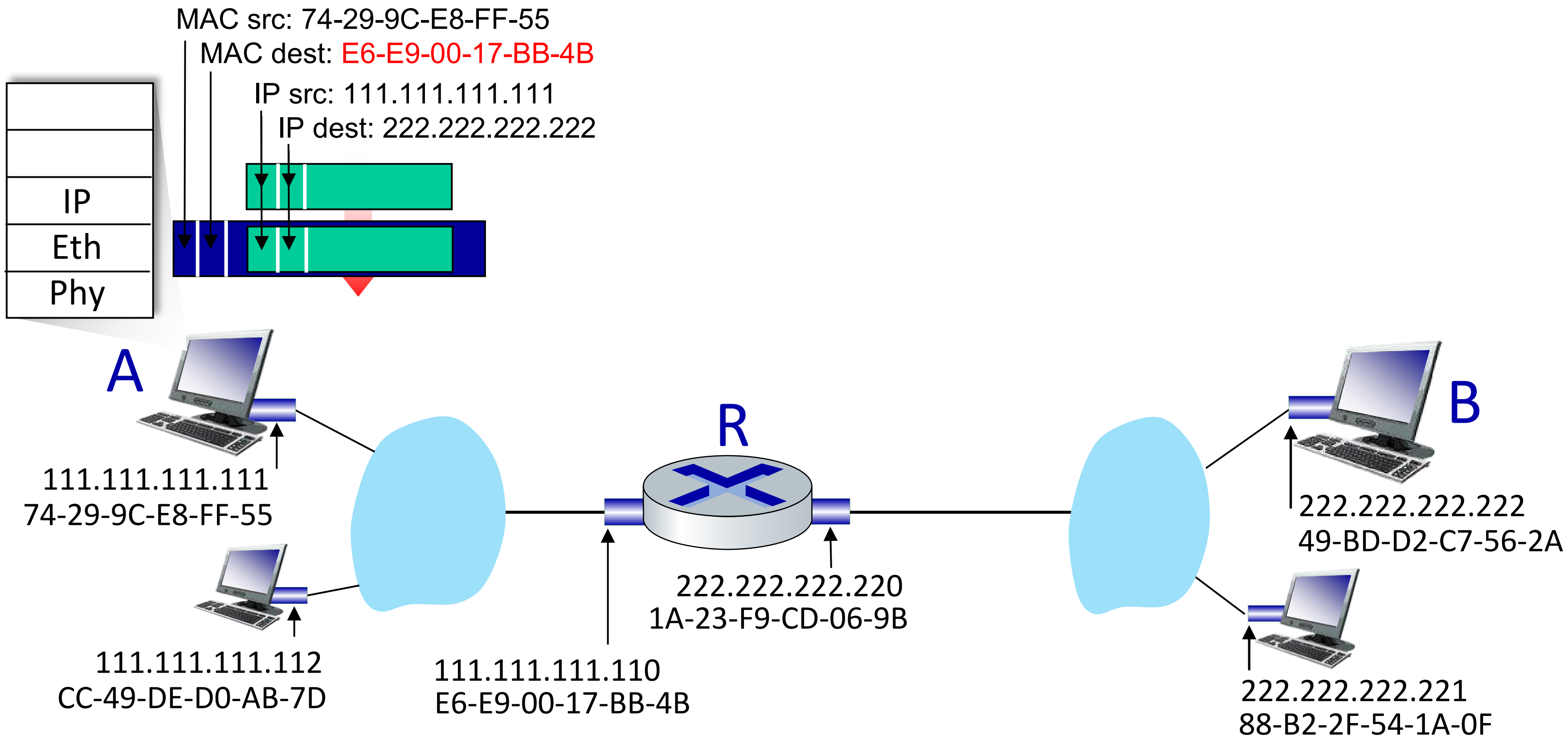
Walkthrough: sending a datagram from *A* to *B* via *R*

- 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?)



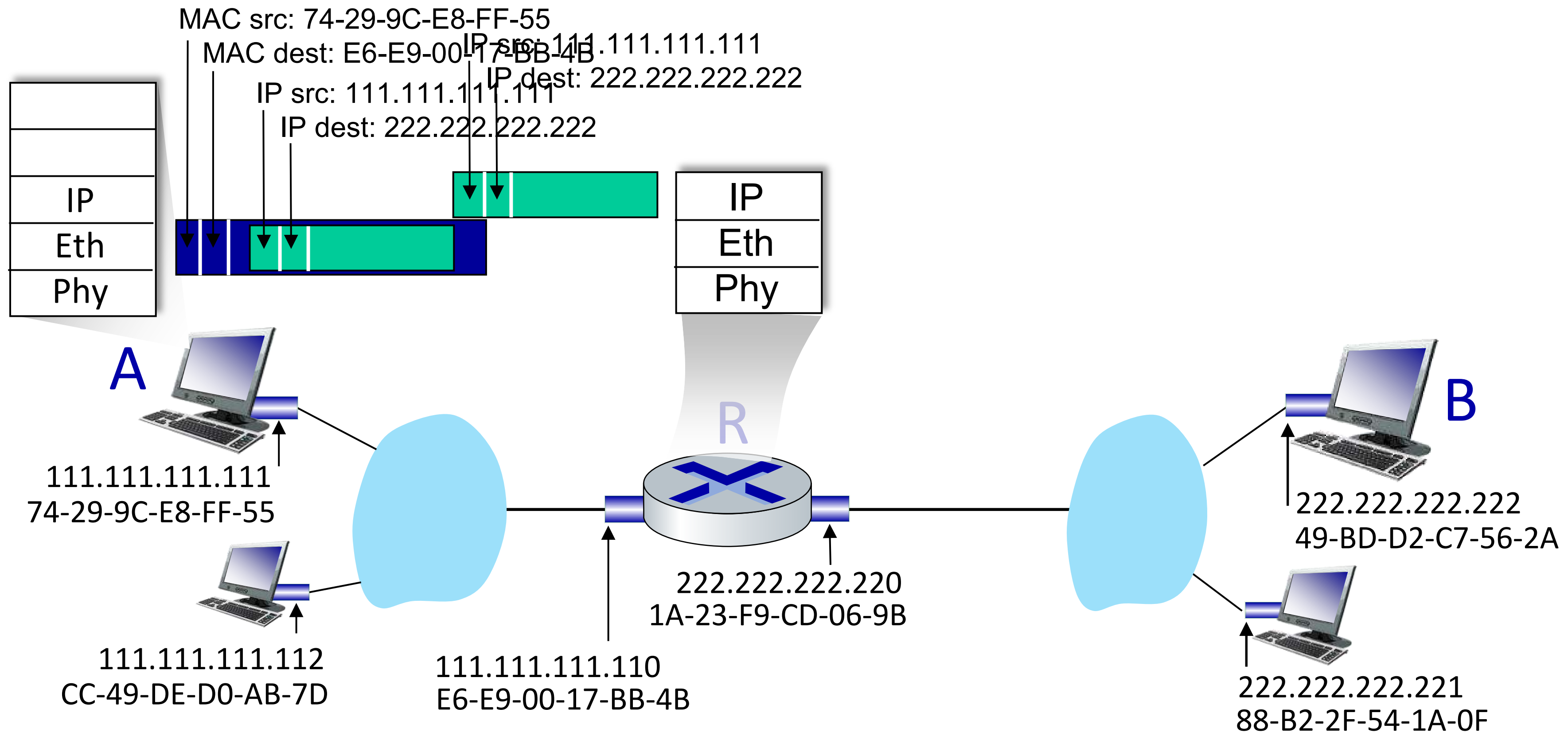
Routing to another Subnet : Addressing

- 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



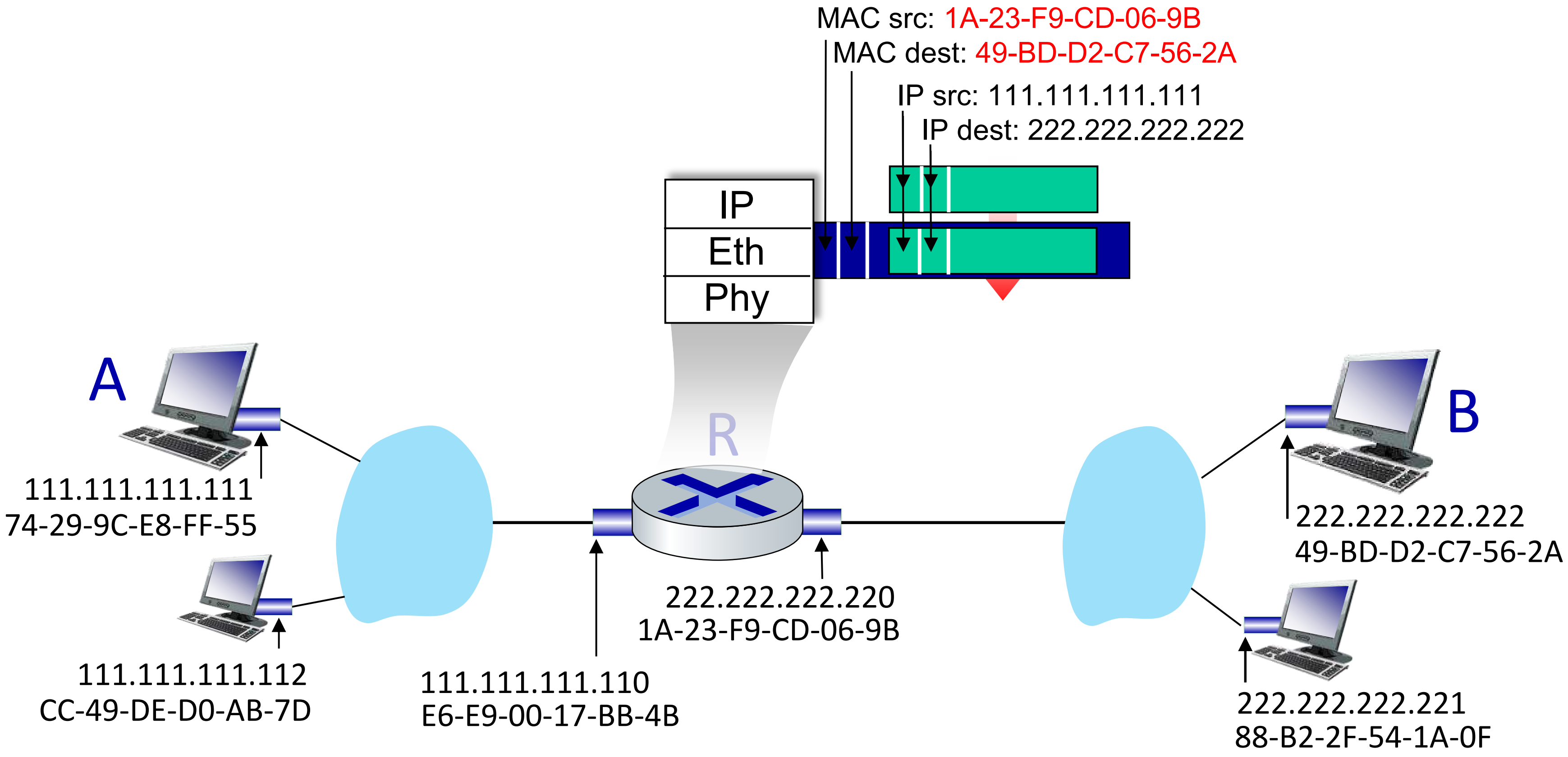
Routing to another Subnet : Addressing

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



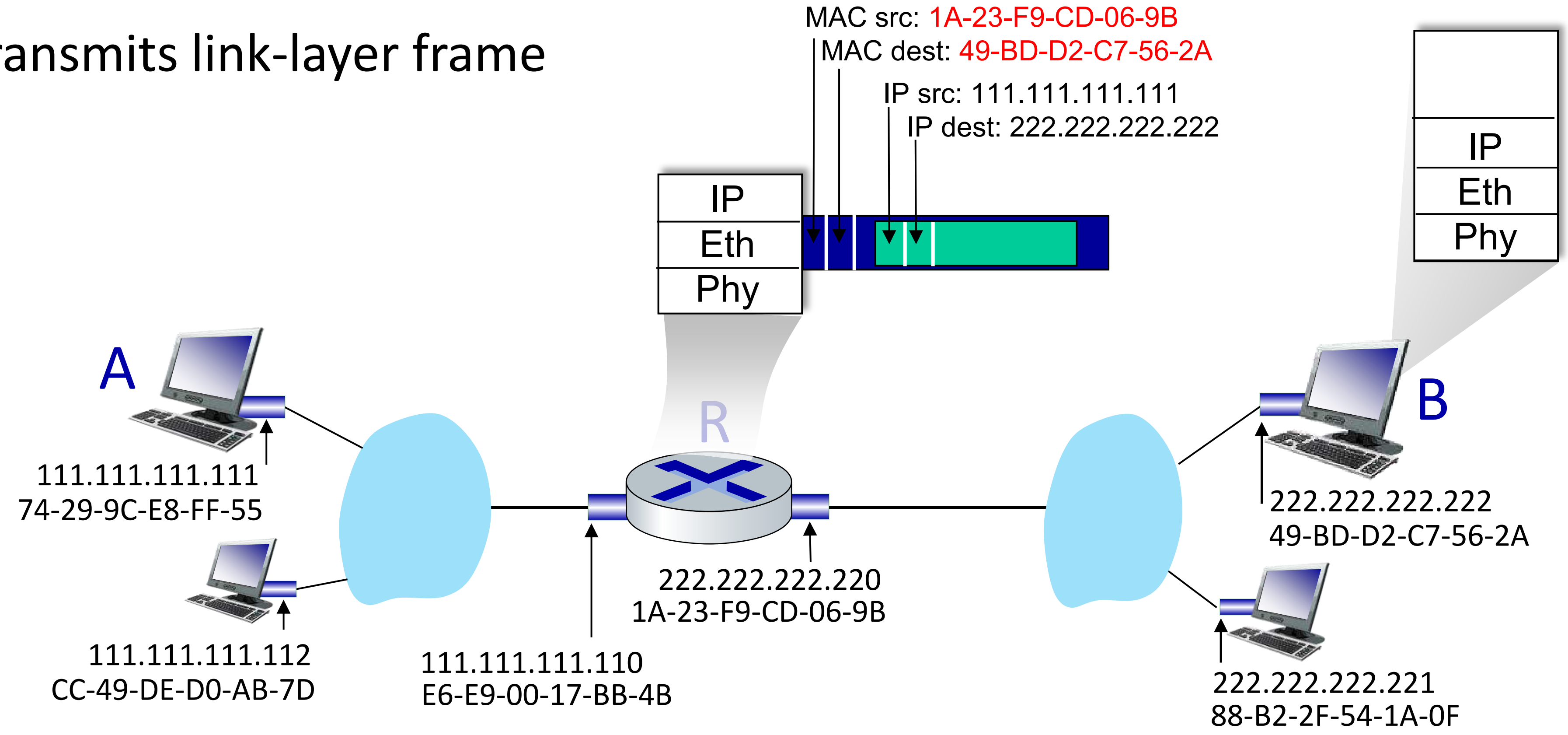
Routing to another Subnet : Addressing

- 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



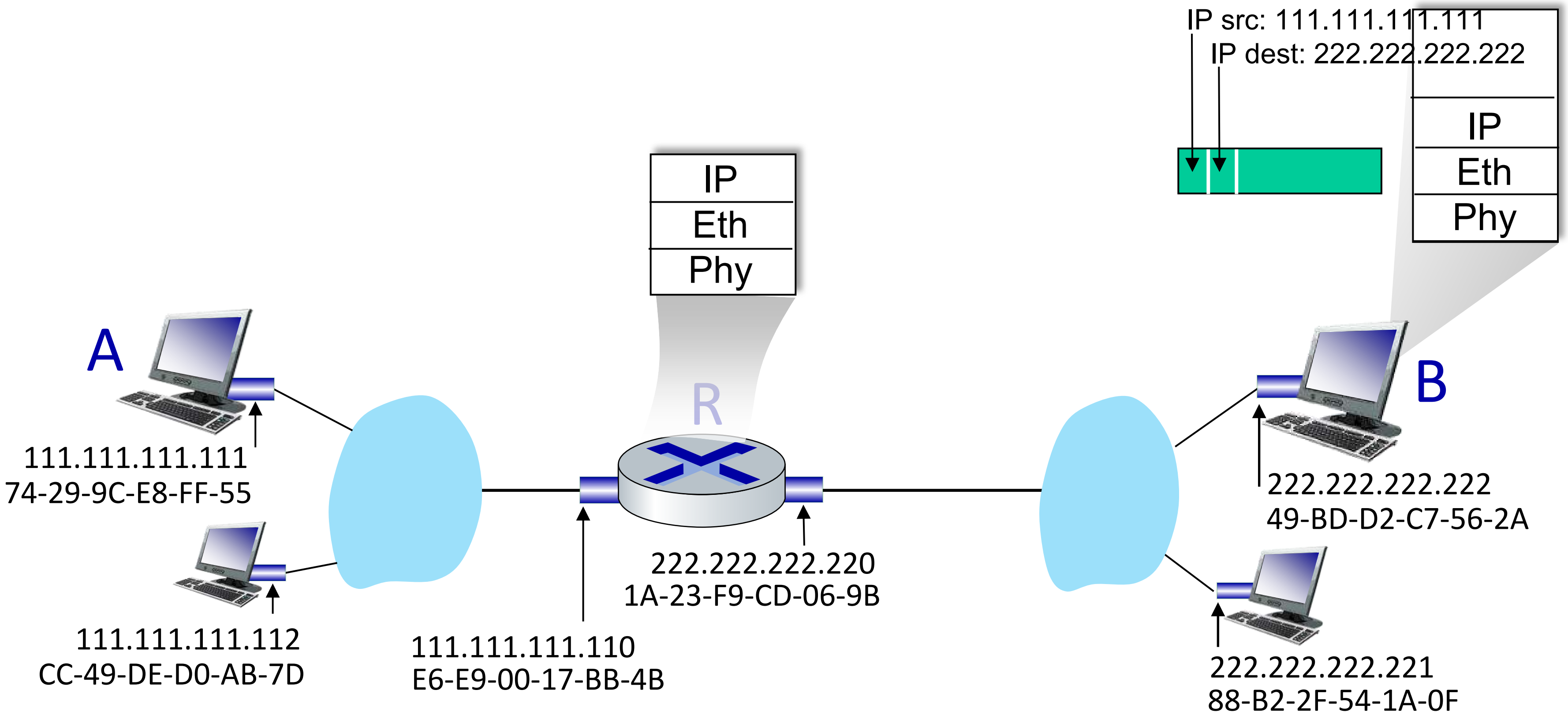
Routing to another Subnet : Addressing

- 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

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
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

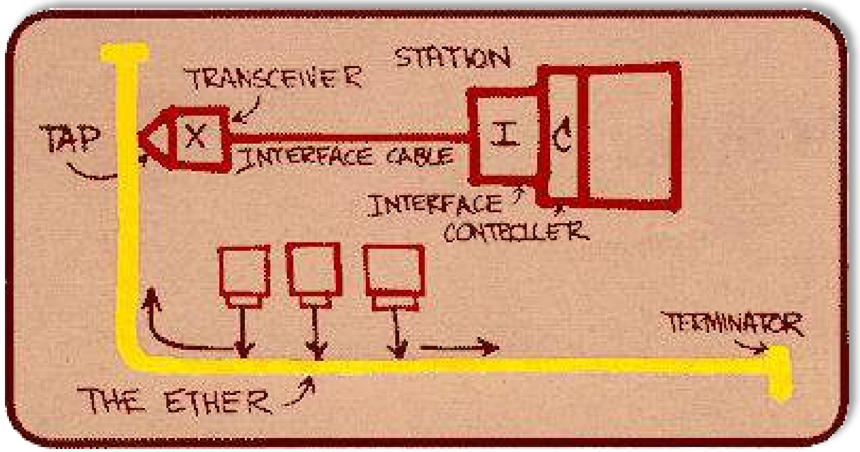
Class 50 : Ethernet : Learning Objectives

- 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

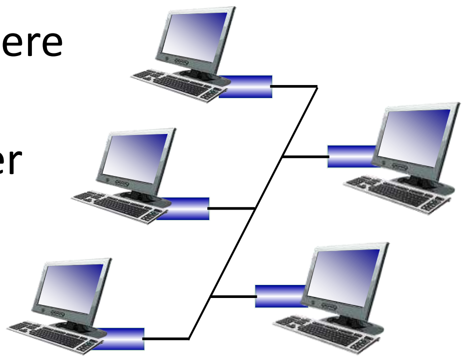
Ethernet : Physical Topology

- 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)

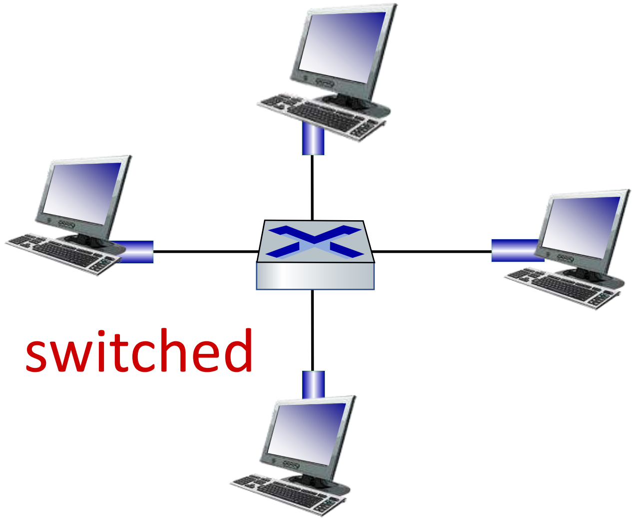
Traditional Ethernet

- Nodes connected with coax
- Long "runs" of wire everywhere
- CSMA/CD protocol

Hub acts as a broadcast repeater
Shorted cable "runs", Useful for 100 Mbps
– CSMA/CD protocol
– Easy to add/remove users
– Easy to localize faults
– Cheap cabling (twisted pair, 10baseT)



bus: coaxial cable



switched

Easy to increase data rate (e.g., Gbit Ethernet)

- Nodes transmit when they want
- Switch queues the packets and transmits to destination
- Typical switch capacity of 20-40 ports
- Each node can now transmit at the full rate of 10/100/Gbps
- Modularity: Switches can be connected to each ther using high rate ports

Ethernet Frame Structure

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

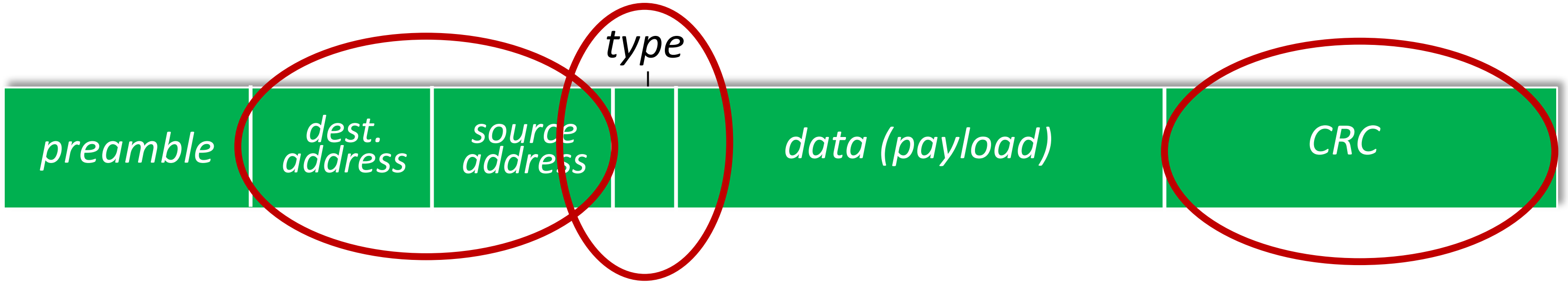
Preamble:

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

Data:

- 46 to 1,500 bytes
- Min-46

Ethernet Frame Structure (more)



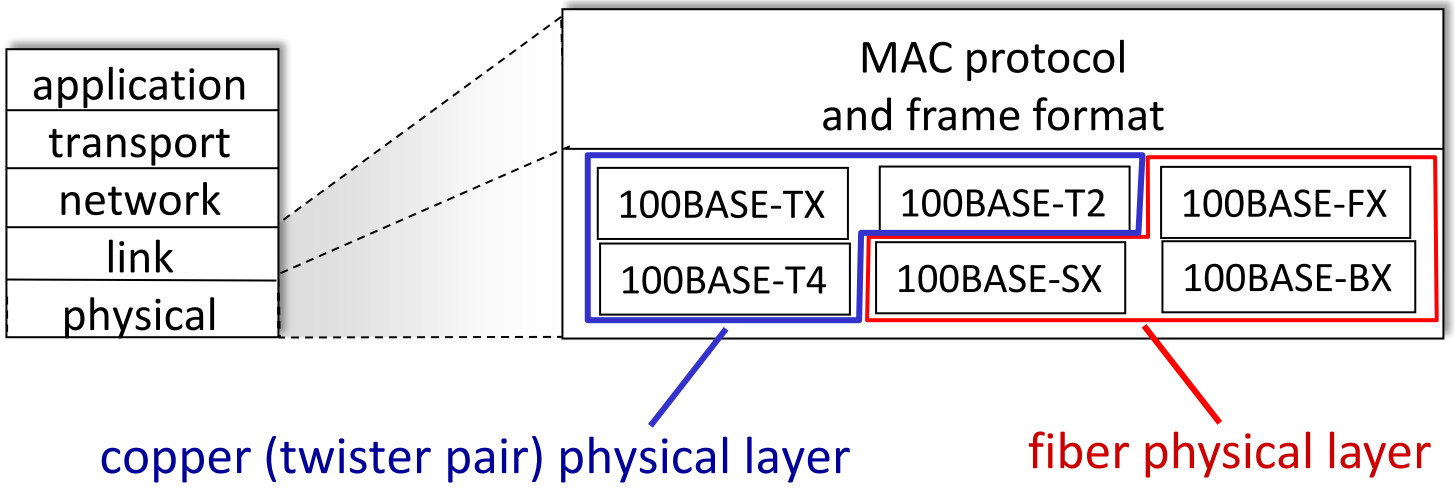
- Addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- Type: indicates higher layer protocol
  - mostly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



802.3 Ethernet Standards: Link and Physical Layers

Gigabit Ethernet is an extension of Ethernet standards

- Data rate- 40,000 Mbps, 40 Gigabit Ethernet
- Fully compatible with the huge installed base of Ethernet equipment.
- Standard - IEEE 802.3z, does the following:
  - Uses the standard Ethernet frame format
  - Backward compatible with 10BASE-T and 100BASE-T technologies.
  - Allows for point-to-point links as well as shared broadcast channels
    - Point-to-point links use switches
    - Broadcast channels use hubs
    - Hubs-*buffered distributors*.
    - Uses CSMA/CD for shared broadcast channels.
    - In order to have acceptable efficiency, the maximum distance between nodes must be severely restricted.
    - Allows full-duplex operation at 40 Gbps in both directions for point-to-point channels.

THANK YOU

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
Department of Computer Science and Engineering

COMPUTER NETWORKS

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

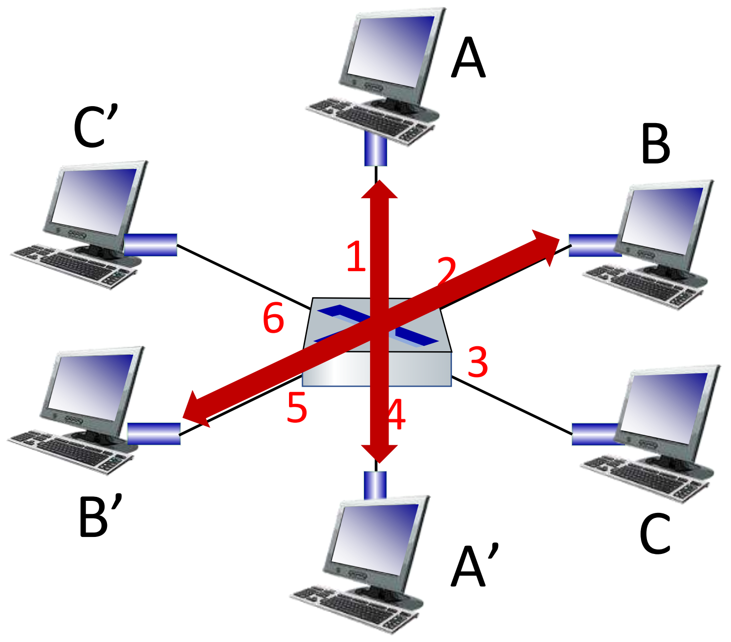
- Multiple Simultaneous Transmissions
- Frame Forwarding and Filtering

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,
  - 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

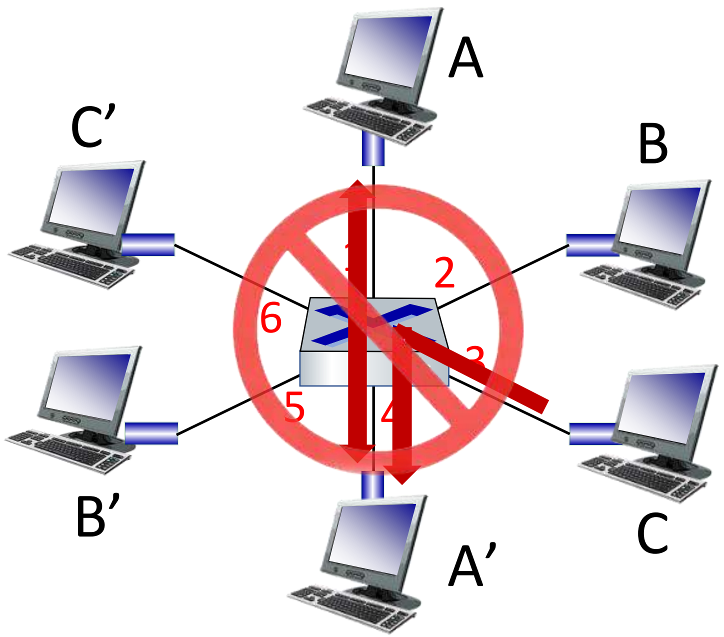
- Hosts have dedicated, direct connection to switch
- Switches buffer packets
- Ethernet protocol used on *each* incoming link, so:
  - no collisions; full duplex
  - each link is its own collision domain
- Switching: A-to-A' and B-to-B' can transmit simultaneously, without collisions



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



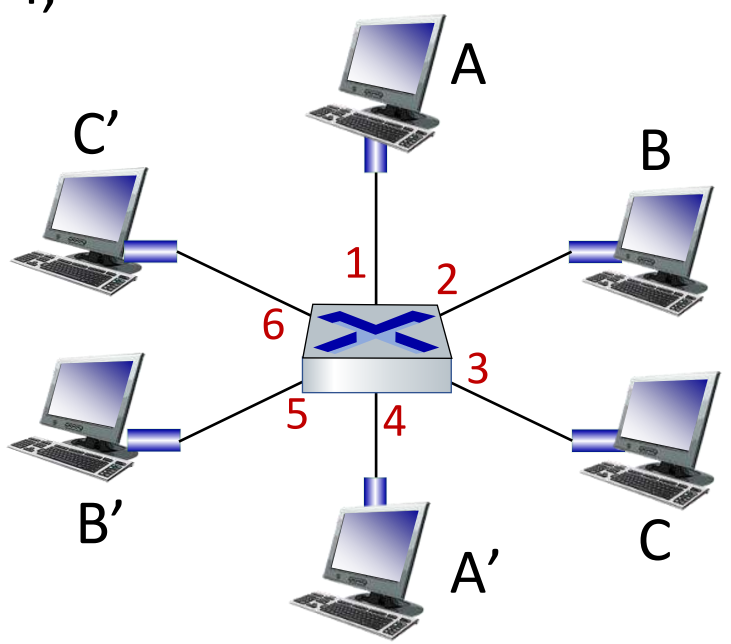
switch with six interfaces (1,2,3,4,5,6)

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!

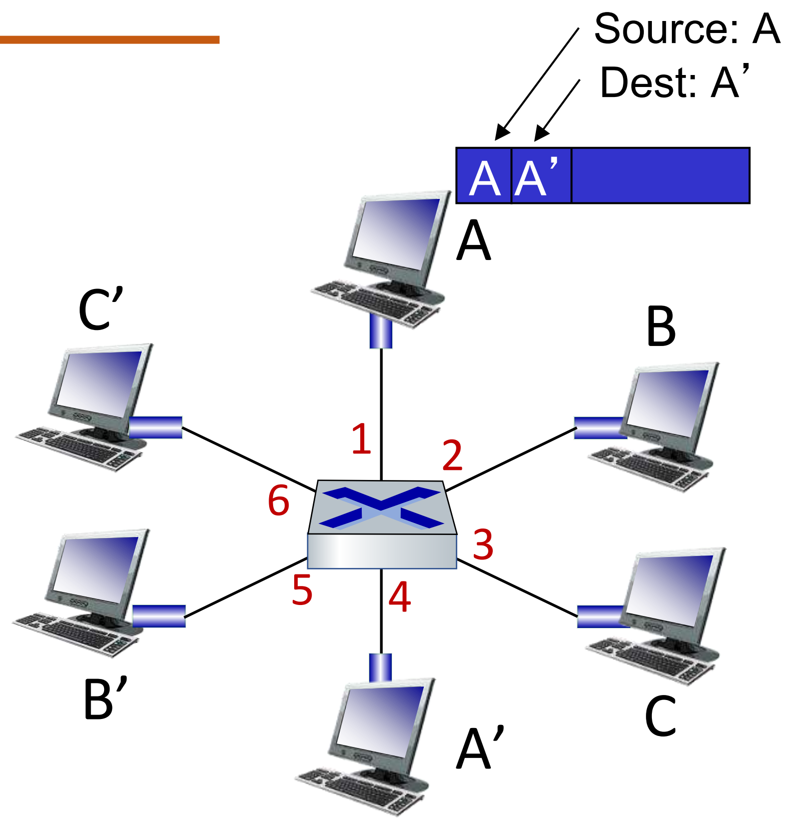


Q: How are entries created, maintained in switch table?

- 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

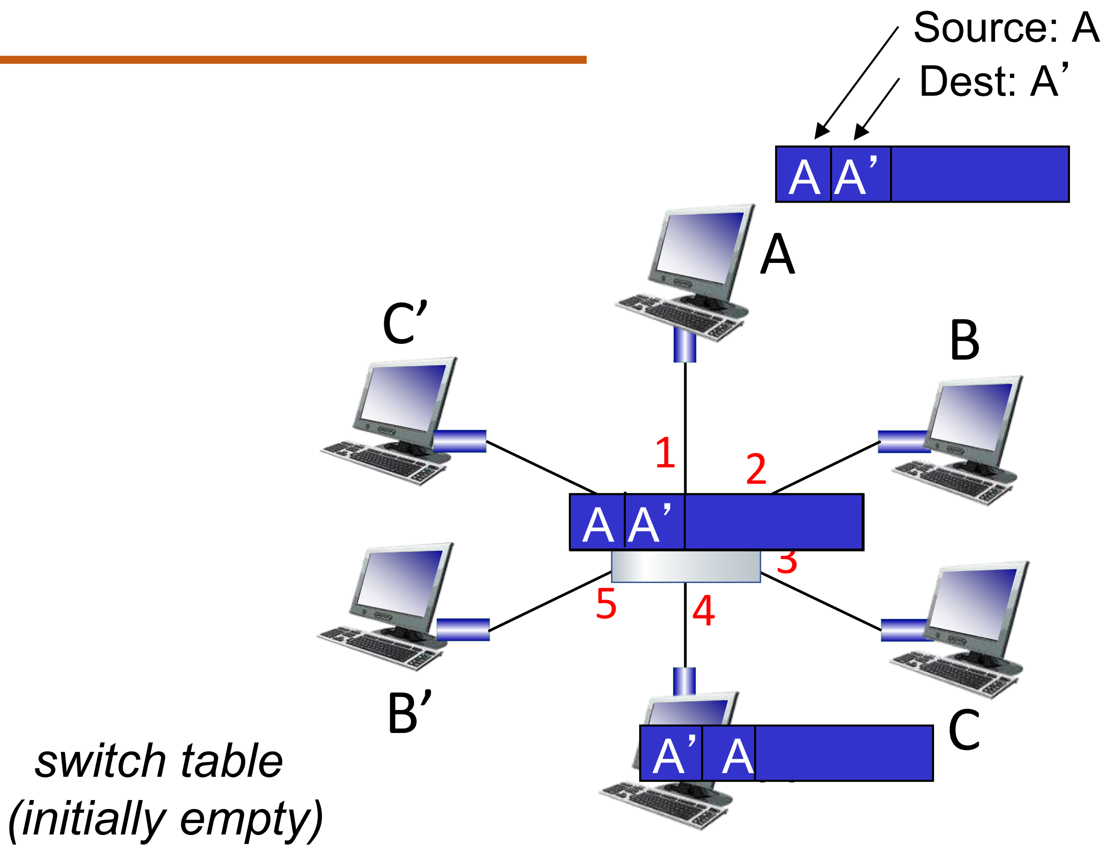
When frame received at switch:

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

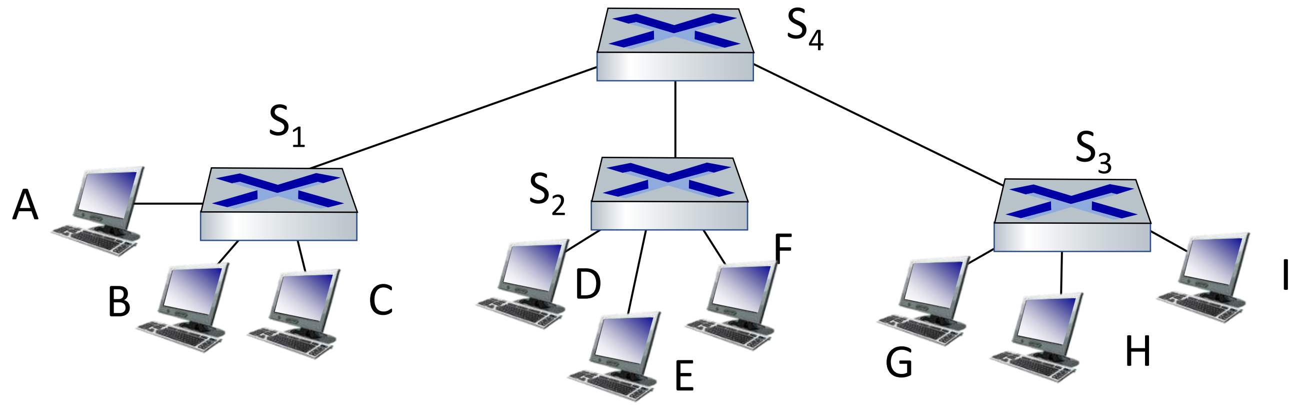
- Frame destination, A', location unknown: Flood
- Destination A location known: Selectively send on just one link

MAC addr	interface	TTL
A	1	60
A'	4	60



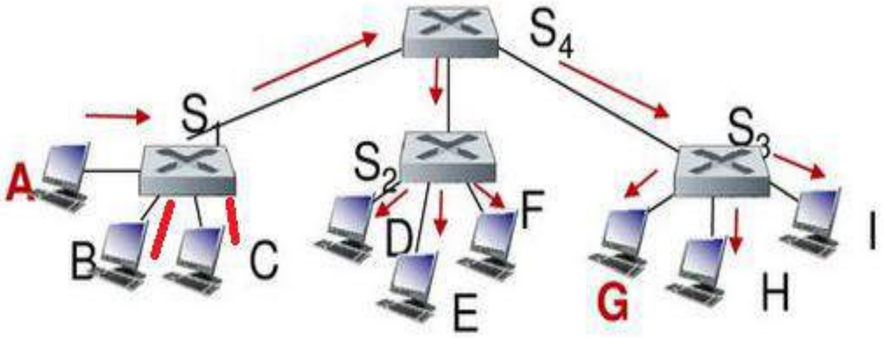
Interconnecting Switches

Self-learning switches can be connected together:



Q:

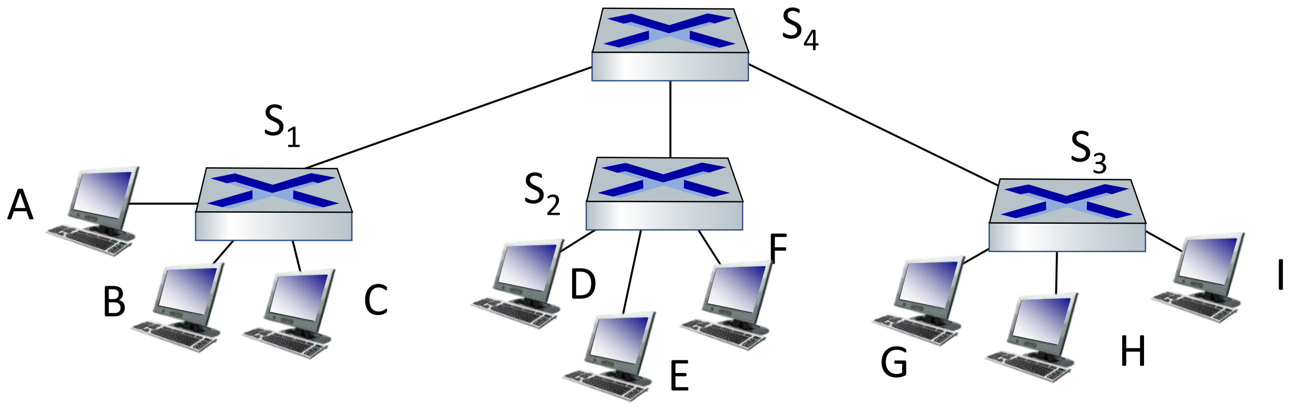
Sending from A to G – how does S_1 know to forward frame destined to G via S_4 and S_3?



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

Self-learning Multi-switch Example

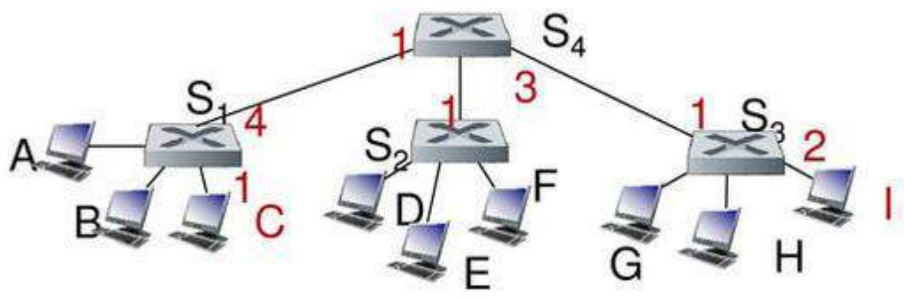
Suppose C sends frame to I, I responds to C



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

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

S1

Address	Port
C	1
I	4

S4

Address	Port
C	1
I	3

S3

Address	Port
C	1
I	2

S2

Address	Port
C	1

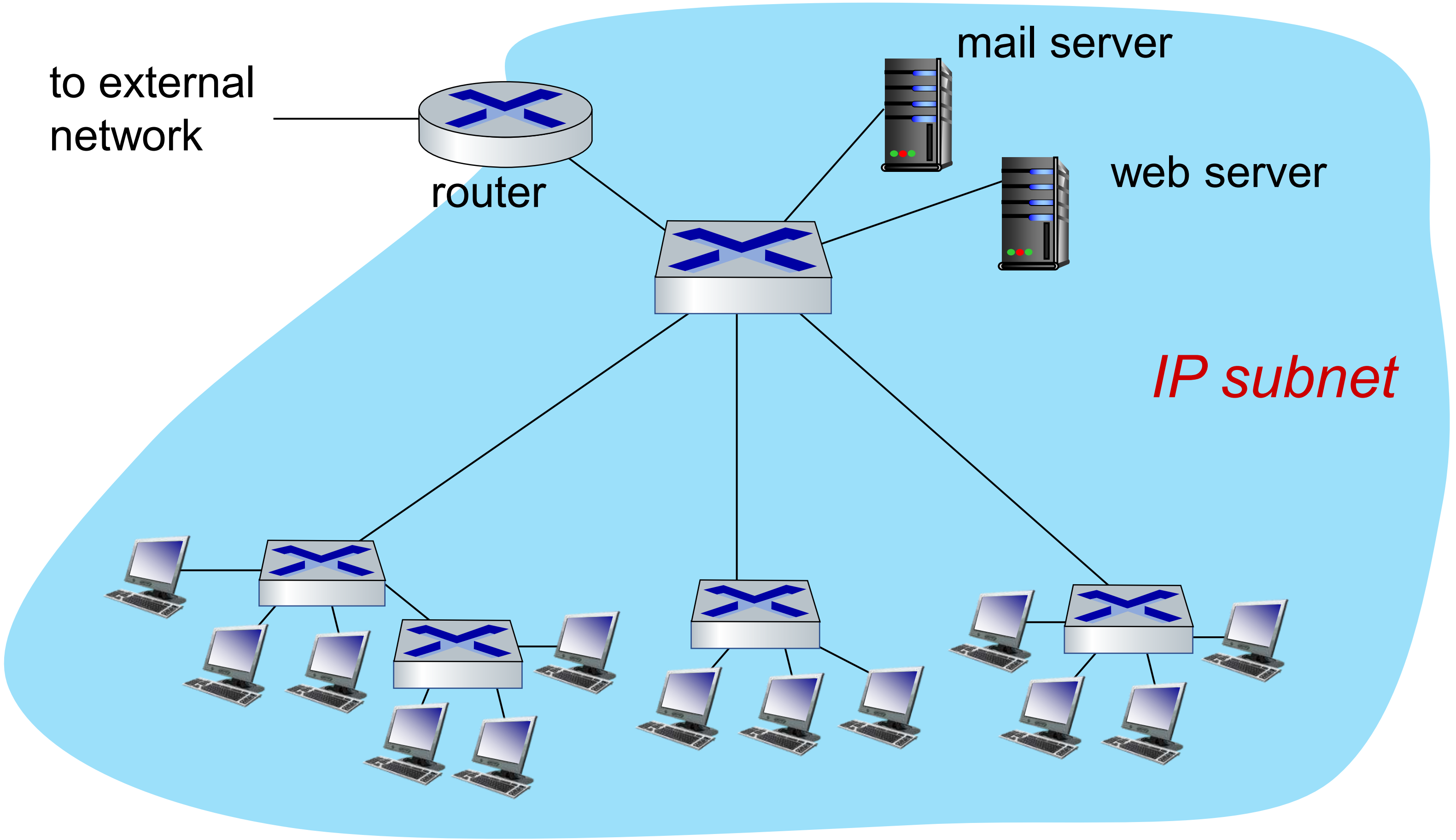
Properties of Link Layer Switching

- *Elimination of collisions*
  - In a LAN built from switches (and without hubs), there is no wasted bandwidth due to collisions!
  - buffer frames and never transmit more than one frame on a segment at any one time.
  - As with a router, the maximum aggregate throughput of a switch is the sum of all the switch interface rates.
  - provide a significant performance improvement over LANs with broadcast links.
- *Heterogeneous links*
  - Because a switch isolates one link from another, the different links in the LAN can operate at different speeds and can run over different media.
  - Example, three1 Gbps 1000BASE-T copper links, two 100 Mbps 100BASE-FX fiber links, and one 100BASE-T copper link.

Properties of Link Layer Switching

- *Management*
  - providing enhanced security,
  - eases network management
    - Example,
    - If an adapter malfunctions and continually sends Ethernet frames (called a jabbering adapter),
      - a switch can detect the problem and internally disconnect the malfunctioning adapter.
    - Similarly, a cable cut disconnects only that host that was using the cut cable to connect to the switch.
    - Gather statistics on bandwidth usage, collision rates, and traffic types, and make this information available to the network manager.
    - Used to debug and correct problems, and to plan future LAN

Small Institutional Network



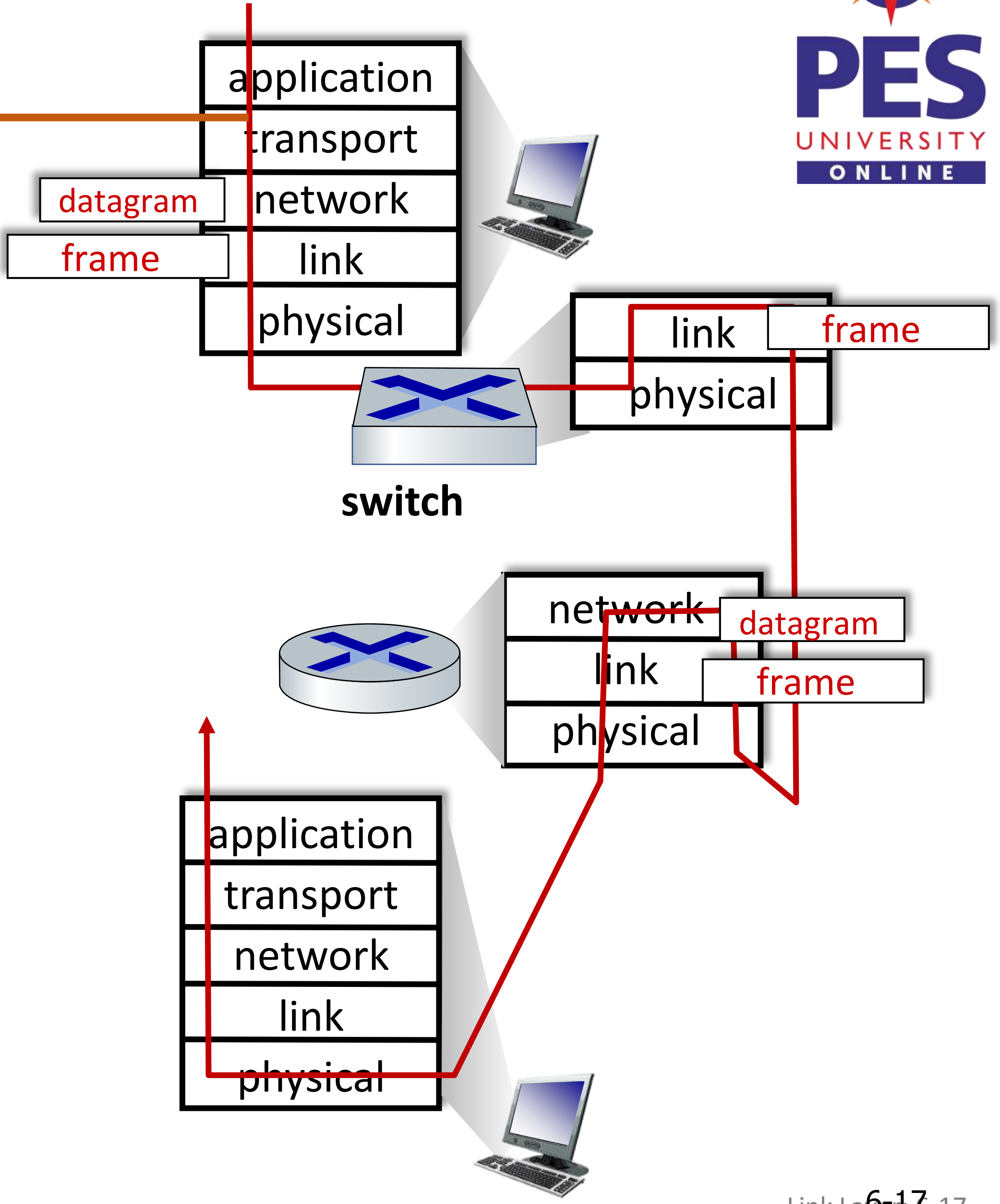
Switches Vs Routers

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



Switches Vs Routers

Switches

Pros

- plug-and-play
- relatively high filtering and forwarding rates
- prevent the cycling of broadcast frames, the active topology of a switched network is restricted to a spanning tree.

Cons

- large switched network would require large ARP tables in the hosts and routers and generate substantial ARP traffic and processing.
- susceptible to broadcast storms
- if one host goes haywire and transmits an endless stream of Ethernet broadcast frames, the switches will forward all of these frames, causing the entire network to collapse

Switches Vs Routers

Routers

Pros

- Because network addressing is hierarchical, packets do not normally cycle through routers even when the network has redundant paths.
- packets can cycle when router tables are misconfigured;
- IP uses a special datagram header field to limit the cycling.
- packets are not restricted to a spanning tree and can use the best path between source and destination.
- allowed the Internet to be built with a rich topology. Ex: multiple active links between Europe and North America.
- provide firewall protection against layer-2 broadcast storms.

Cons

- not plug-and-play—they and the hosts that connect to them need their IP addresses to be configured.
- Larger per-packet processing time than switches

Hubs Vs Switches Vs Routers

	Hubs	Routers	Switches
Traffic isolation	No	Yes	Yes
Plug and play	Yes	No	Yes
Optimal routing	No	Yes	No

Table 6.1 ♦ Comparison of the typical features of popular interconnection devices

THANK YOU

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
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
- Physical layer
- Wireless LANs: IEEE 802.11
- A day in the life of a web request

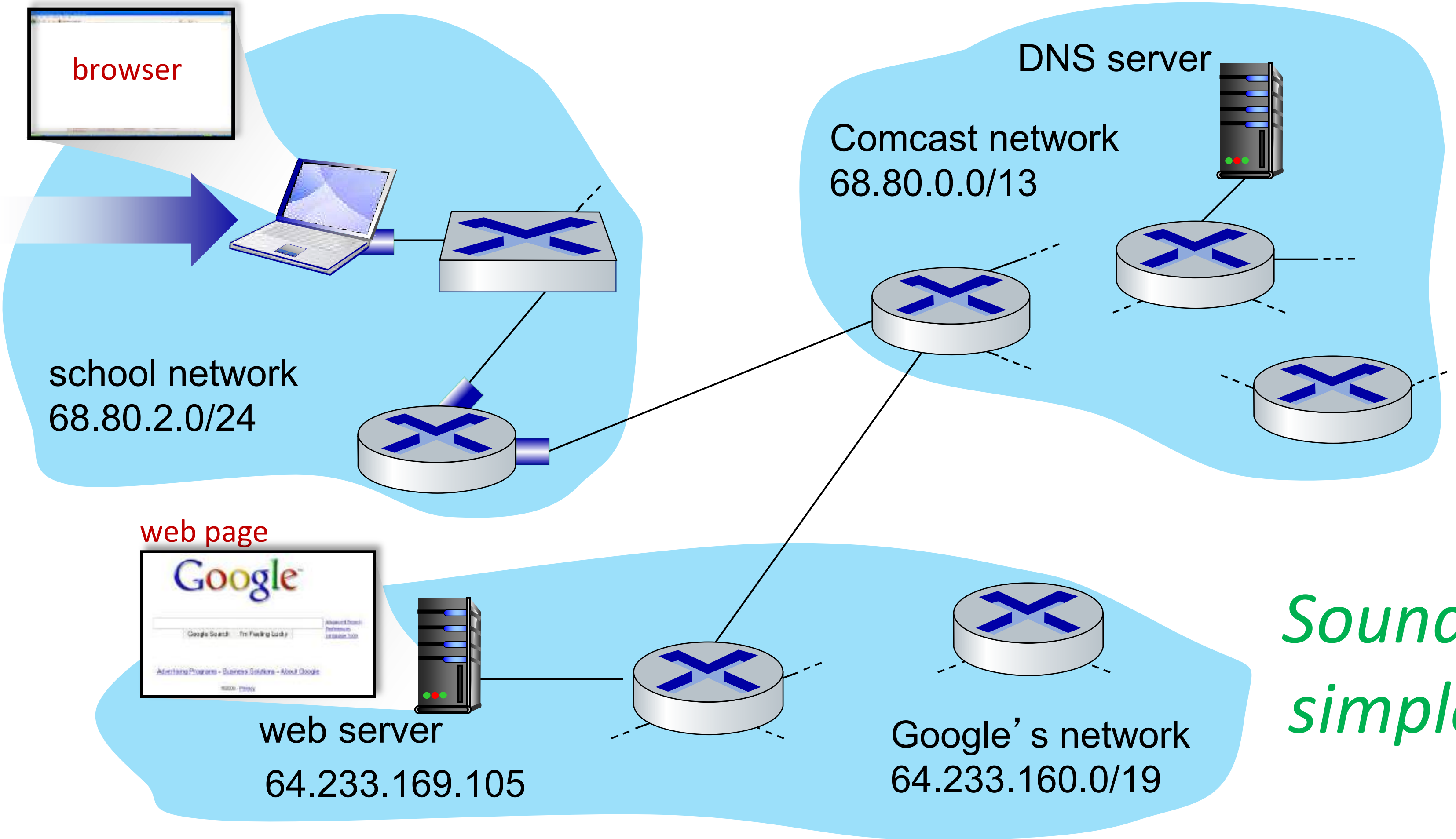
Class 56 : A day in the life of a web request : Learning Objectives

- 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

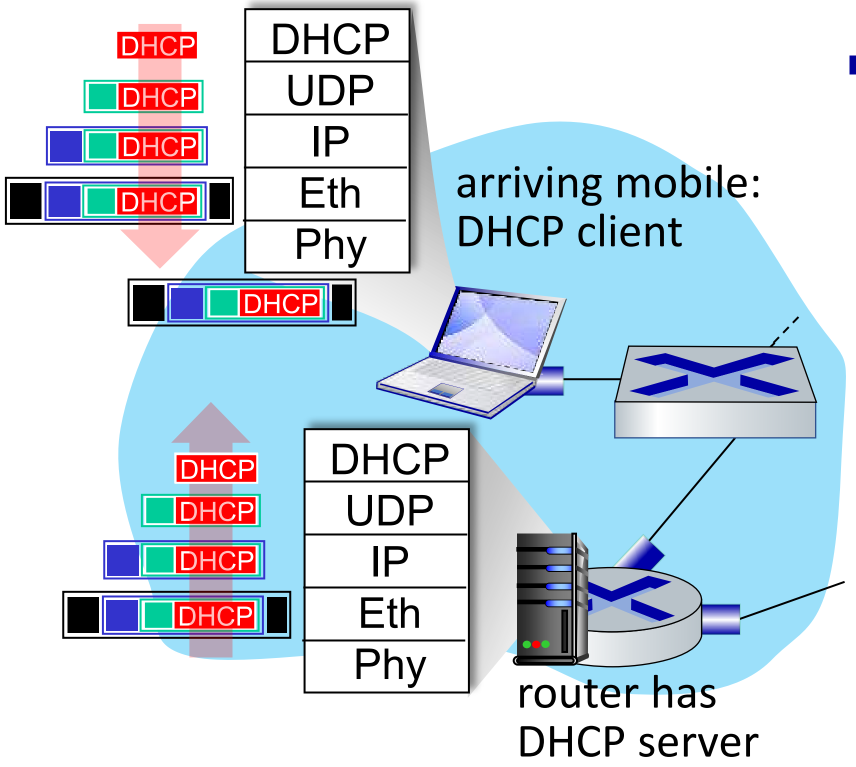


Scenario:

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

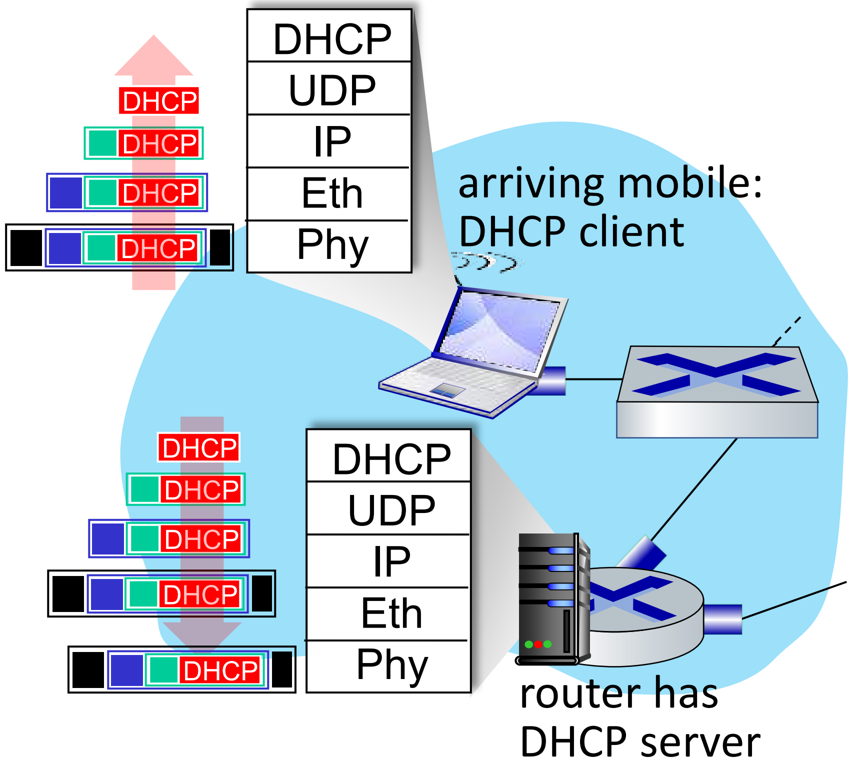
Sounds simple!

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

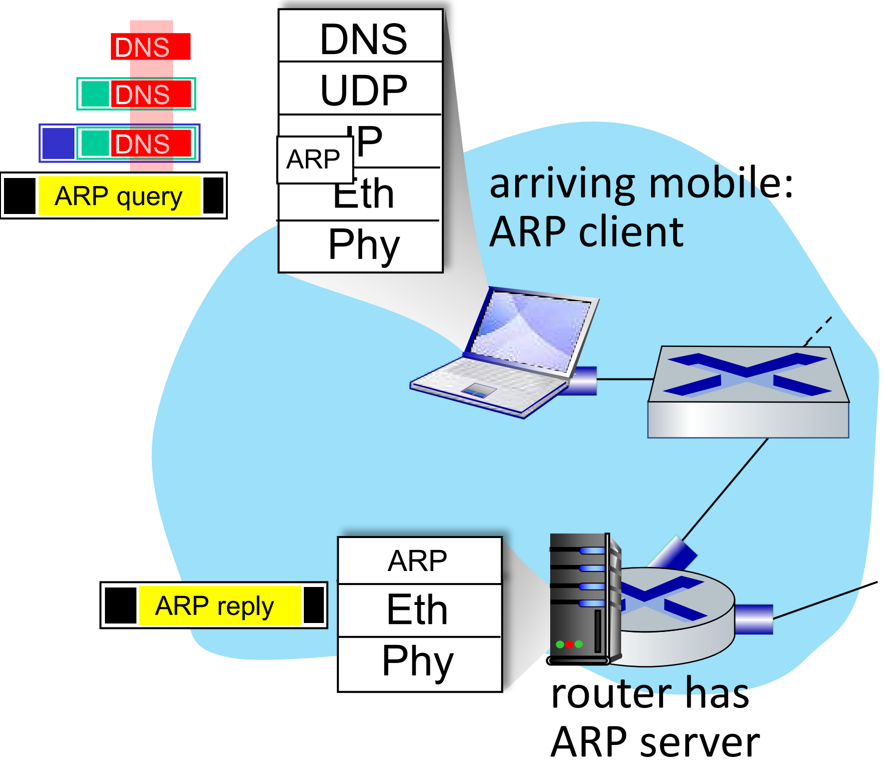
A day in the life : Connecting to the Internet



- 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

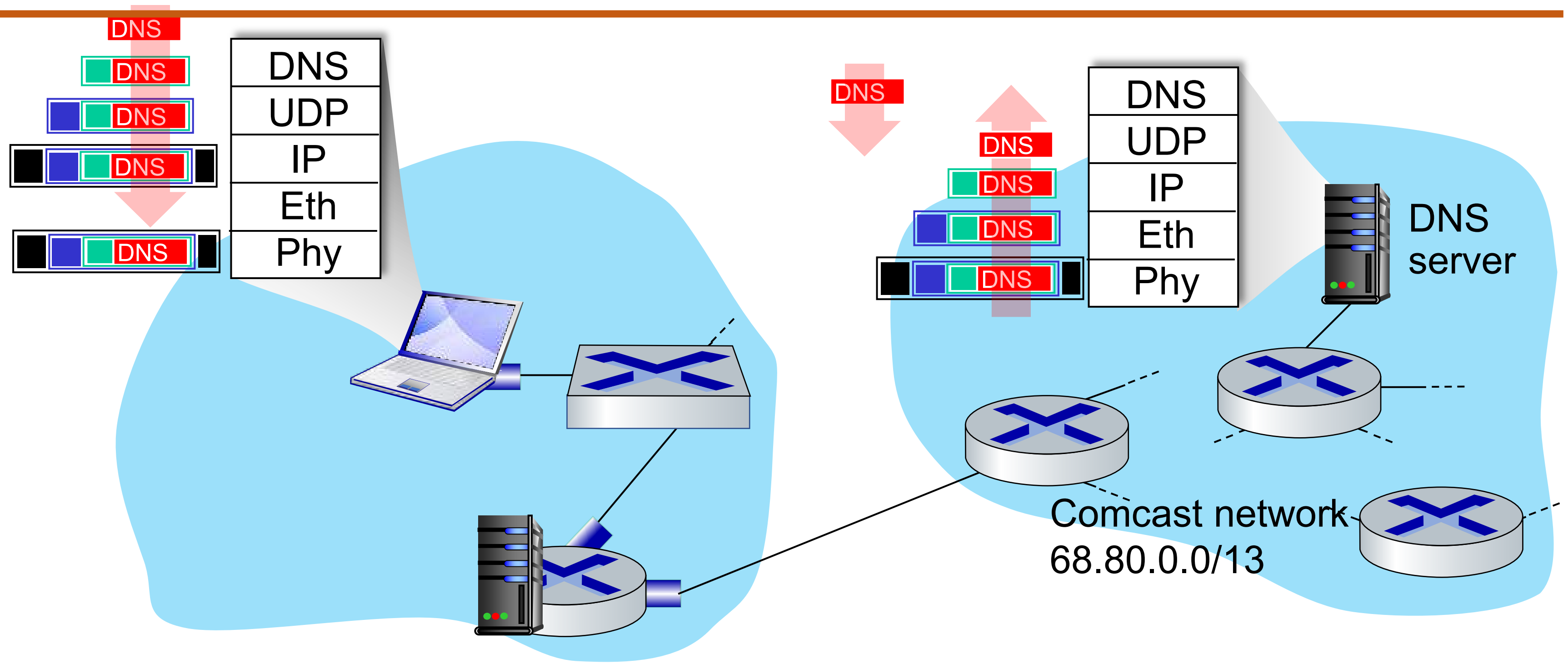
Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

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

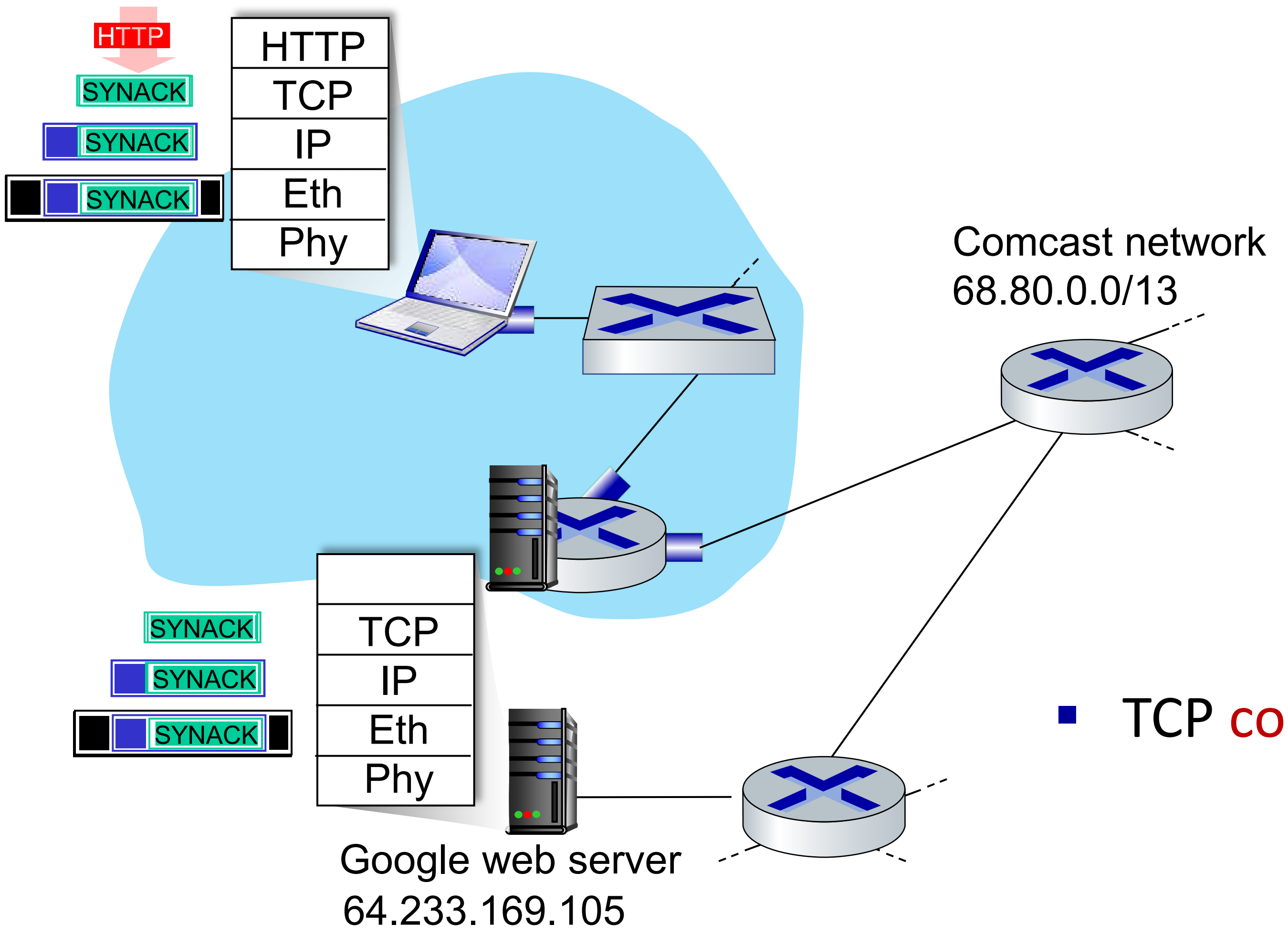
A day in the life…. Using DNS



- Demuxed to DNS
- DNS replies to client with IP address of www.google.com

- 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

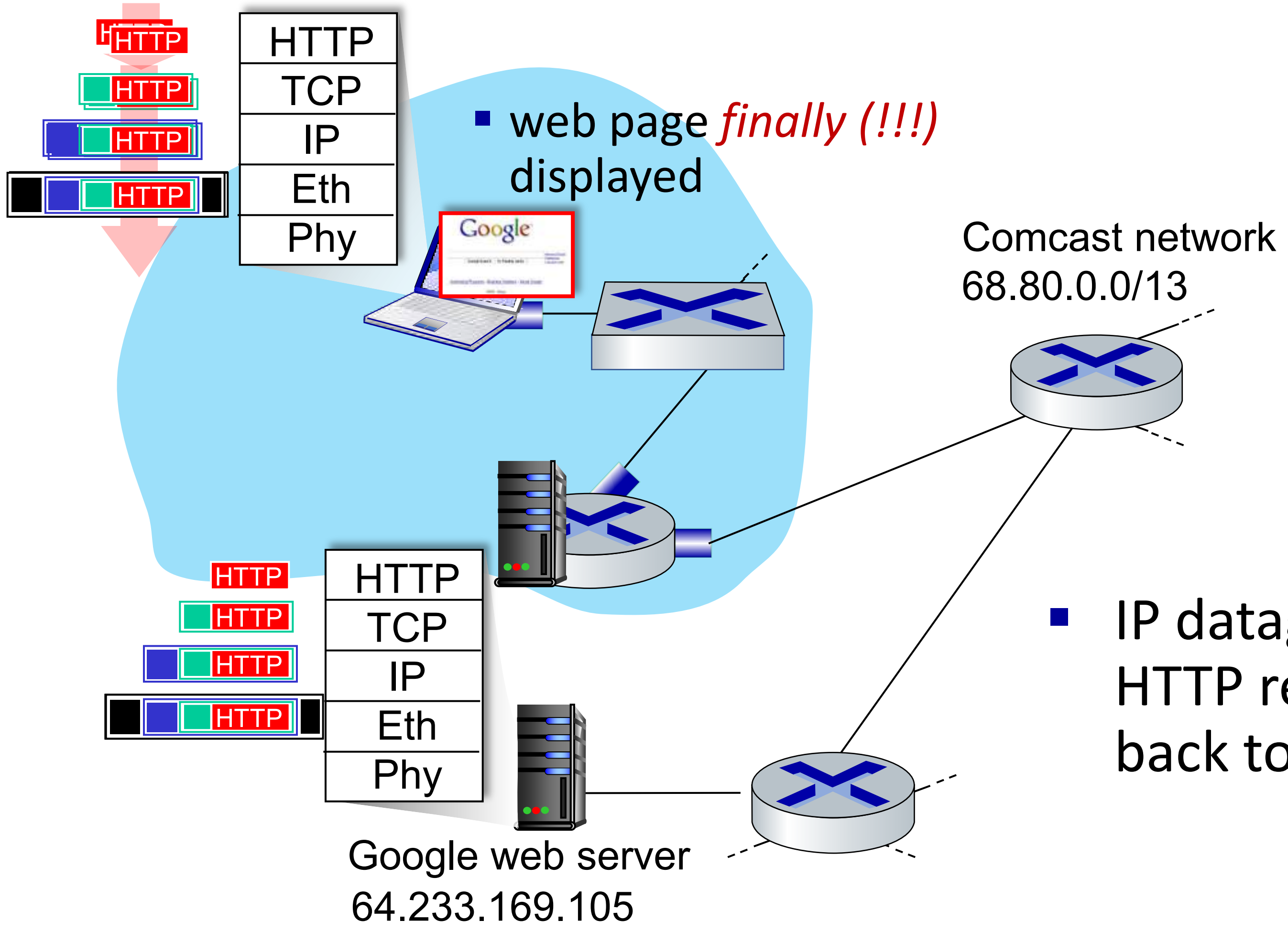
A day in the life.... TCP Connection carrying HTTP



- 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

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

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
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 53 : Intro to Physical layer : Learning Objectives

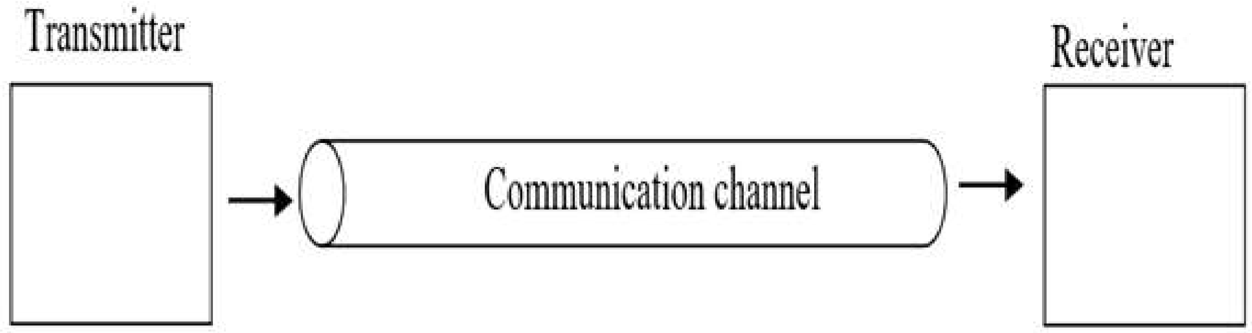
- Purpose
- Signals to Packets

Physical layer

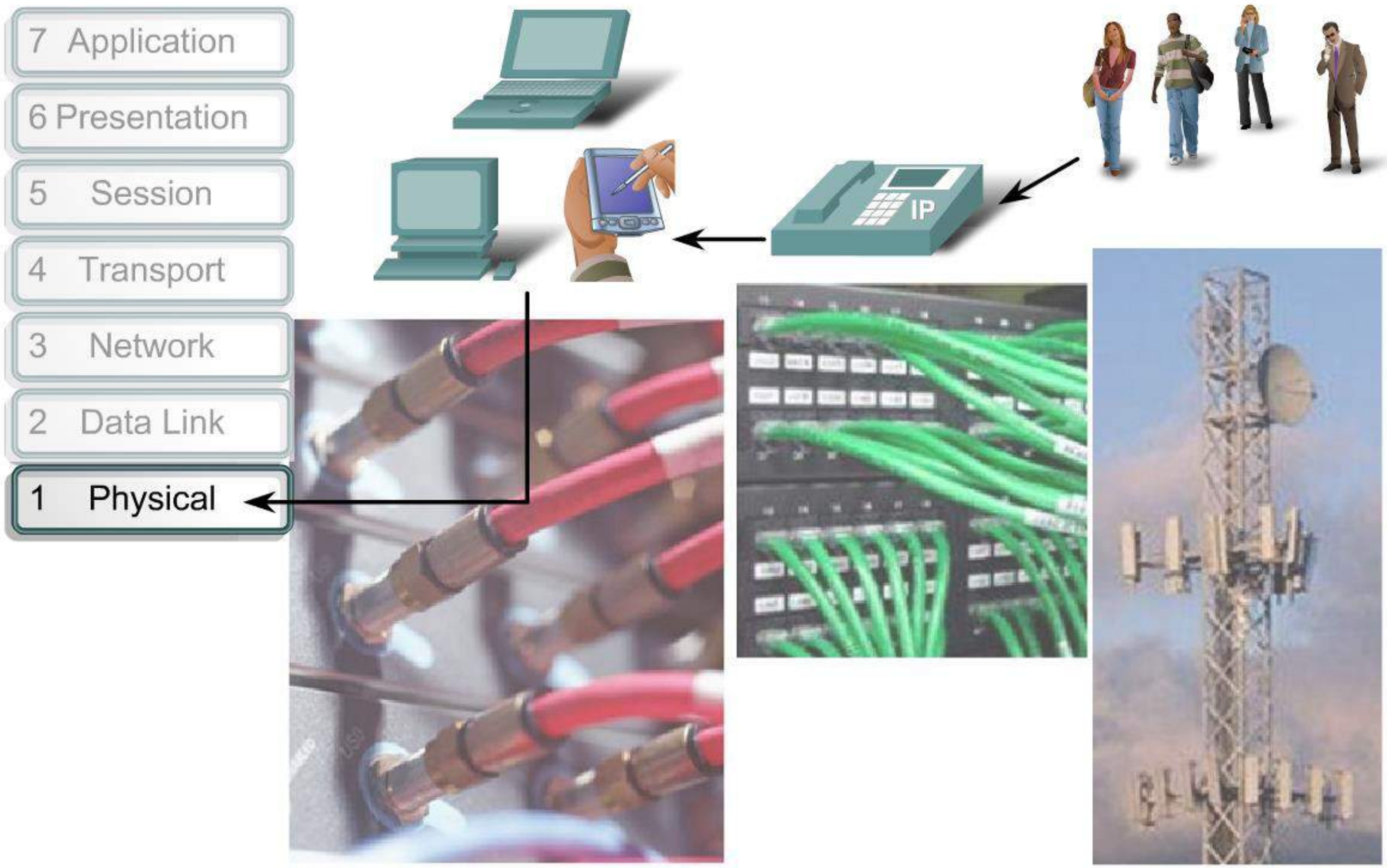
Role:

- encode the binary digits that represent data link layer frames into signals
- to transmit and receive these signals across the physical media
  - copper wires, optical fiber, and wireless that connect network devices.

Physical medium : capable of conducting a signal in the form of voltage, light, or radio waves from one device to another.



Physical layer

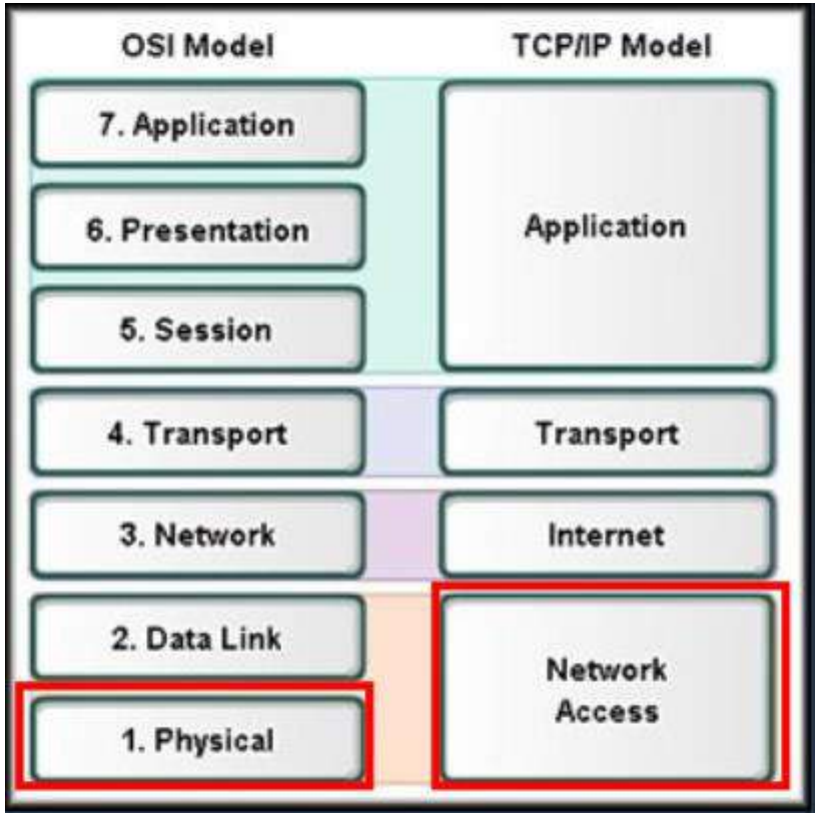


The Physical layer interconnects our data networks.

The Physical layer consists of hardware, in the form of

- electronic circuitry,
- media, and
- connectors.

Physical Layer

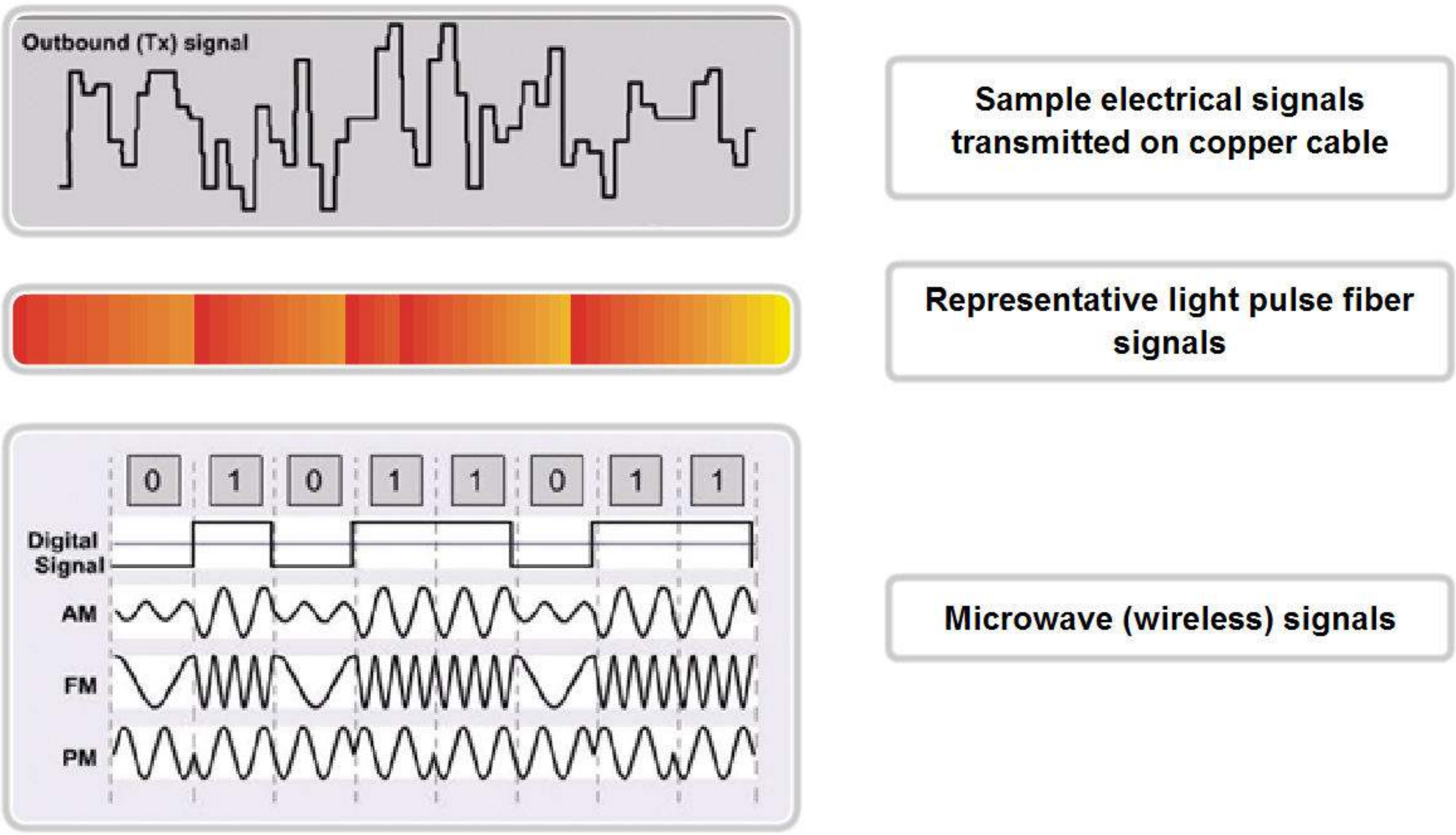


Purpose:

- *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

Physical Layer Operation

Representations of Signals on the Physical Media



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

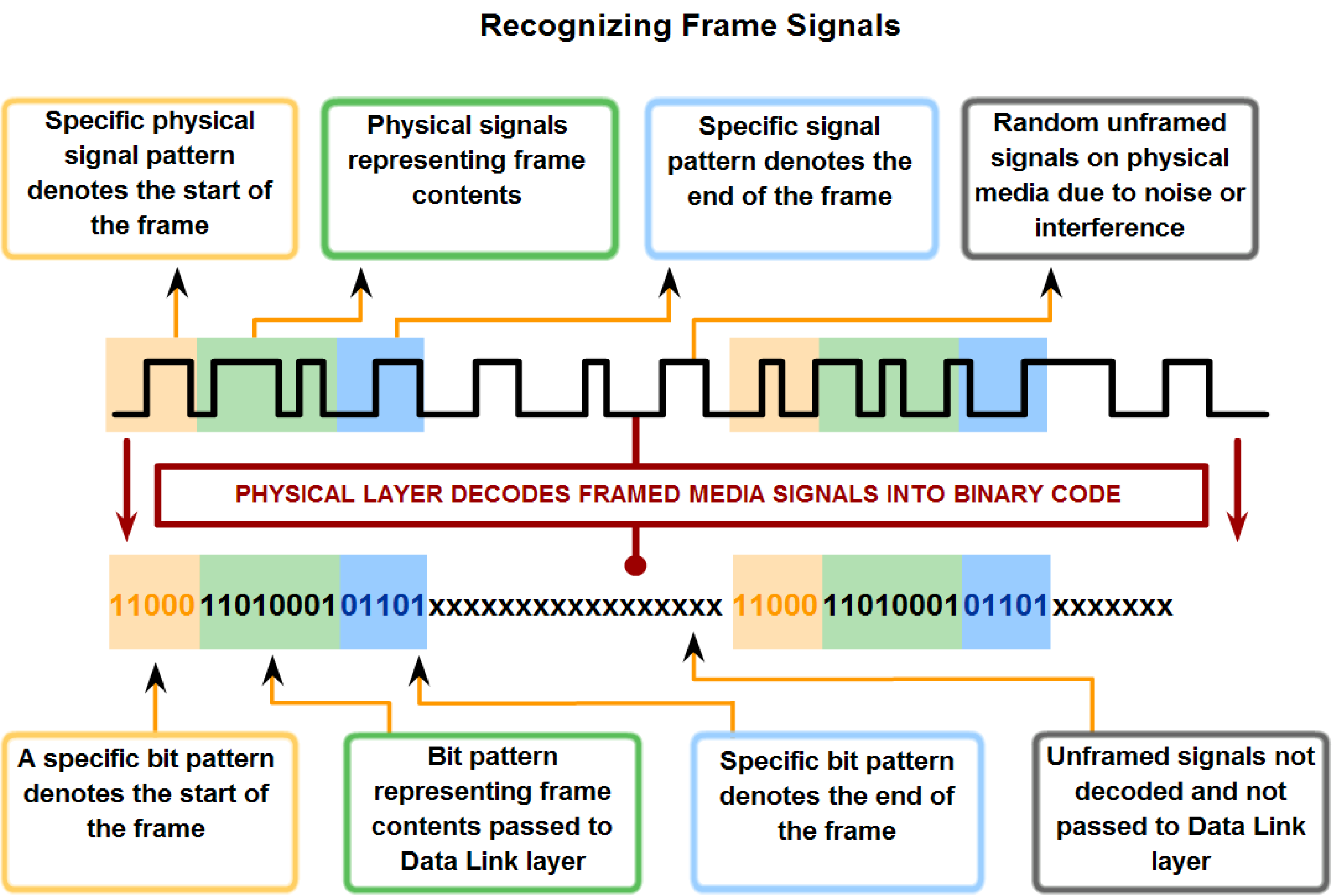
Table 8-1 Signal Types for Each of the Media at the Physical Layer

Media	Signal Type
Copper cable	Patterns of electrical pulses
Fiber-optic cable	Patterns of light pulses
Wireless	Patterns of radio transmissions

Physical Layer Operation

- When the physical layer puts a frame out onto media, it generates a set patterns of bits, or signal pattern, that can be understood by the receiving device.
- Many OSI Layer 1 technologies require the adding of signals at the beginning and the end of frames.
- To mark the beginning and end of frames, the transmitting device uses a bit pattern that is unique and is only used to identify the start or end of frames.

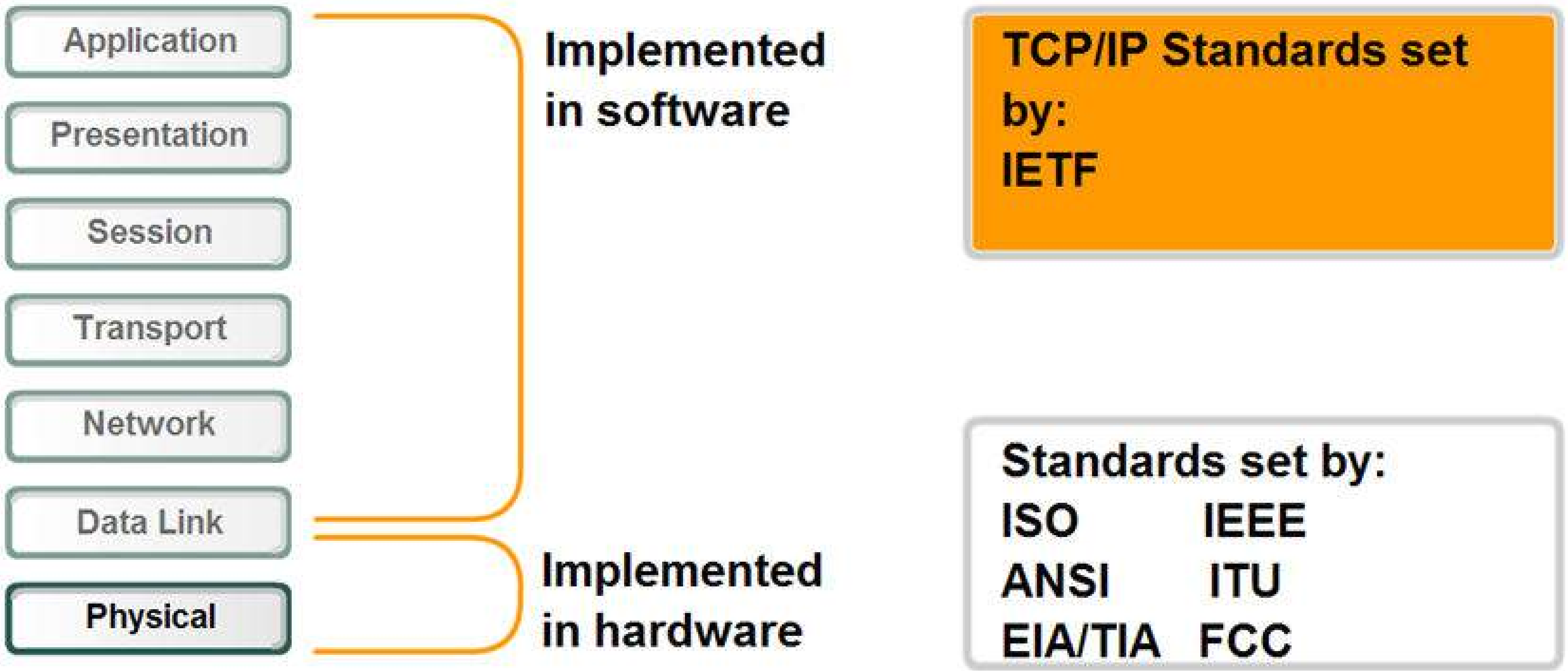
Physical Layer Operation



Key Challenge

- Digital computers
  - 0s and 1s
- Analog world
  - Amplitudes and frequencies

Physical Layer Standards



Physical Layer

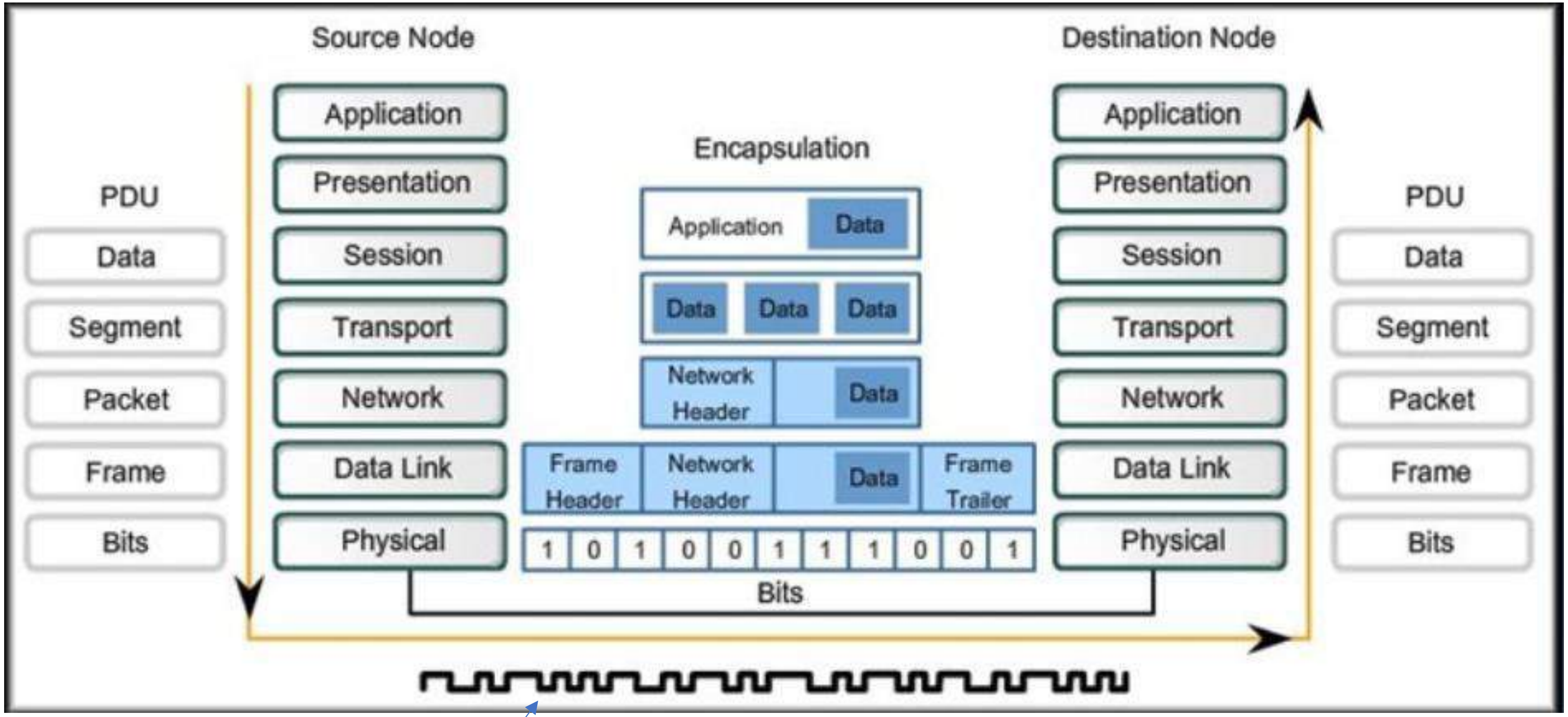
Hardware components such as

- 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

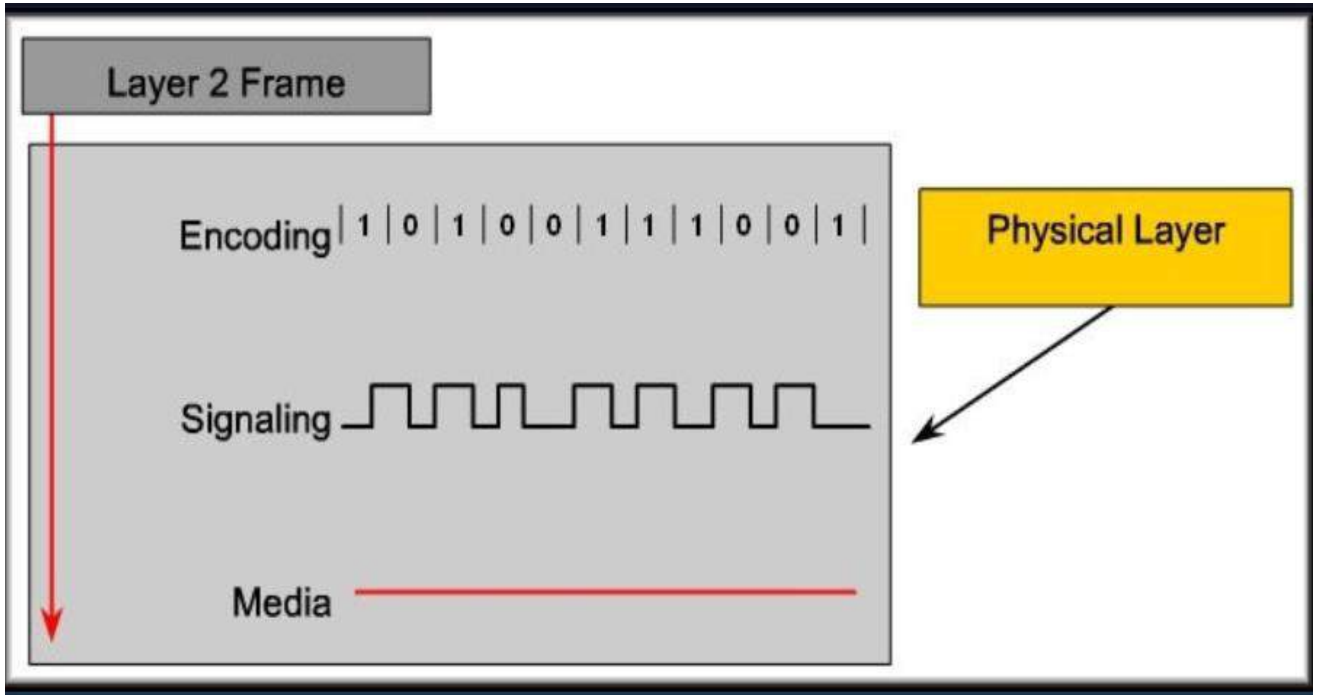
Physical Layer



Encoded signal

Physical layer Fundamental Principles

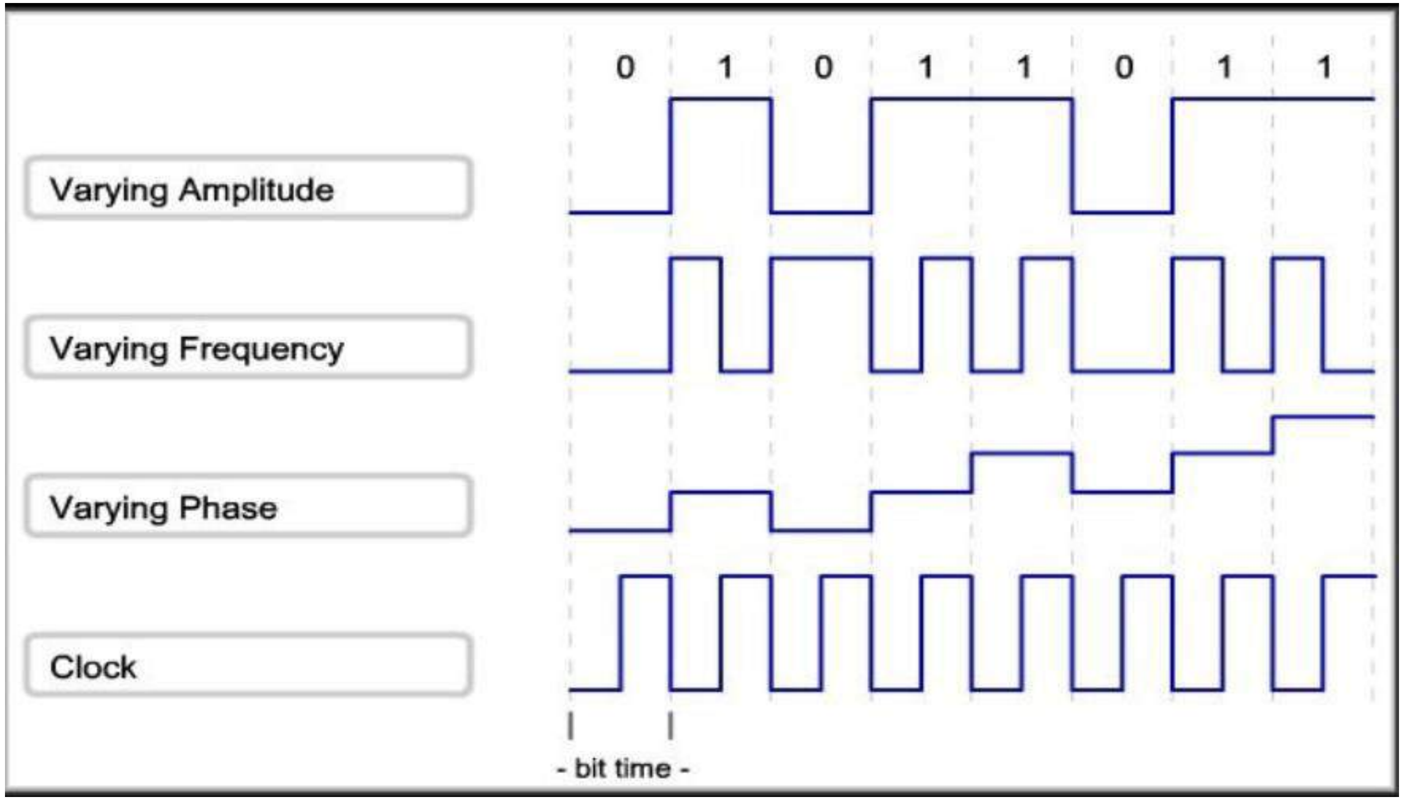
- The physical components
- Data encoding-Computing the stream of data bits from higher layers into a predefined code
- Signaling –Generation of the electrical/optical/wireless signals that represent the data bits

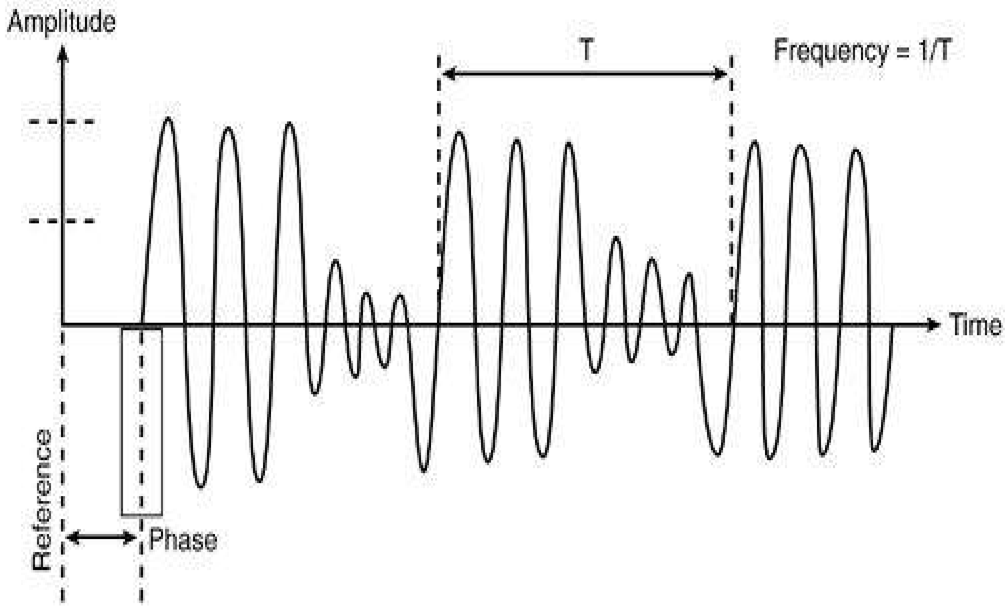


Signaling Bits for the Media

- *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
  - Bit time
    - Each signal has a specific amount of time to occupy the media
    - Each method finds a way to convert a pulse of energy into a defined amount of time
    - Time taken for a NIC at OSI Layer 2 to generate 1 bit of data and send it out to the media as a signal.

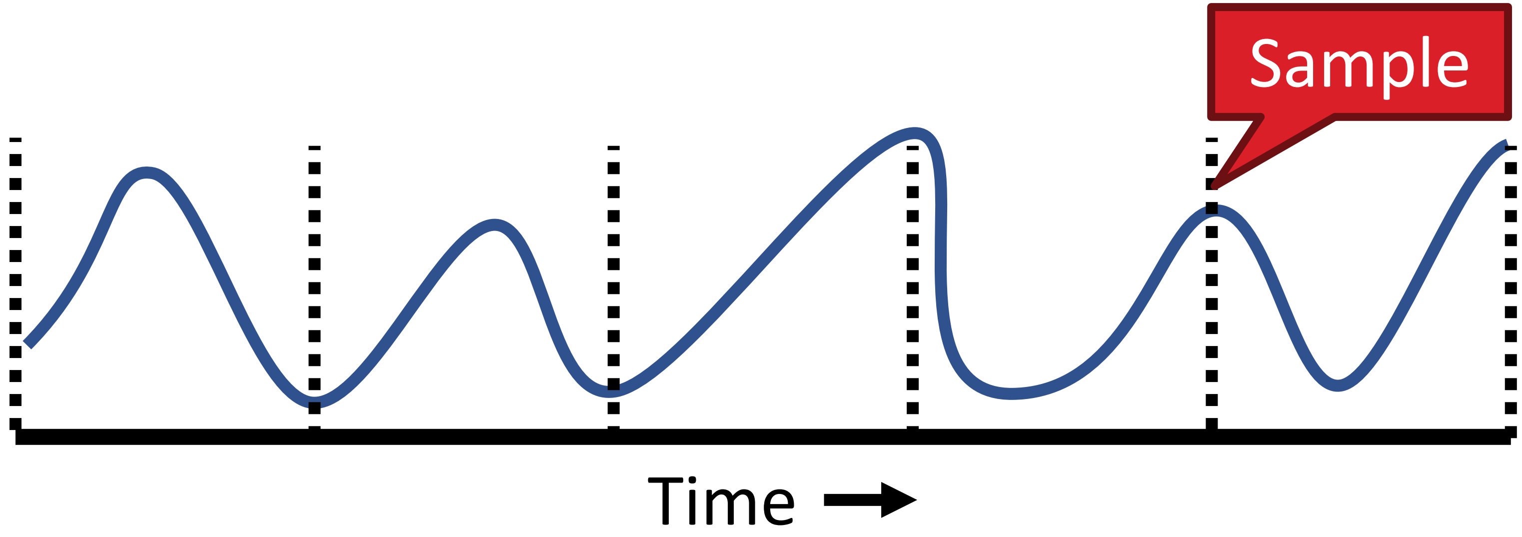
Signaling Bits for the Media





Assumptions

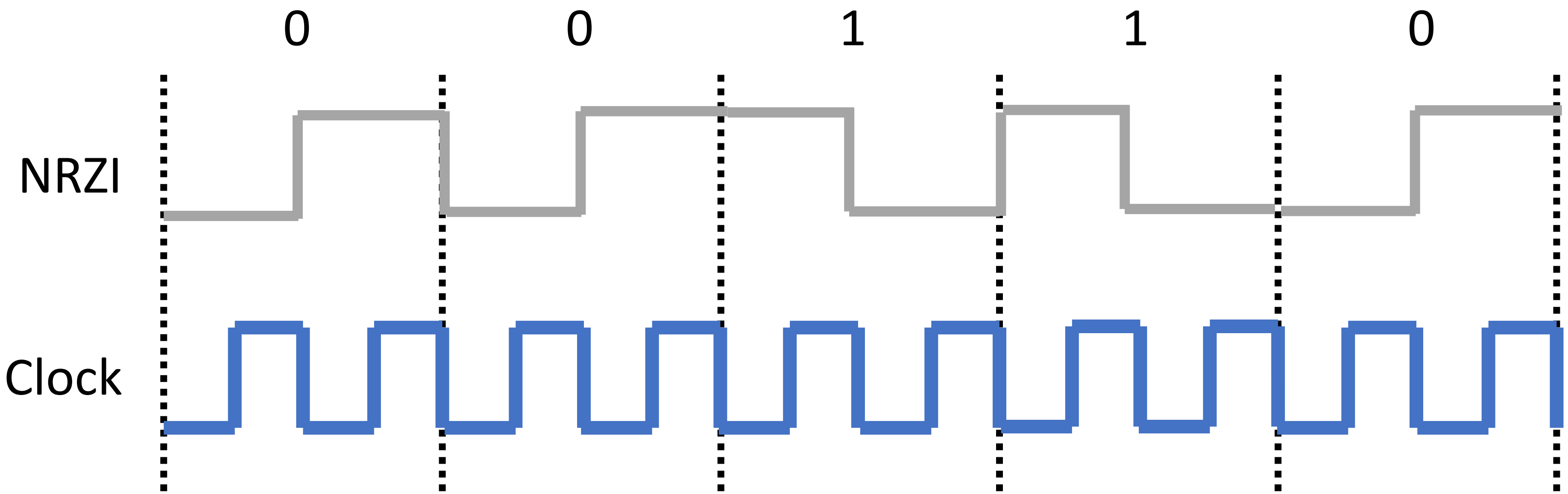
- We have two discrete signals, high and low, to encode 1 and 0
- Transmission is synchronous, i.e. there is a clock that controls signal sampling



- Amplitude and duration of signal must be significant

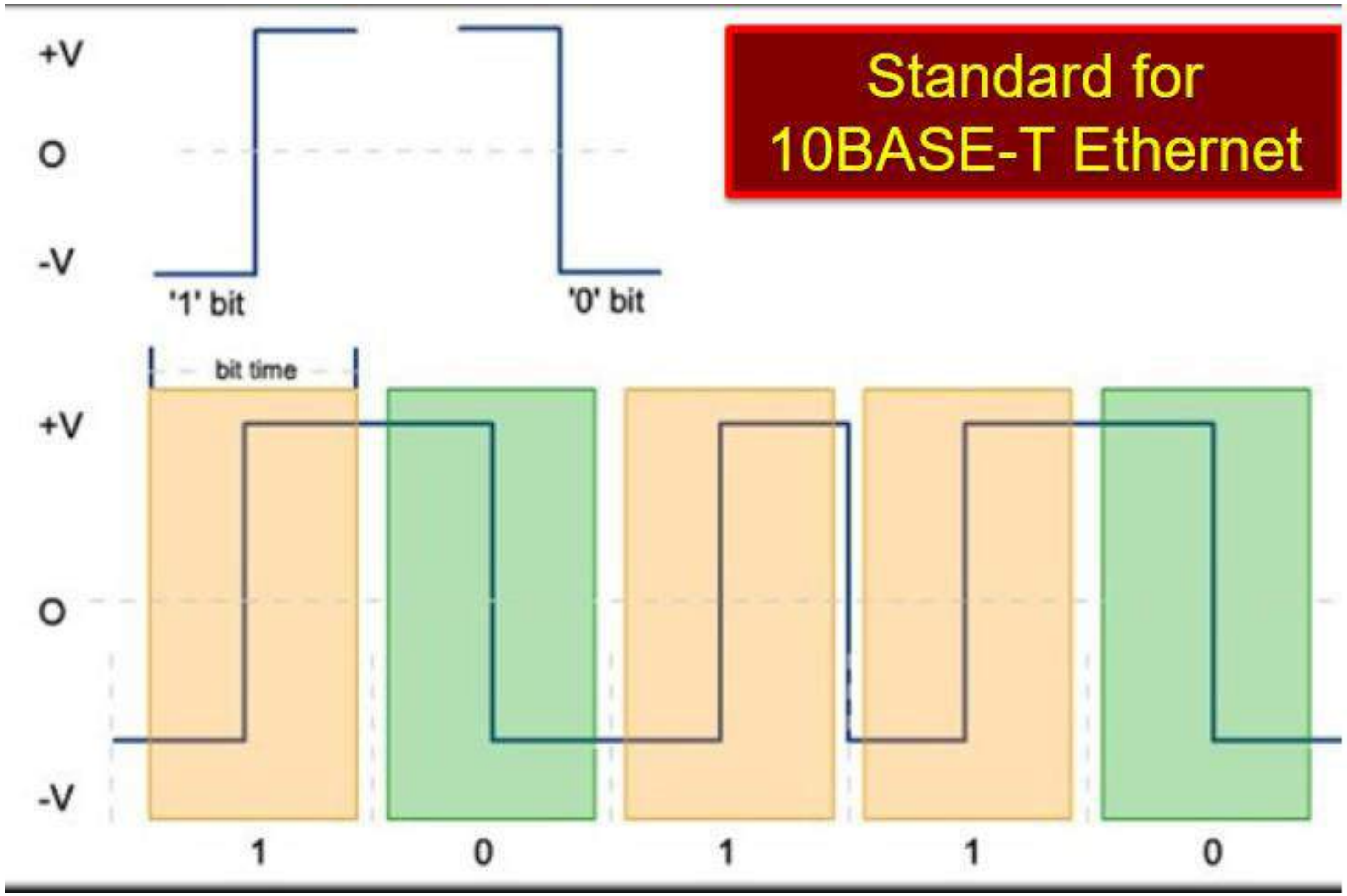
Manchester

- 1 → high-to-low, 0 → low-to-high



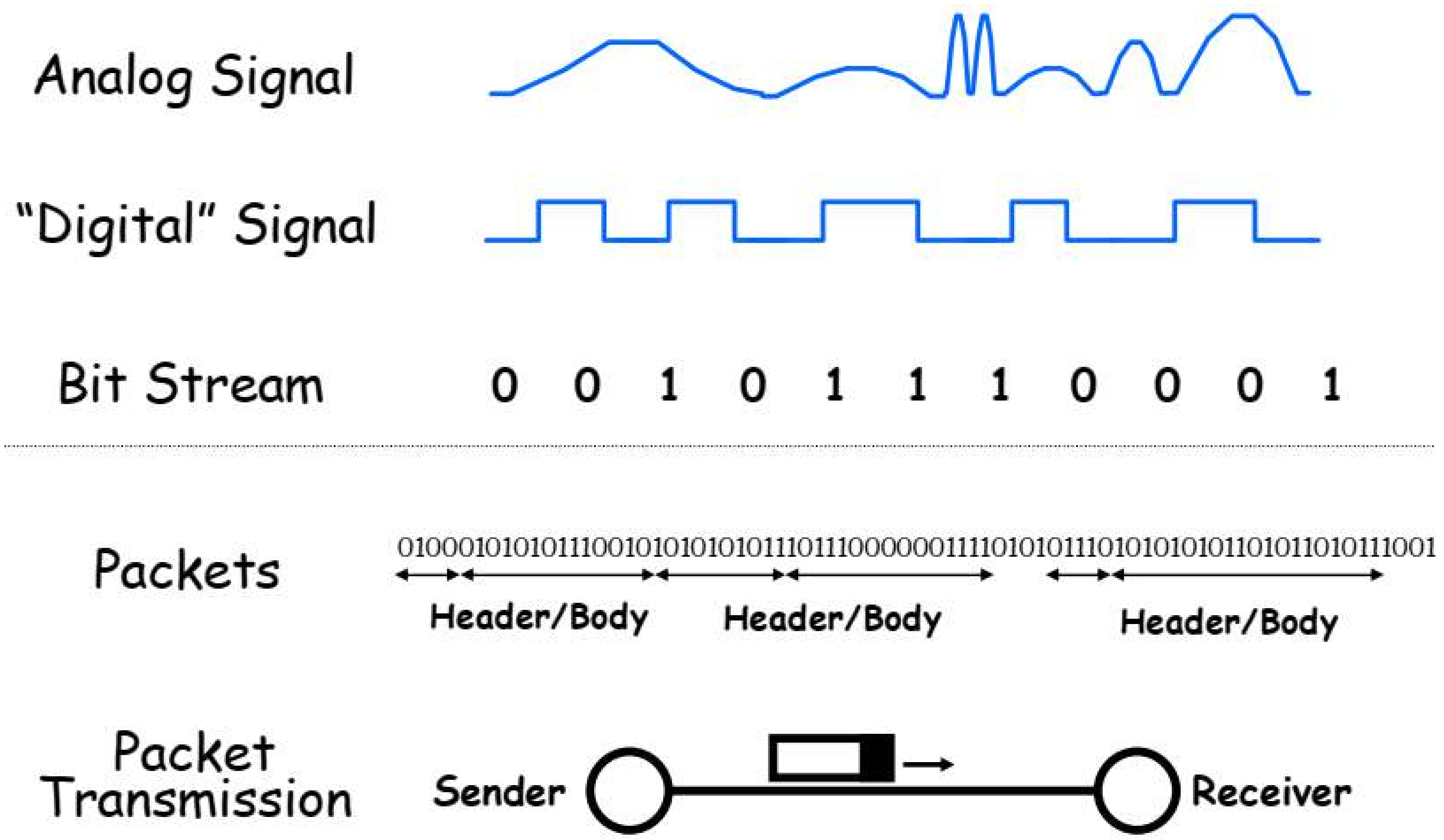
- Good: Solves clock skew (every bit is a transition)
- Bad: Halves throughput (two clock cycles per bit)

Manchester Encoding

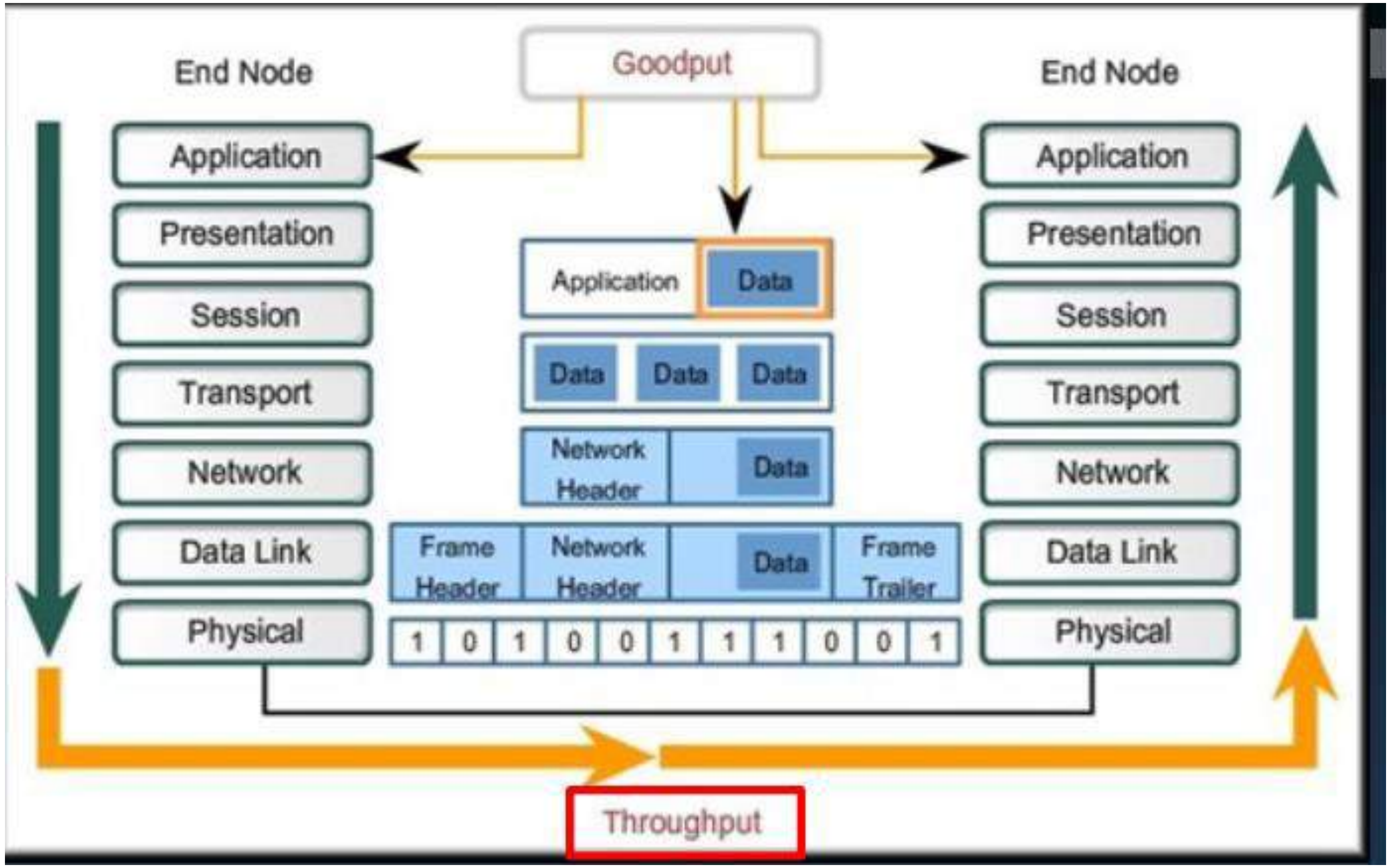


Manchester Encoding:
Uses the change in signal level in the middle of the bit time to represent the bits

Signals to Packets



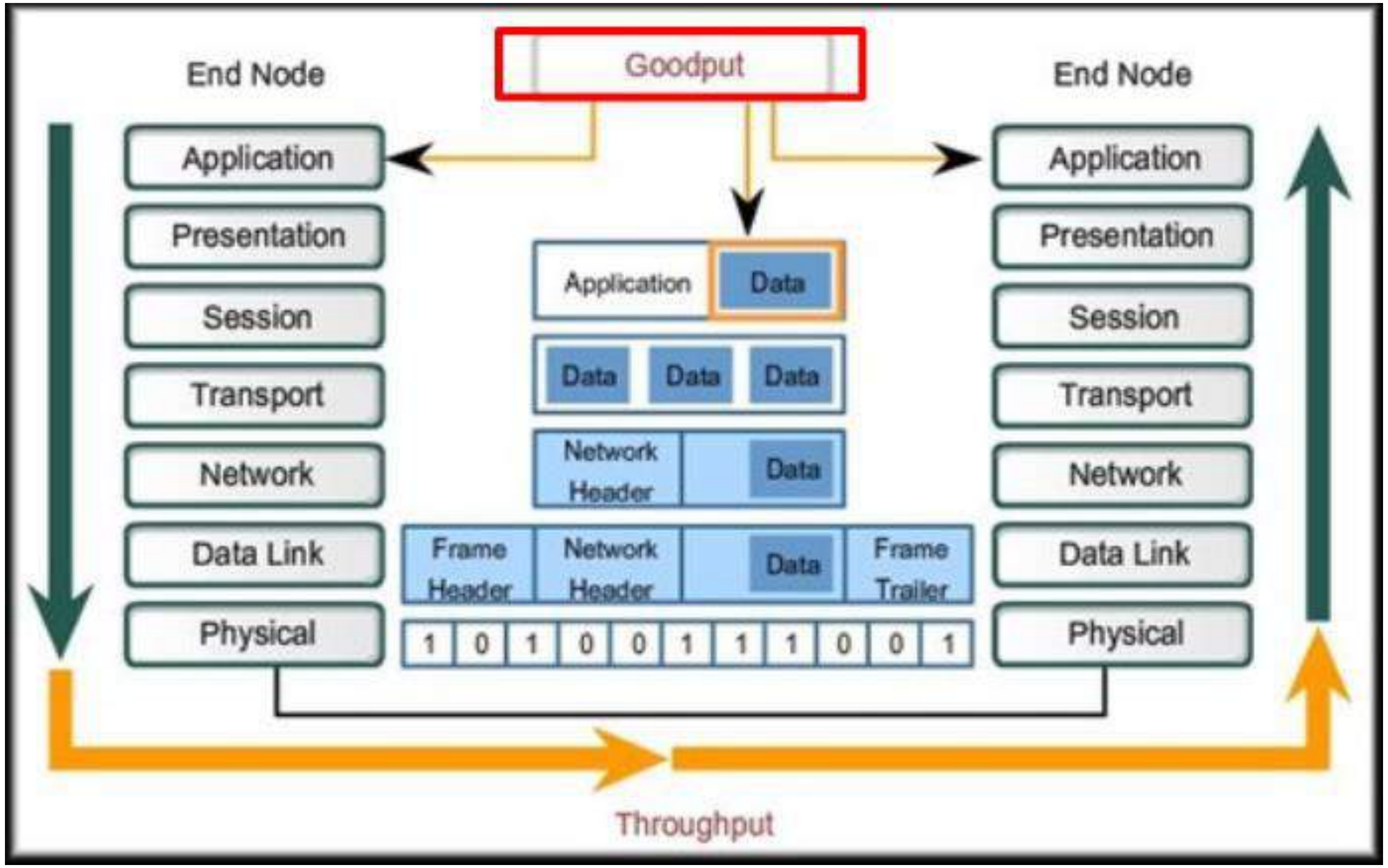
Data Carrying Capacity



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

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
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

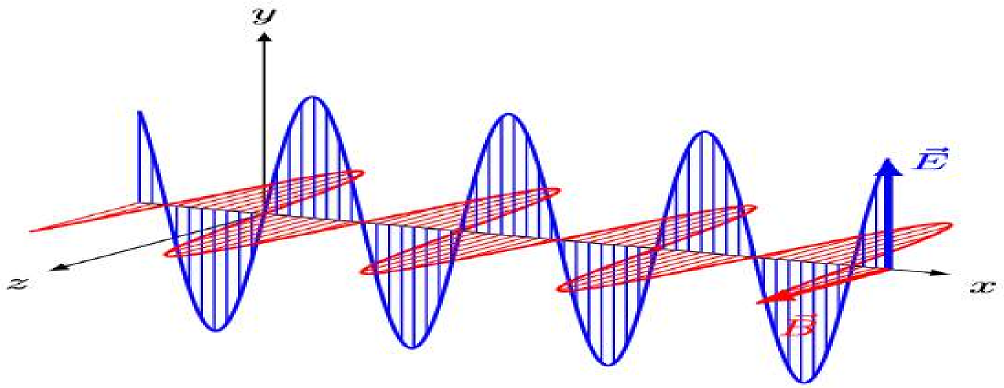
Class 54 : Physical layer : Learning Objectives

- Analog Vs Digital Signals
- Transmission Media

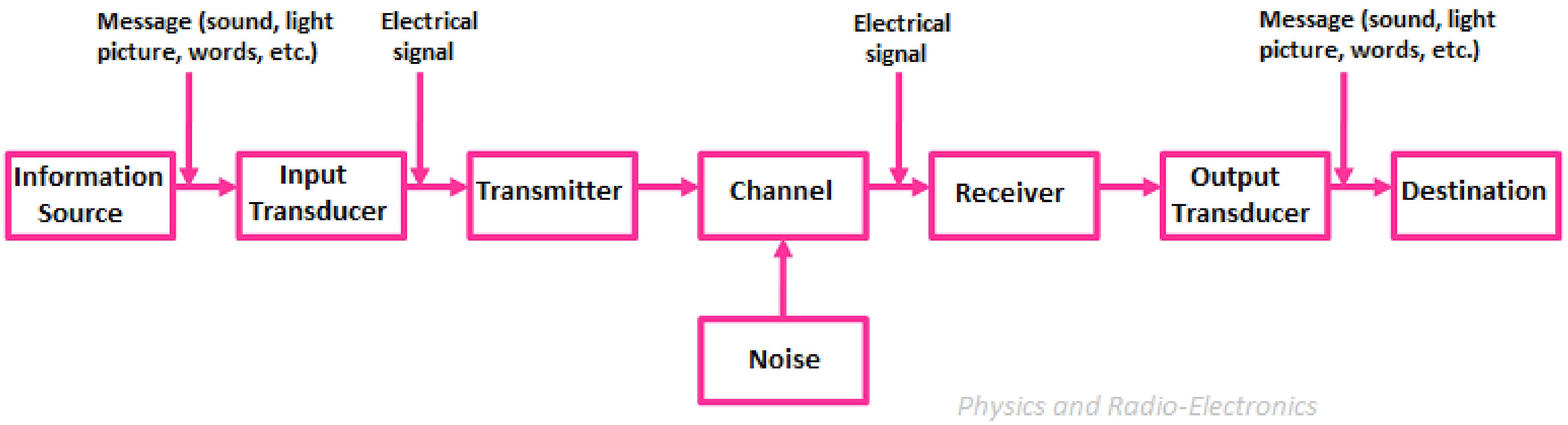
Signal

Signal

- function that conveys information
- electromagnetic or electrical current that carries data from one system or network to another.
- Signal may be Analog or Digital



Analog Communication System



- Any information may be conveyed by an analog signal;
- measured response to changes in a physical variable, such as sound, light, temperature, position, or pressure.
- physical variable is converted to an analog signal by a transducer

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.

Digital signal

A digital signal

- is a sequence of voltage pulses that may be transmitted over a copper wire medium;
- for example, a constant positive voltage level may represent binary 0 and
- a constant negative voltage level may represent binary 1.

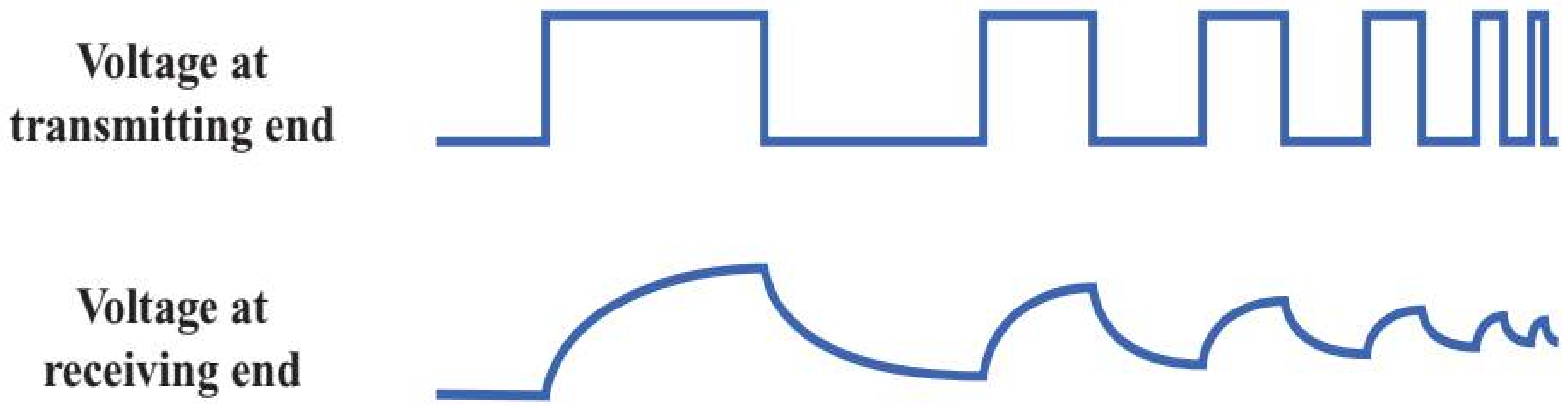
Analog and Digital signaling

The principal advantages of digital signaling

- generally cheaper
- less susceptible to noise interference.

The principal disadvantage is that digital signals

- suffer more from attenuation than do analog signals.



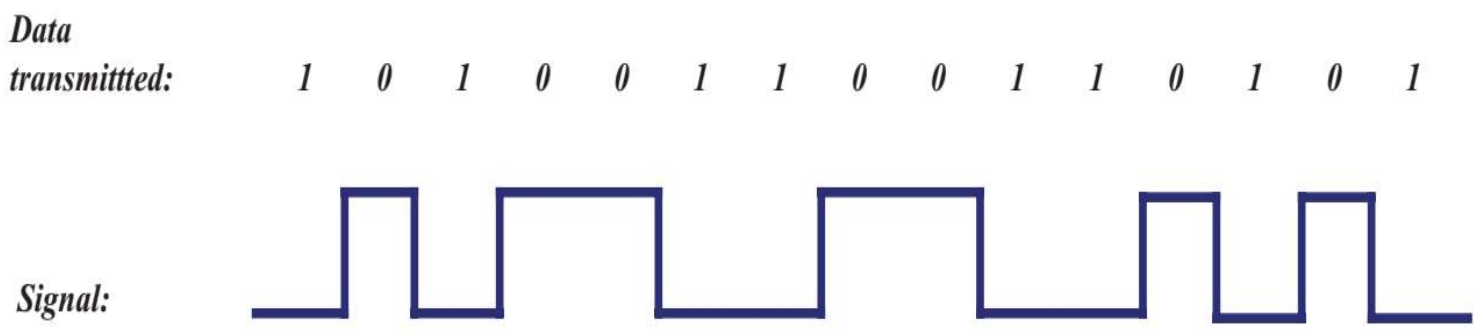
Analog and Digital Data

Analog data
take on continuous values in some interval.
Example:
voice and video are continuously varying patterns of intensity,
Most data collected by sensors, such as temperature and pressure

Digital data take on discrete values
Examples : text and integers.

Analog and Digital Data

- Data is defined as entities that convey meaning, or information.
- Signals are electric or electromagnetic representations of data.
- Transmission is the communication of data by the propagation and processing of signals.



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).

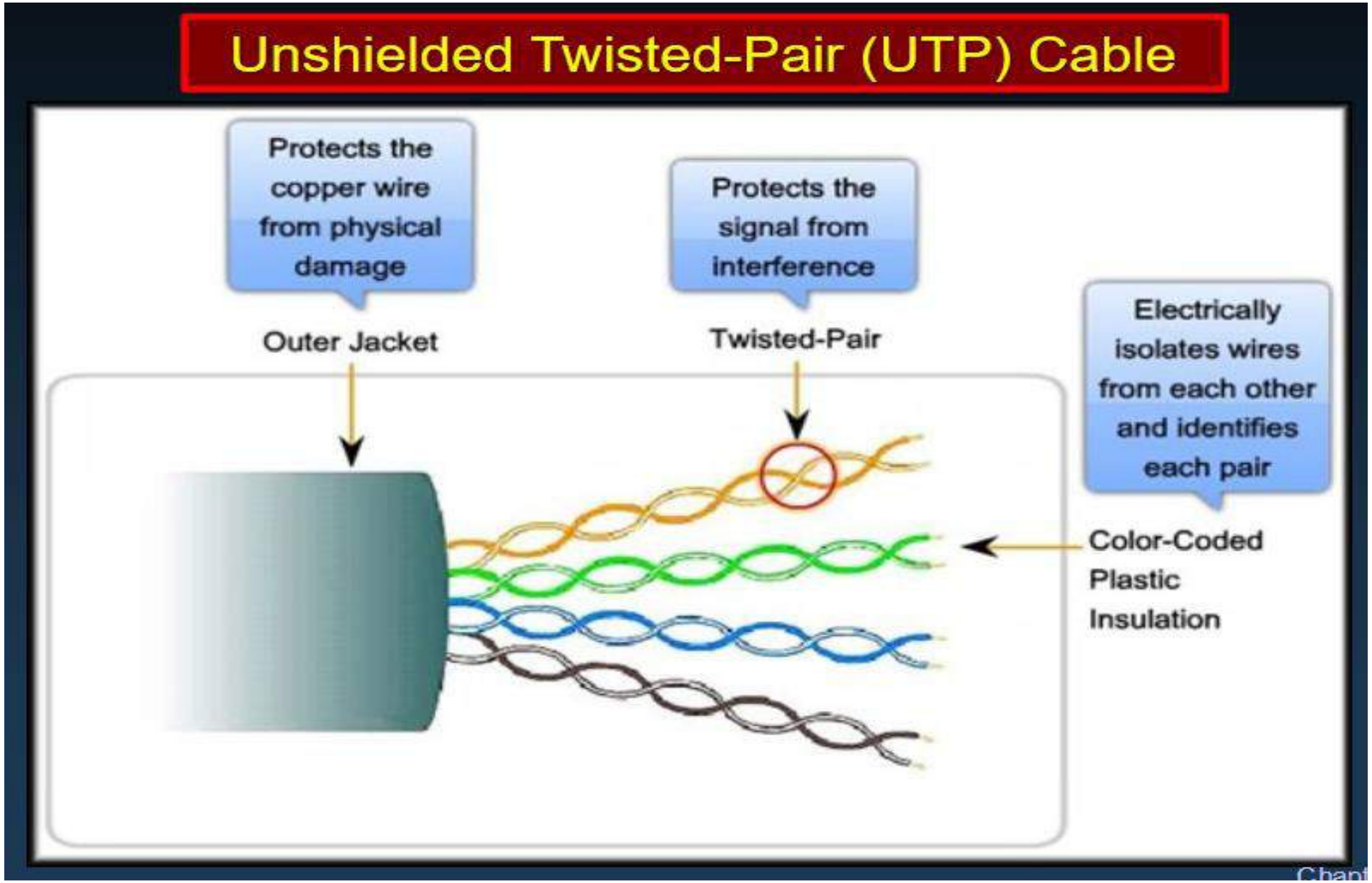
Types of Physical Transmission Media

- 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	

Copper Media



Copper Media

- The colored pairs identify the wires for proper connection at the terminals.
- There are several categories of UTP cable. Each category indicates a level of bandwidth performance as defined by the IEEE.
- Category 3 (Cat 3) to Category 5 (Cat 5), 100-megabit transmissions.
- In 1999, Cat 5e, full-duplex Fast Ethernet gigabit
- In 2002, Category 6 (Cat 6). Allow higher performance and less crosstalk.

Copper Media

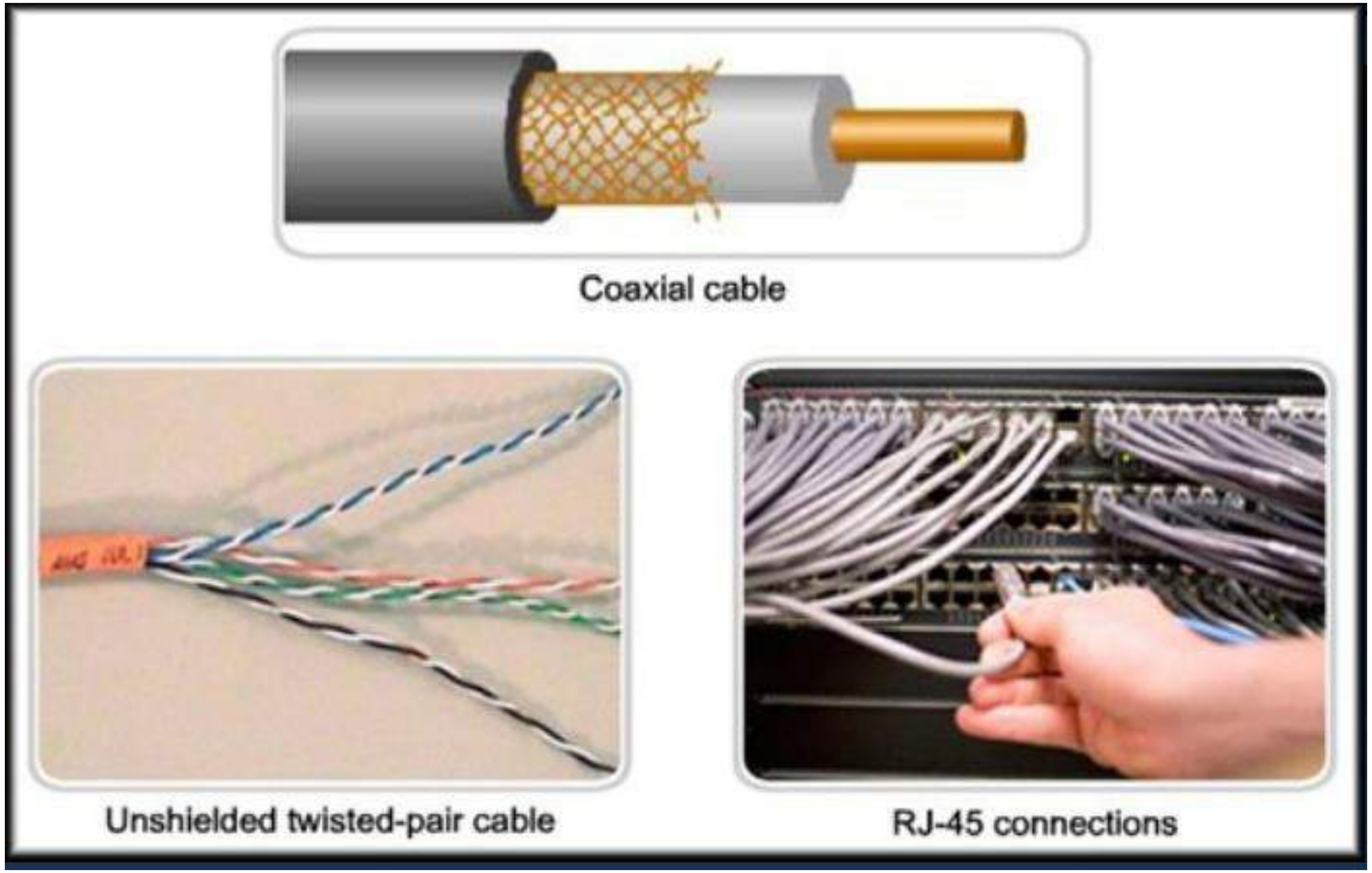
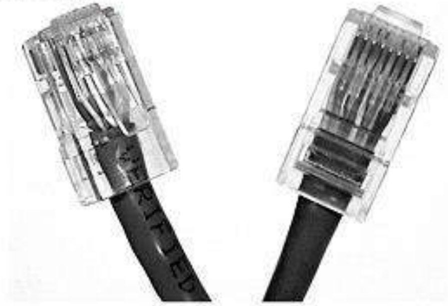
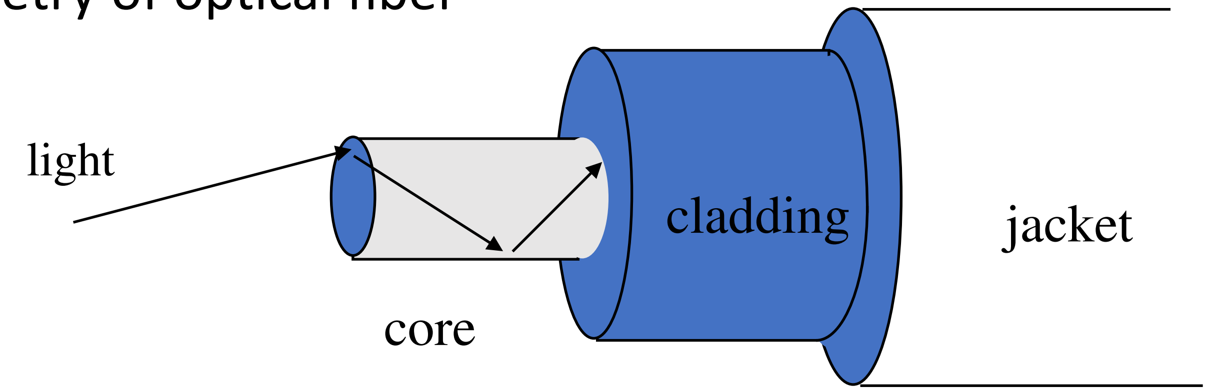


Figure 8-12 RJ-45 Connector

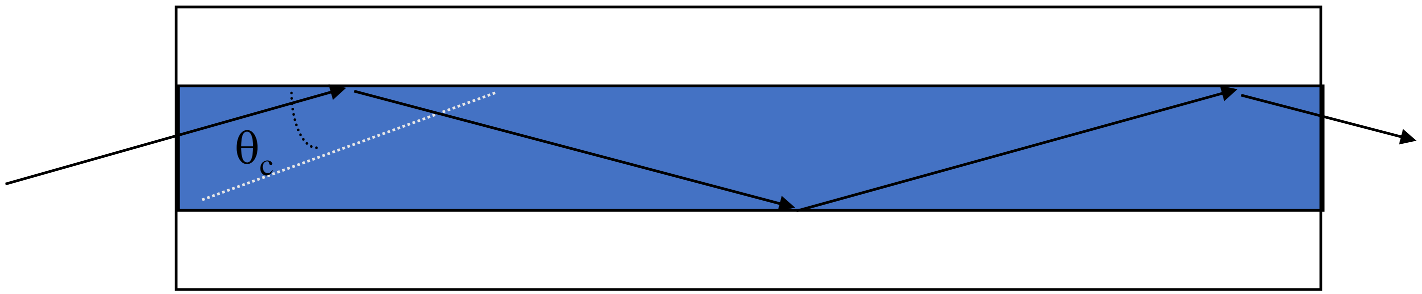


Optical fiber

(a) Geometry of optical fiber

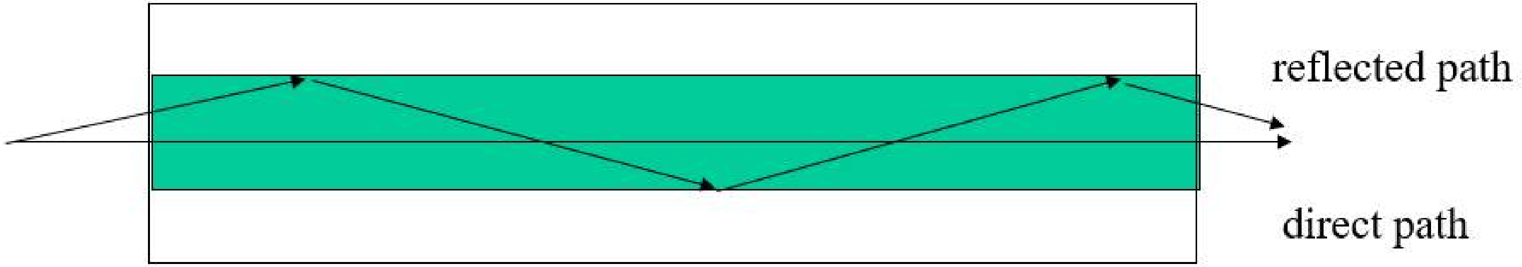


(b) Reflection in optical fiber

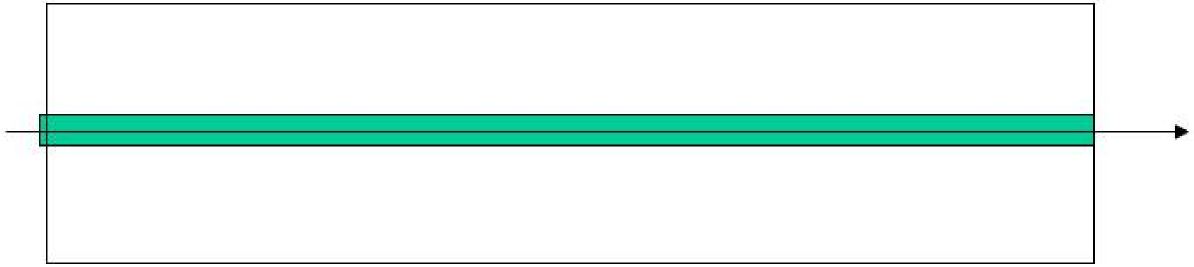


Optical fiber

(a) Multimode fiber: multiple rays follow different paths



(b) Single mode: only direct path propagates in fiber



Optical fiber

Three techniques

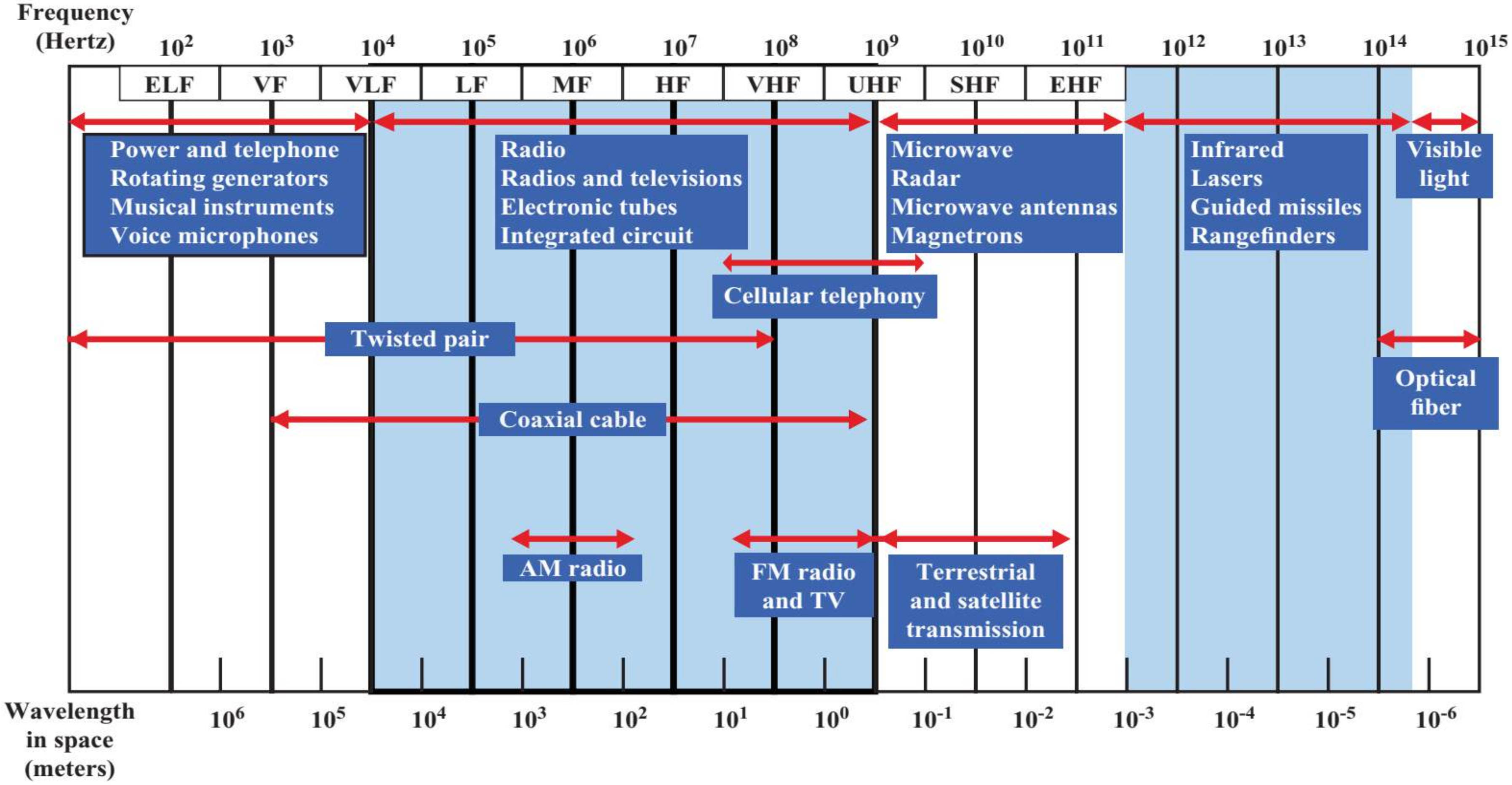
1. Multimode step-index
    - light propagates in the shape of a zigzag along the fiber/core axis according to the principle of total reflection.
    - Light entering the fiber at different angles of incidence will go through different paths.
    - Distance: few kms
2. Multimode graded-index
    - light travels forward in the form of sinusoidal oscillation.
    - Like step-index multimode fibers, different lights in a graded-index multimode fiber travel along different paths
    - Distance: 10-12 kms
    - Better performance

Optical fiber

3. Single-mode step-index
    - propagation of only one traverse electromagnetic **mode**
    - core diameter must be of the order of 2 µm to 10µm.
    - high information carrying capacity.

- Presence of multiple paths ➔ differences in delay ➔ optical rays *interfere* with each other.
- A narrow core can create a single direct path which yields higher speeds.
- WDM (Wavelength Division Multiplexing) yields more available capacity.

Electromagnetic Spectrum



ELF = Extremely low frequency
VF = Voice frequency
VLF = Very low frequency
LF = Low frequency
MF = Medium frequency
HF = High frequency
VHF = Very high frequency
UHF = Ultrahigh frequency
SHF = Superhigh frequency
EHF = Extremely high frequency

THANK YOU

S Nagasundari
Department of Computer Science and Engineering
nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
Department of Computer Science and Engineering

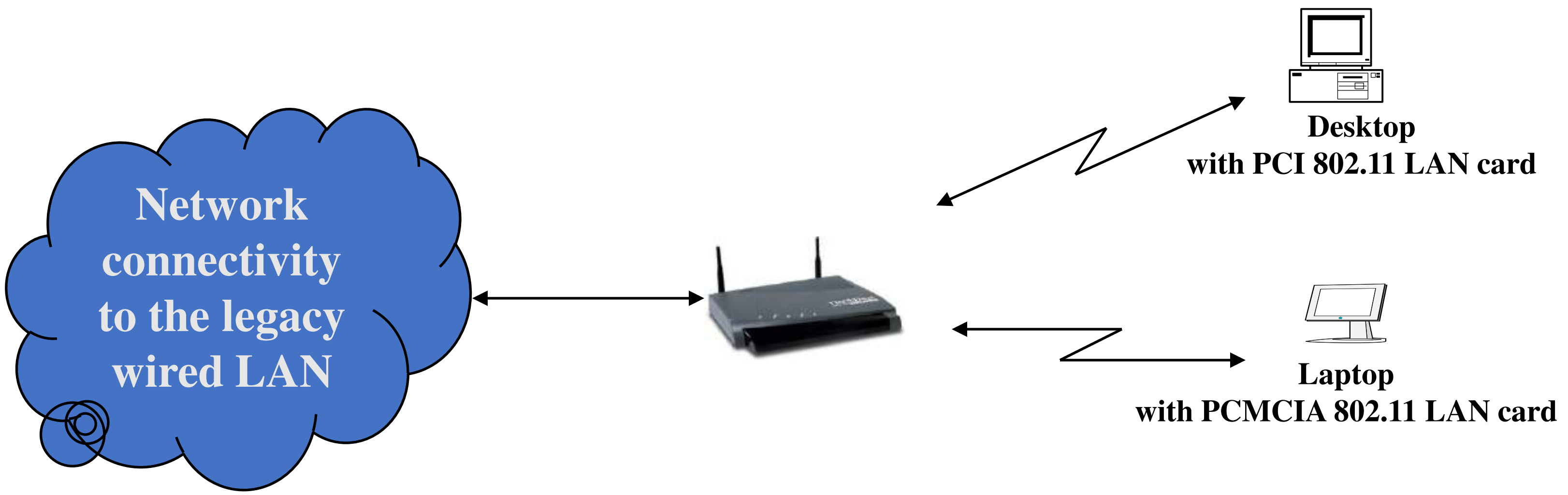
Unit – 5 Link Layer and LAN Roadmap

- 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

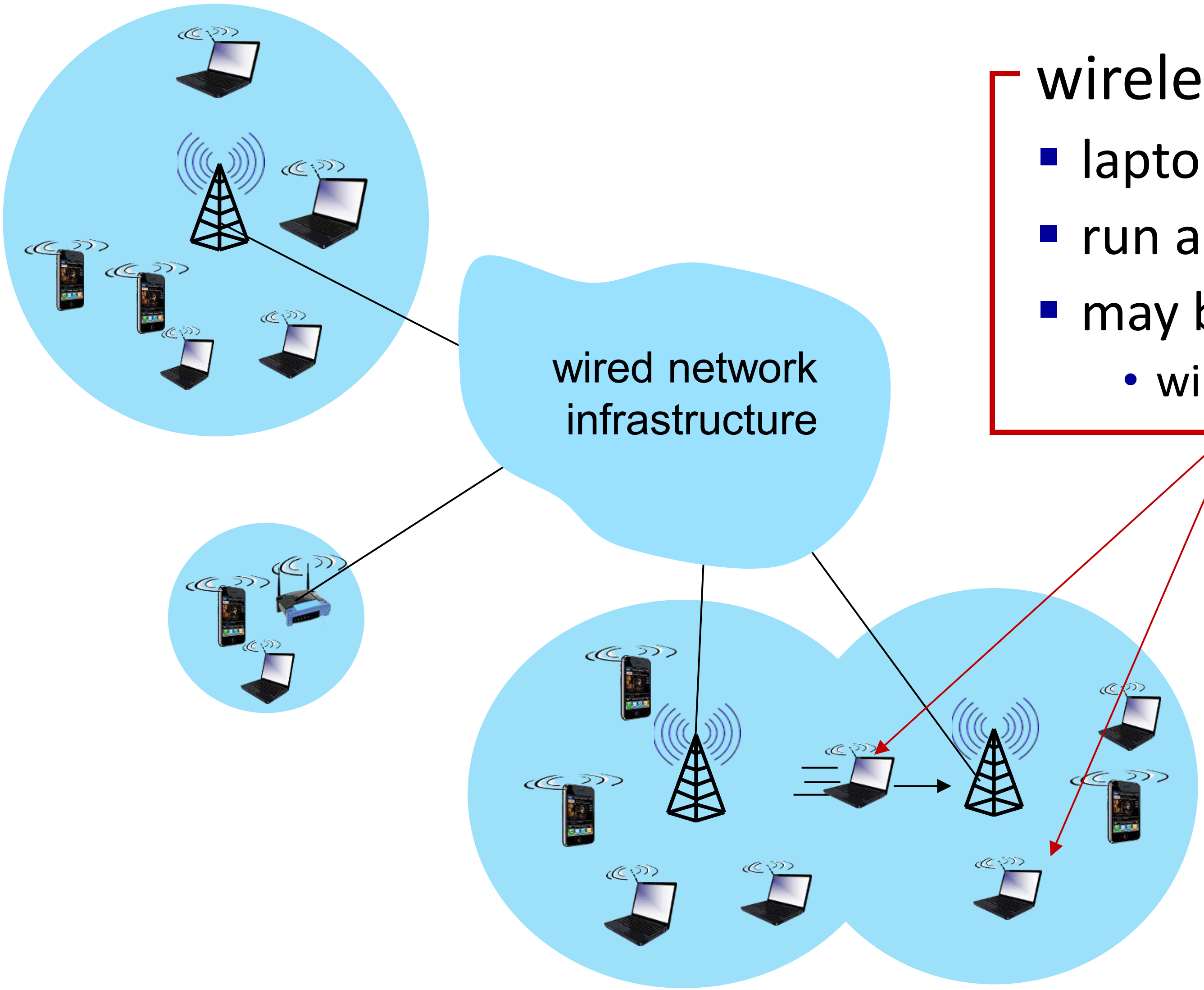
- Why, What- Wireless LAN
- 802.11 Architecture

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

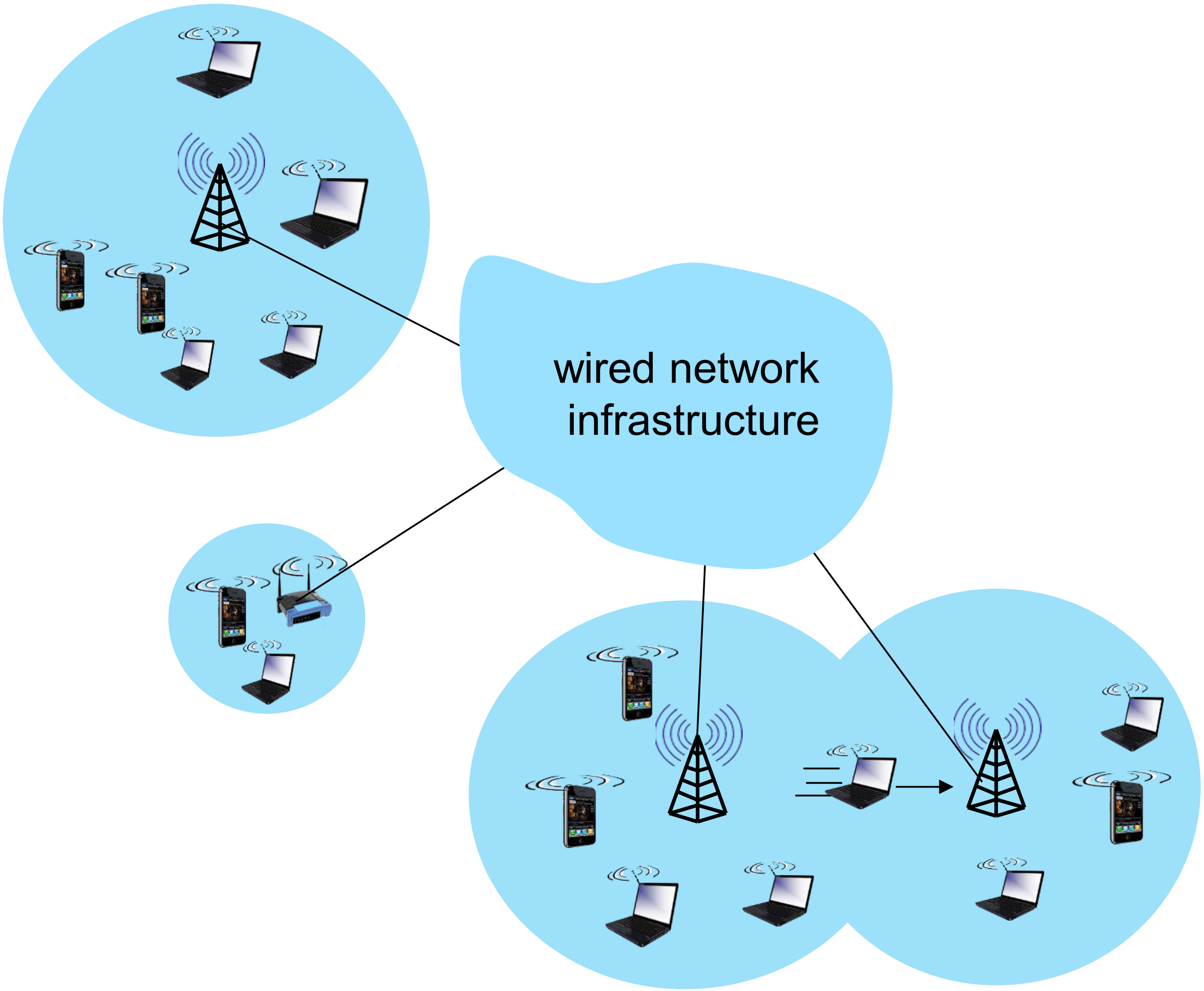
Elements of a Wireless Network



wireless hosts

- laptop, smartphone, IoT
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility!

Elements of a Wireless Network



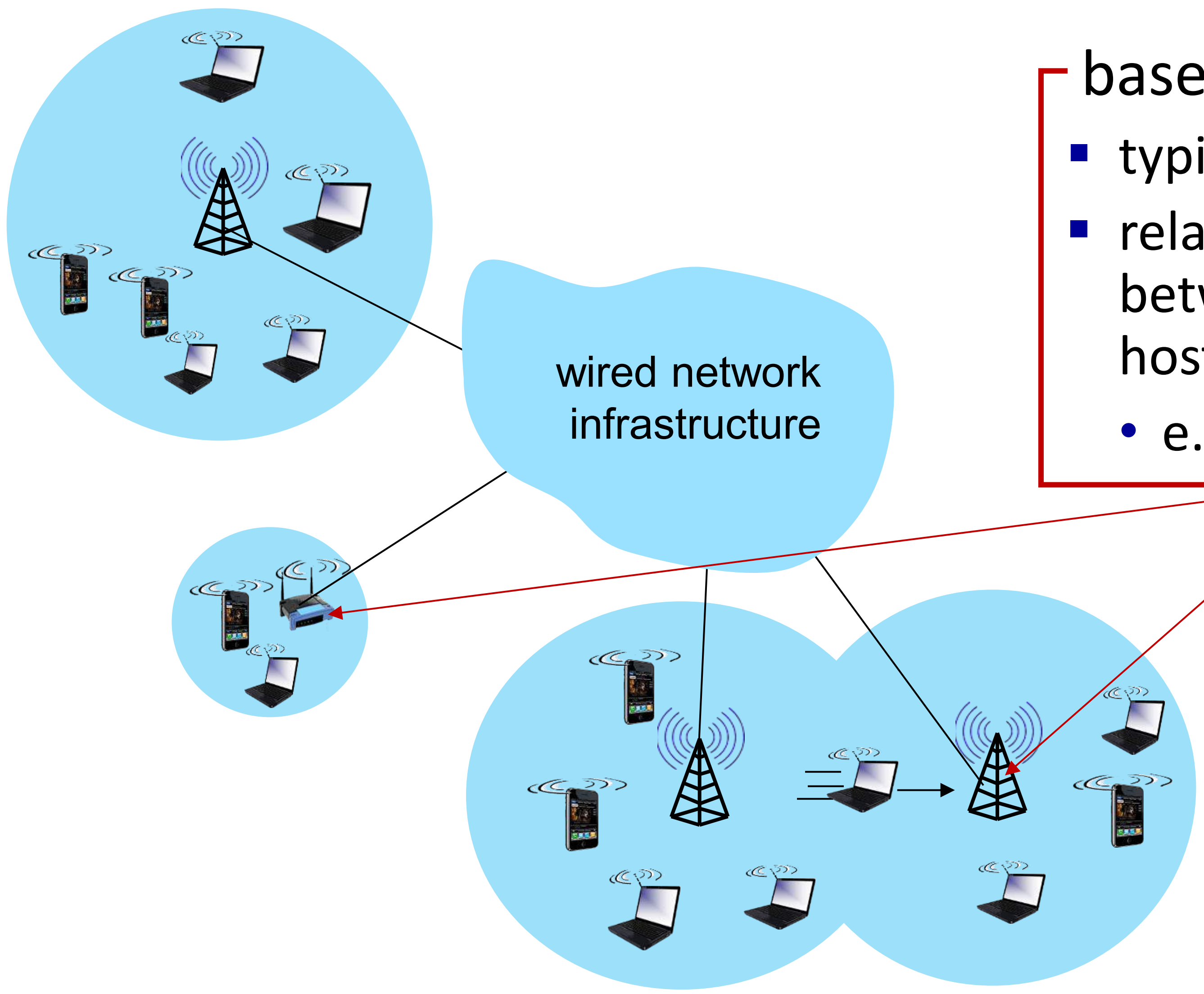
IEEE 802.11- Wireless LAN

IEEE 802.11 defines

- MAC protocol and
- Physical medium specification

for wireless LANs

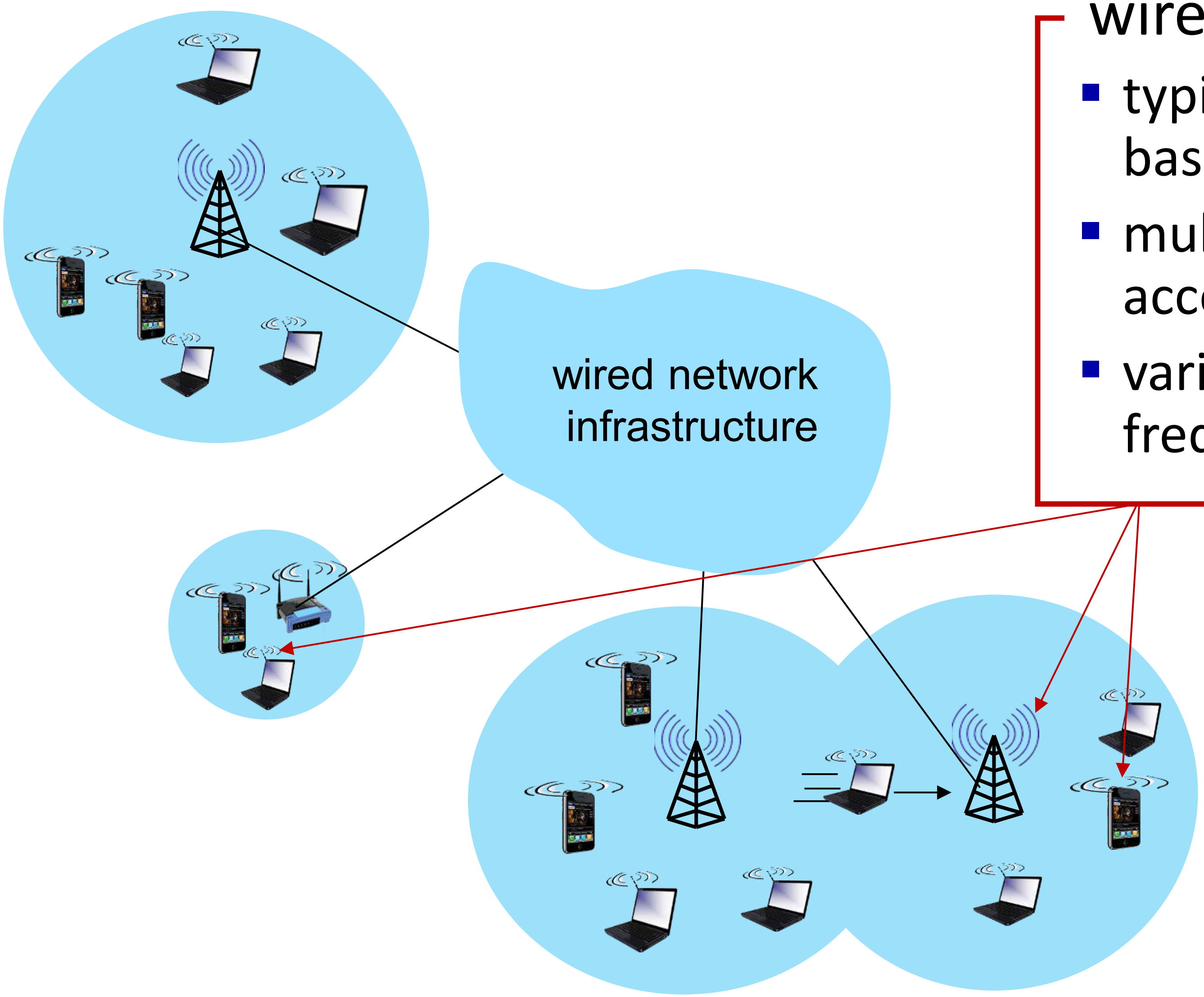
Elements of a Wireless Network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., **cell towers**, **802.11 access points**

Elements of a Wireless Network



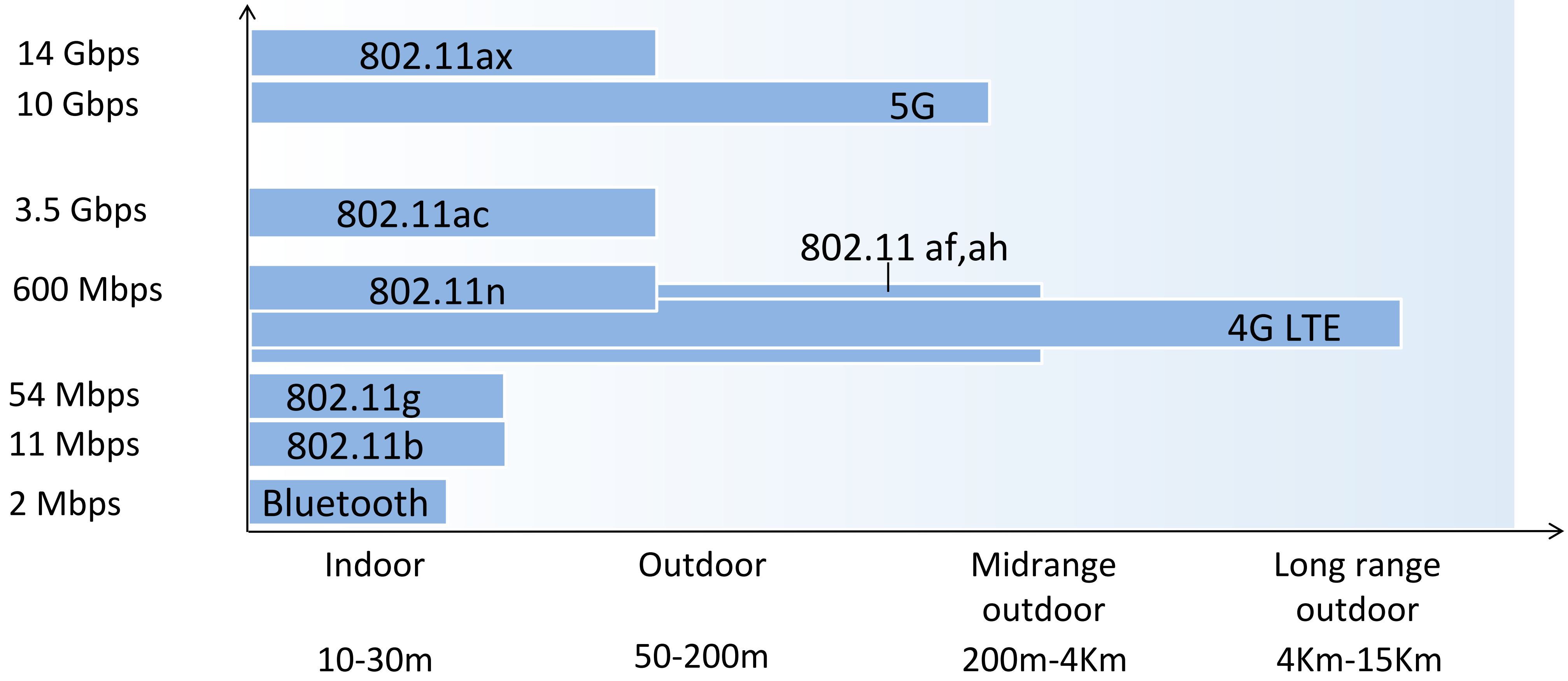
wireless link

- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

IEEE 802.11- Terminology

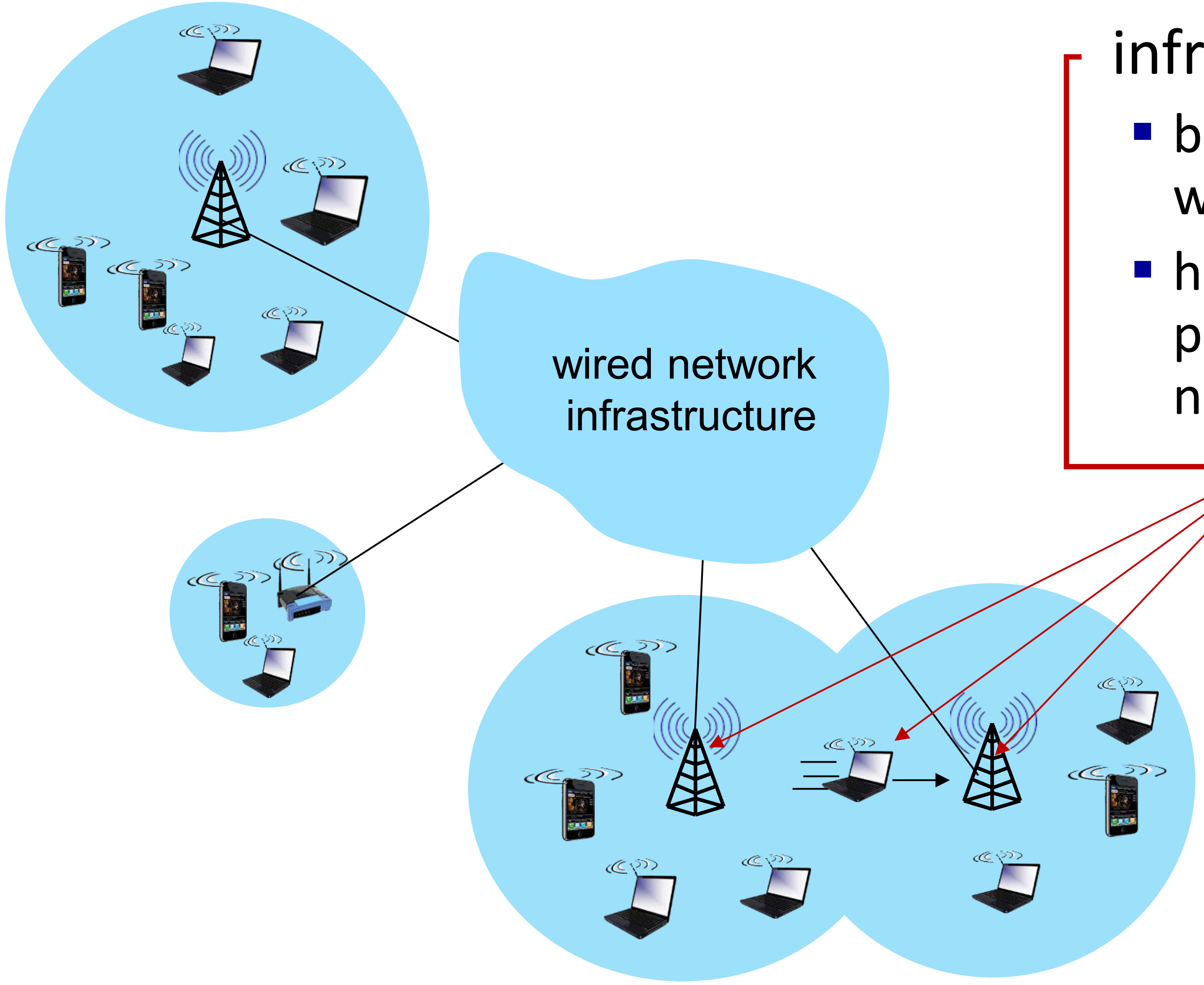
Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines 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.

Characteristics of Selected Wireless Links



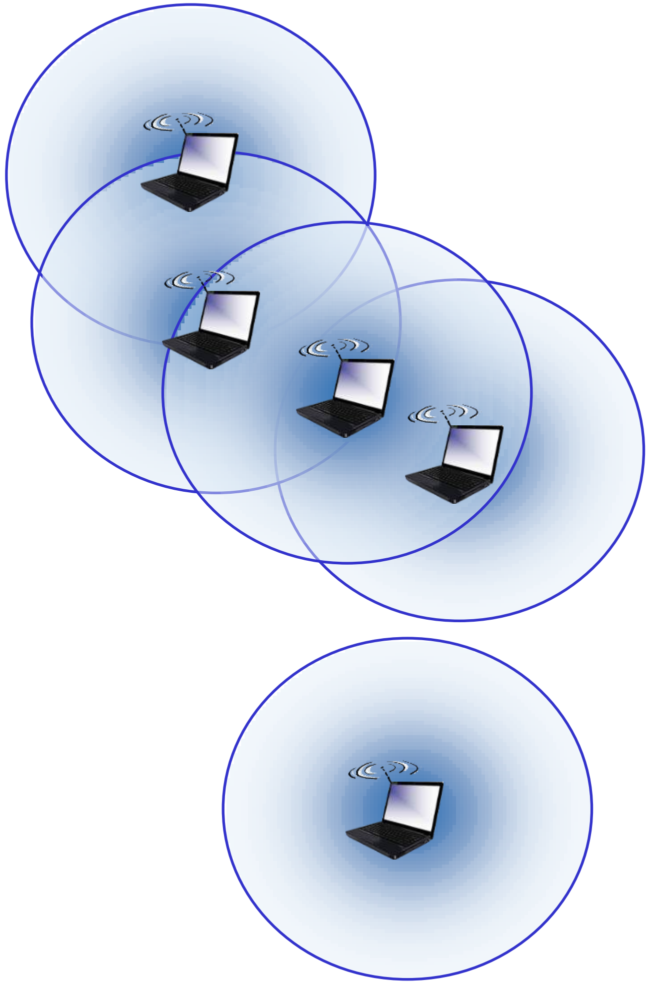
2 Key Areas:

Coverage area & Link rate



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: routing, address assignment, DNS-like name translation, and more.

Wireless network taxonomy

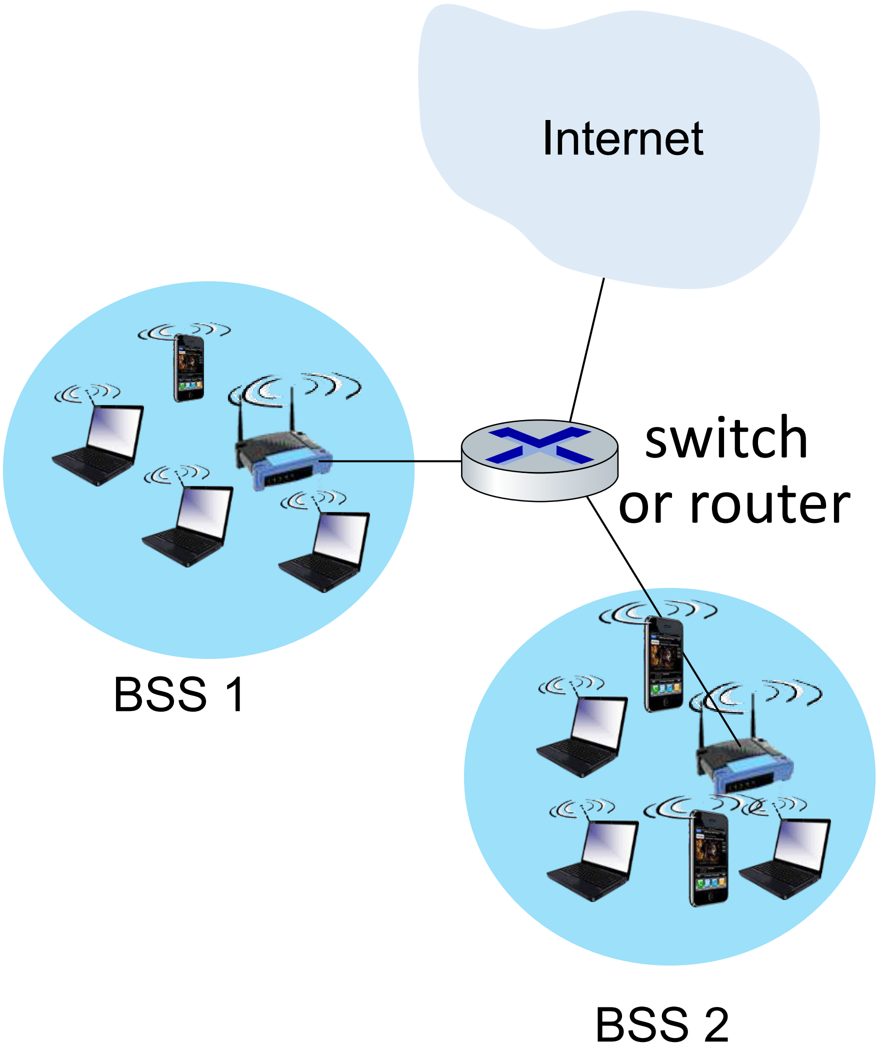
	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, cellular) which connects to larger Internet. **Eg: 4G LTE**	host may have to relay through several wireless nodes to connect to larger Internet: ***mesh net***
infrastructure less	no base station, no connection to larger Internet. eg: **Bluetooth, ad hoc nets**	no base station, no connection to larger Internet. May have to relay to reach other. **eg: MANET, VANET**

IEEE 802.11 Wireless LAN (WiFi)

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

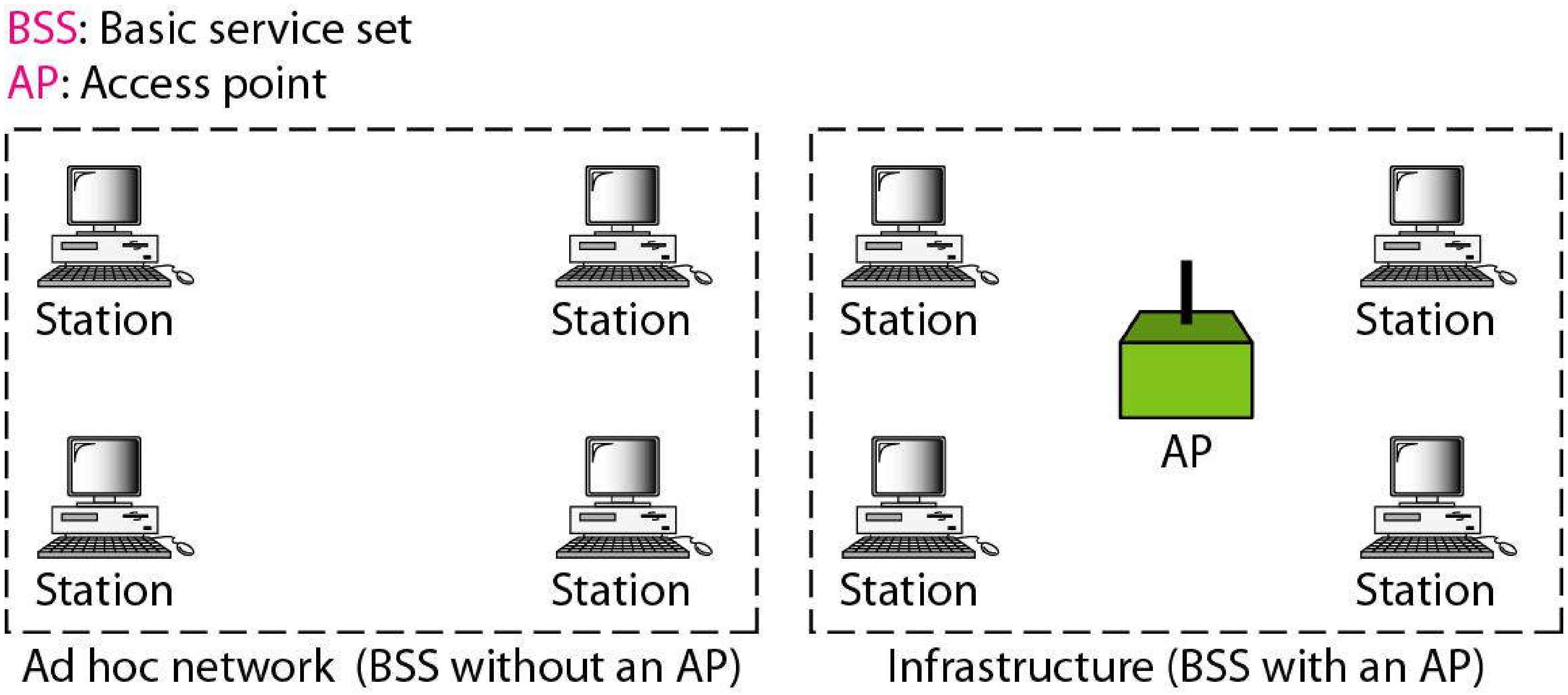
- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

The 802.11 LAN architecture



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

Basic Service Set



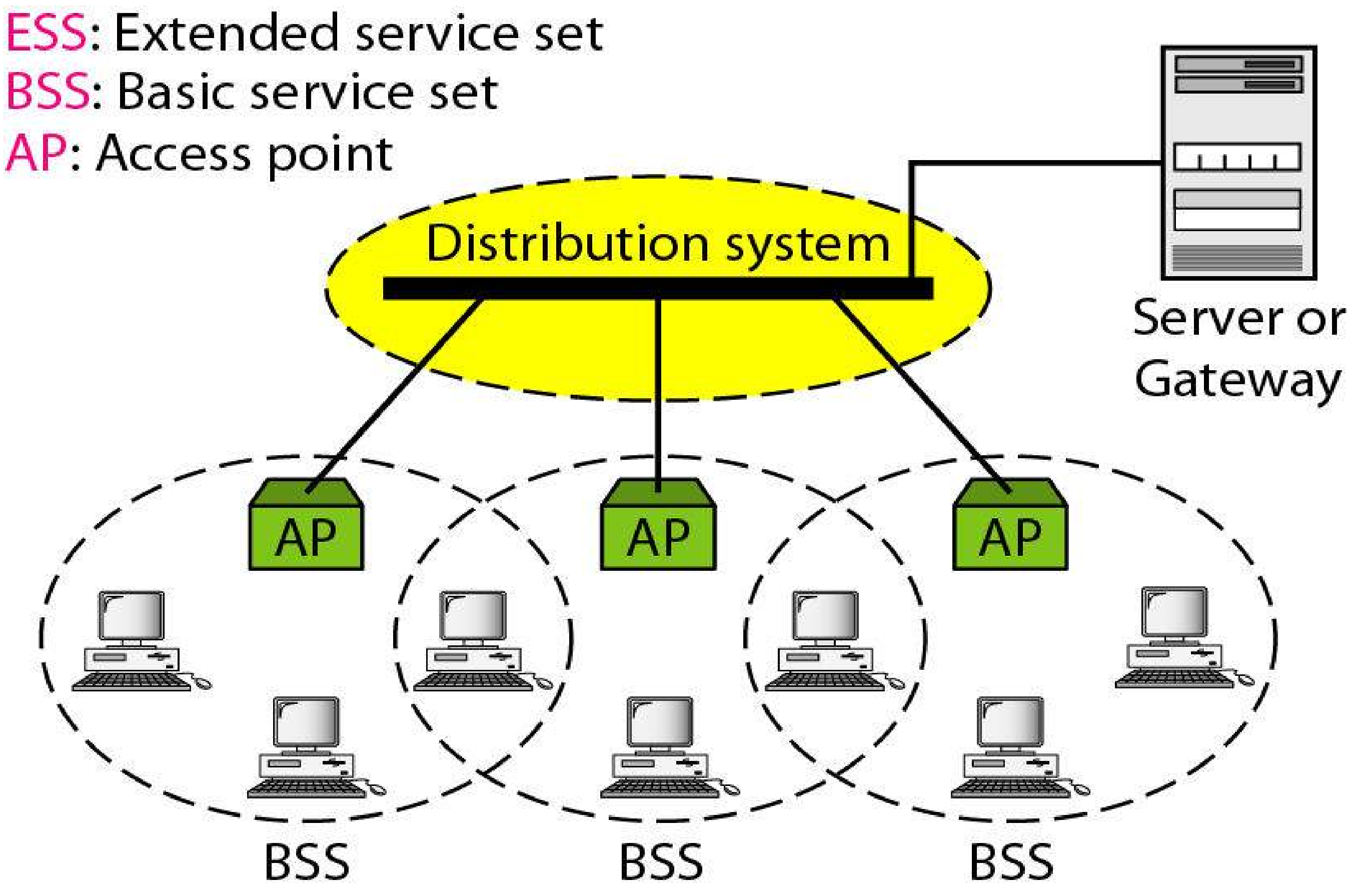
May be isolated or connect to backbone distribution system (DS) through access point (AP)

- AP functions as bridge

BSS- Smallest building block

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

Extended Service Set



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

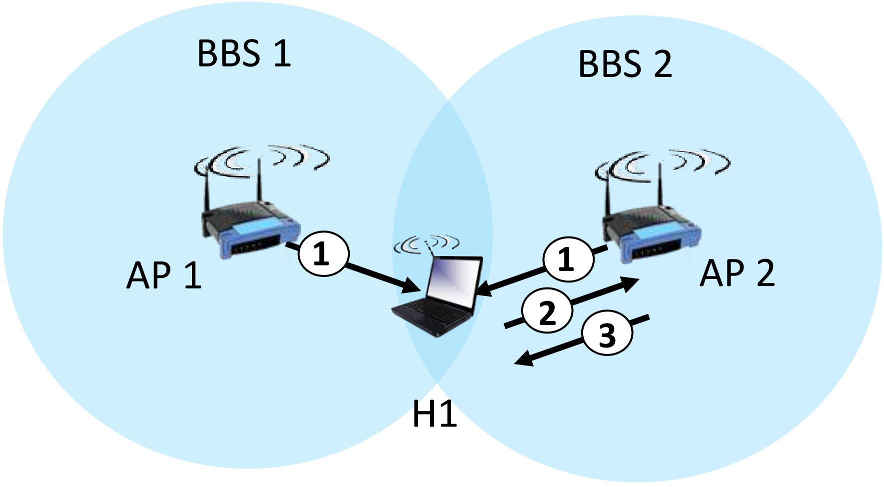
802.11: Channels, Association

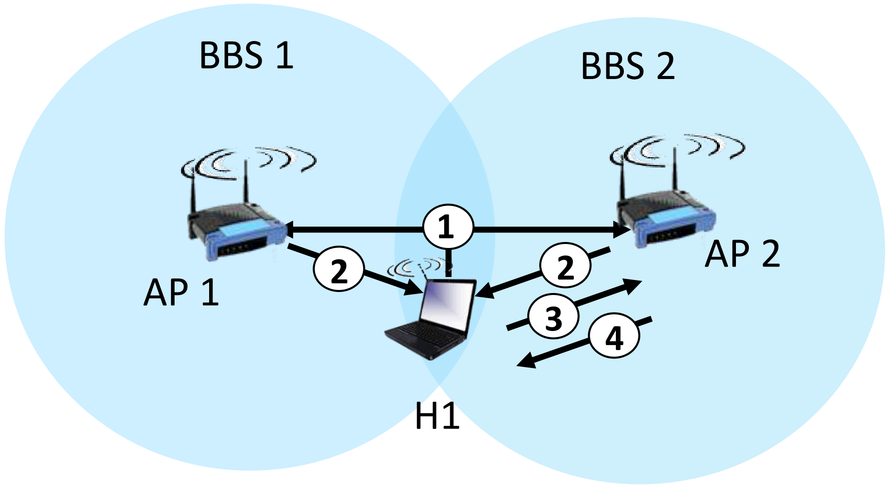
- spectrum divided into channels at different frequencies
  - AP assigns **Service Set ID (SSID)**
  - AP admin chooses frequency for AP (**2.4 GHz to 2.4835 GHz**)
  - interference possible: channel can be same as that chosen by neighboring AP! – **WiFi Jungle**

- arriving host: must associate with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - then may perform authentication
  - then typically run DHCP to get IP address in AP's subnet

BSS

802.11 active/passive scanning





passive scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

Thank You
For Your Attention

THANK YOU

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu

COMPUTER NETWORKS

S Nagasundari
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

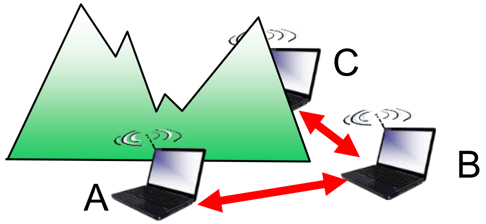
- Physical layer
  - Purpose, Signals to Packets
  - Analog Vs Digital Signals
  - Transmission Media
- Wireless LANs: IEEE 802.11

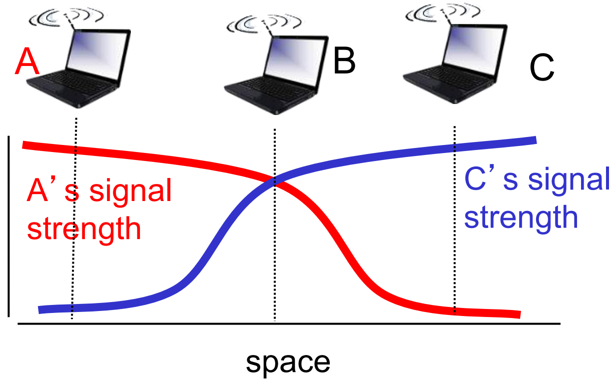
Class 55 : IEEE 802.11- Wireless LAN : Learning Objectives

- MAC Protocol
- Frame Format
- Addressing Mechanism

IEEE 802.11: multiple access

- avoid collisions: 2^+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to fading
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/<u>C</u>ollision<u>A</u>voidance

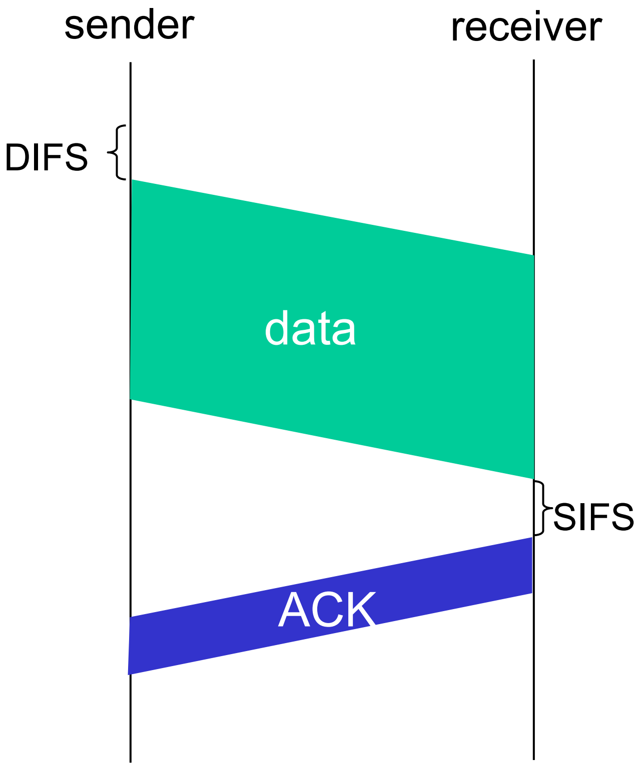




802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2



802.11 receiver

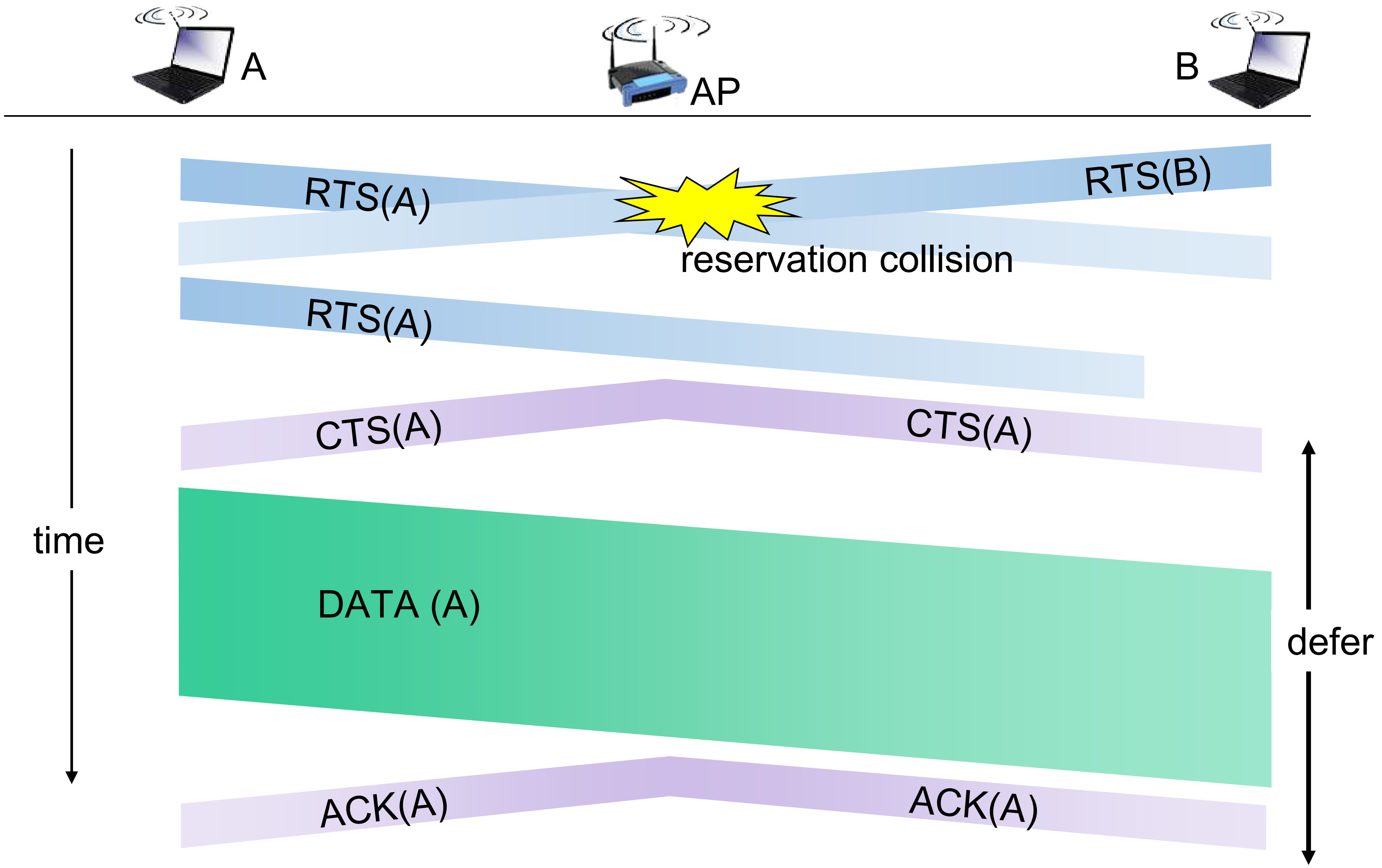
if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)

Avoiding Collisions (more)

idea: sender "reserves" channel use for data frames using small reservation packets

- sender first transmits *small* request-to-send (RTS) packet to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing

duration of reserved transmission time (RTS/CTS)

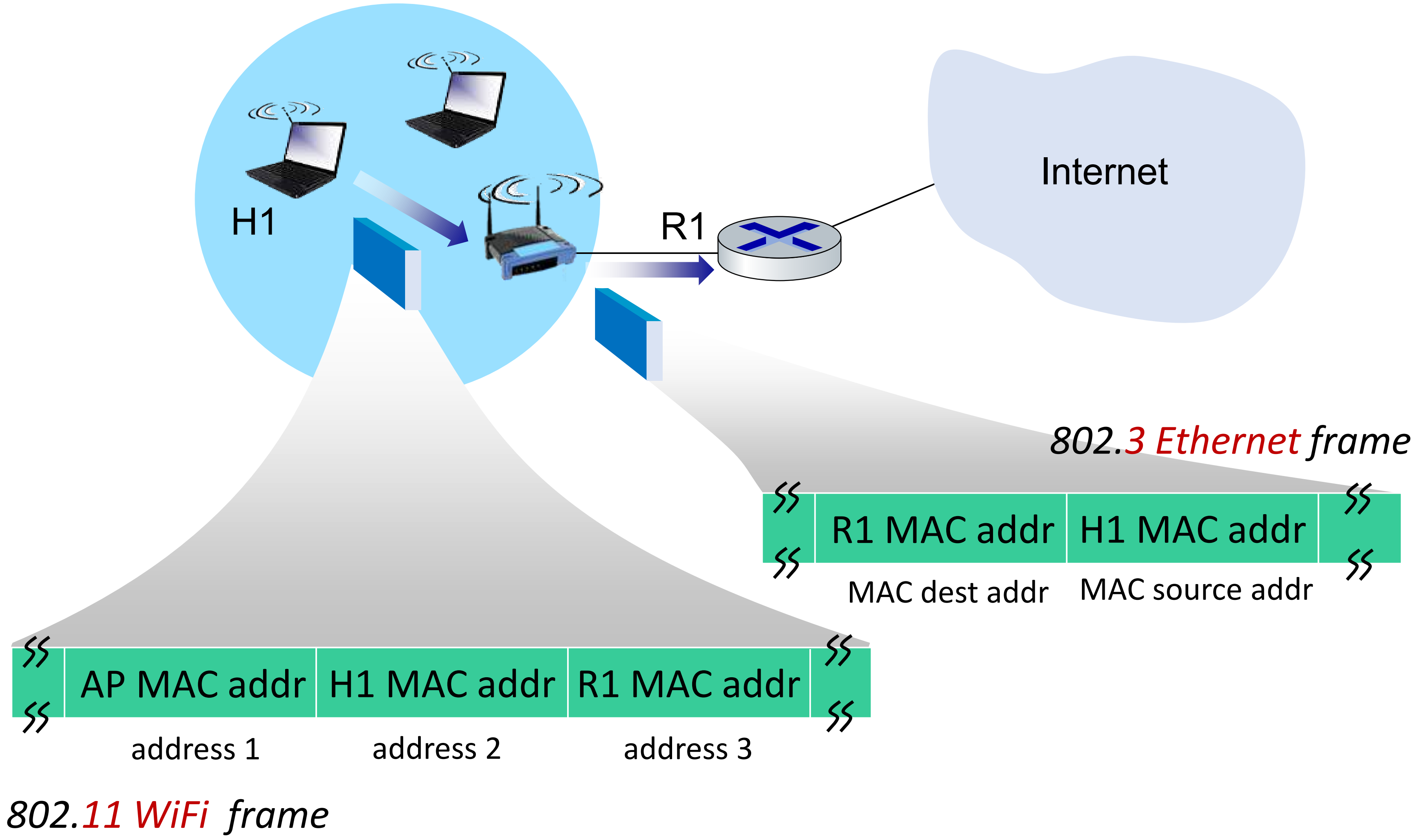
frame sequence # (for reliable data transfer)

2	2	6	6	6	2	6	0 - 2312	4	Bytes
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC	

2	2	4	1	1	1	1	1	1	1	1	Bits
protocol version	type	subtype	to AP	from AP	more frag	retry	power mgt	more data	WEP	rsvd	

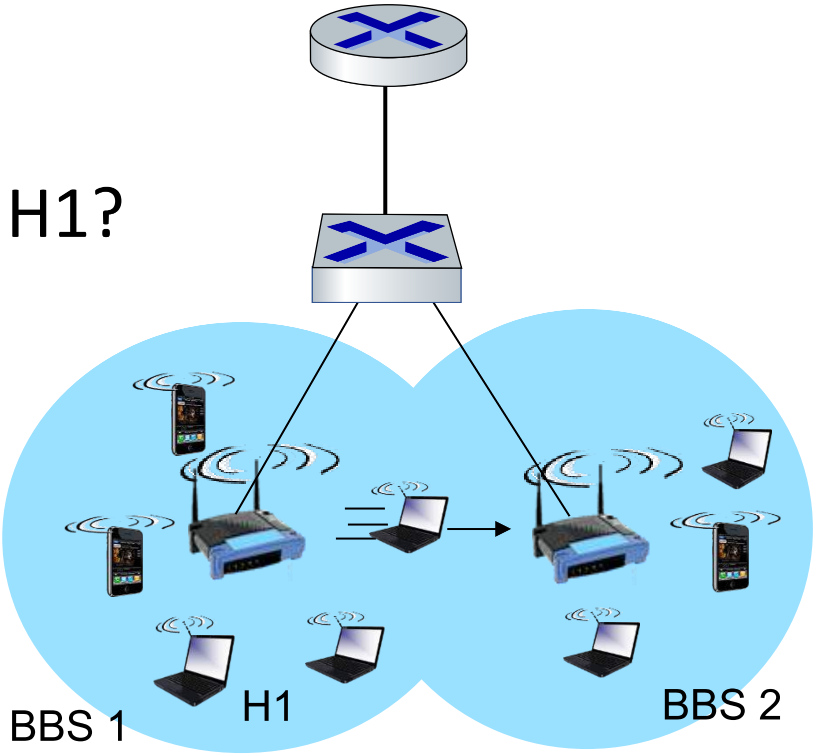
frame type (RTS, CTS, ACK, data)

802.11 frame: addressing



802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning : switch will see frame from H1 and "remember" which switch port can be used to reach H1



Suggested Readings

Thank You
For Your Attention

THANK YOU

S Nagasundari
Department of Computer Science and Engineering

nagasundaris@pes.edu