


Computer Networks

CMSC 417 : Spring 2024

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

Topic: Link layer: Ethernet, WiFi (Textbook chapter 2)

Nirupam Roy

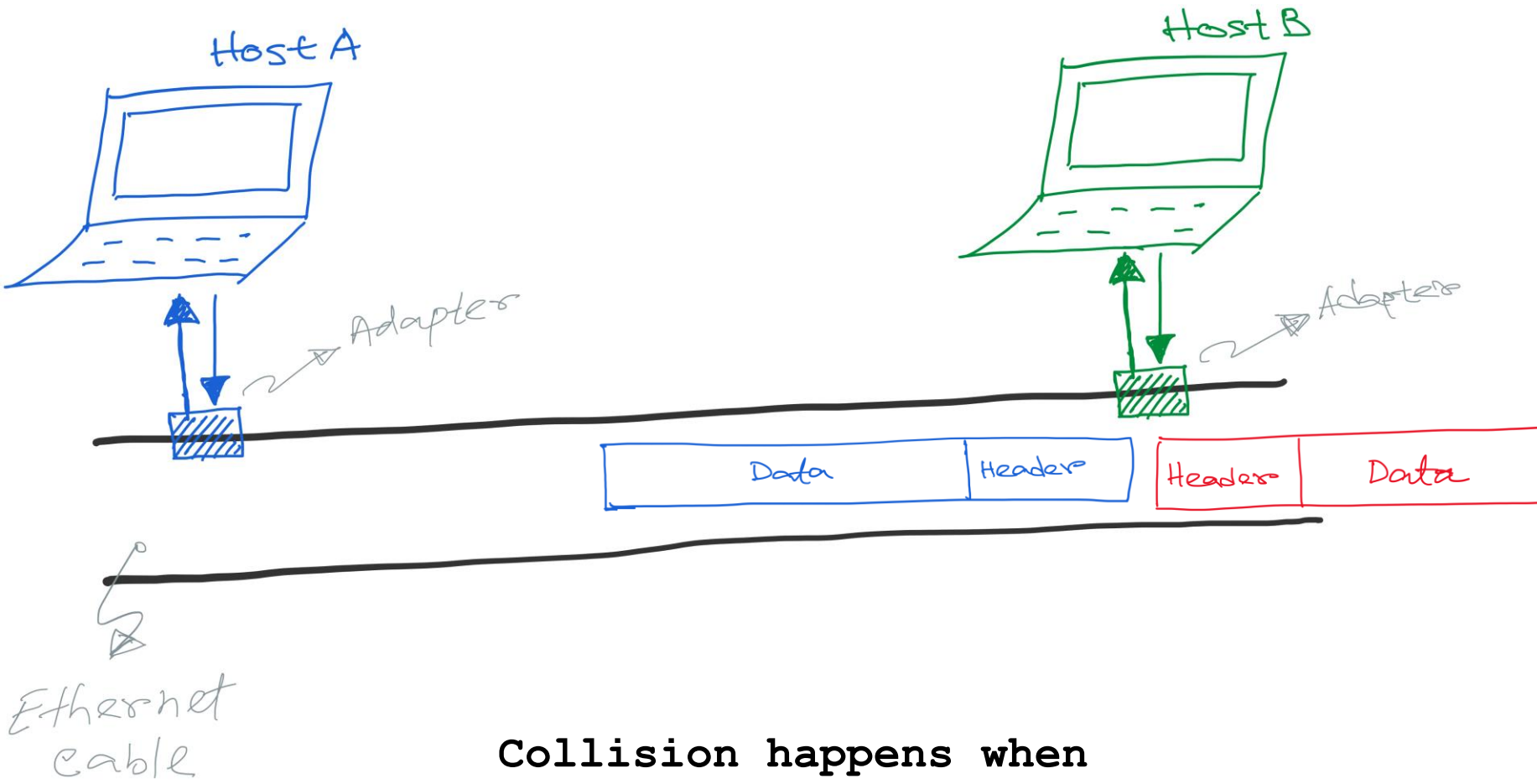
Tu-Th 2:00-3:15pm
CSI 2117

April 18th, 2024



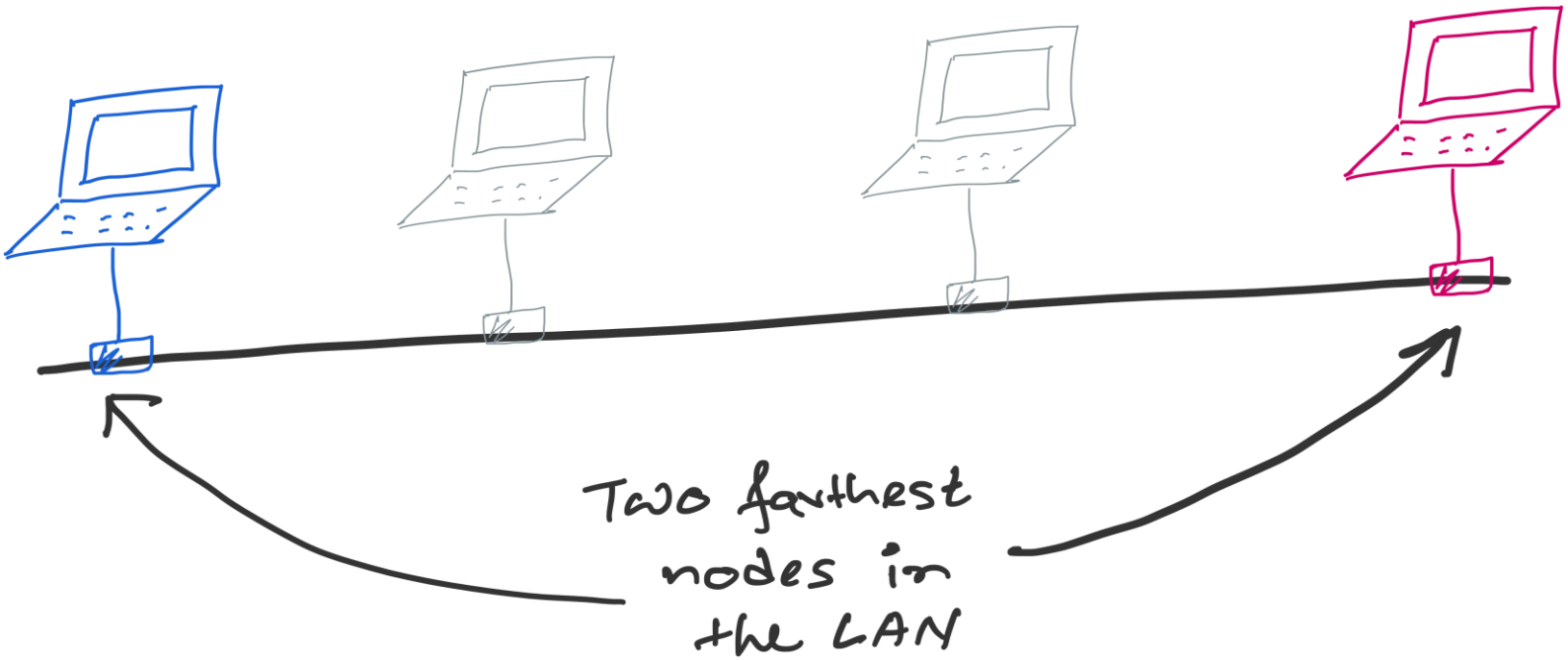

Ethernet

Preparing for the worst-case scenario of collision

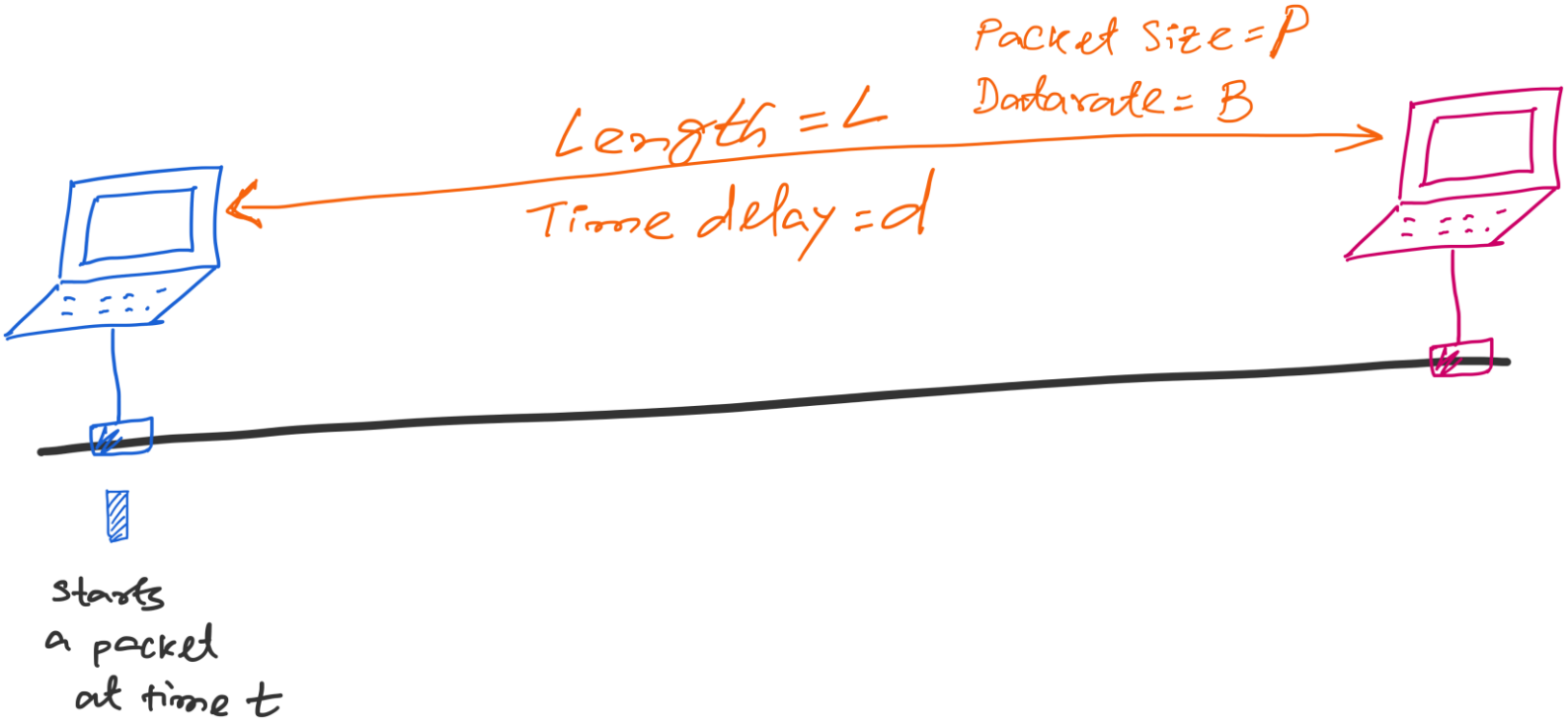


Collision happens when both packet overlaps at the receiver.

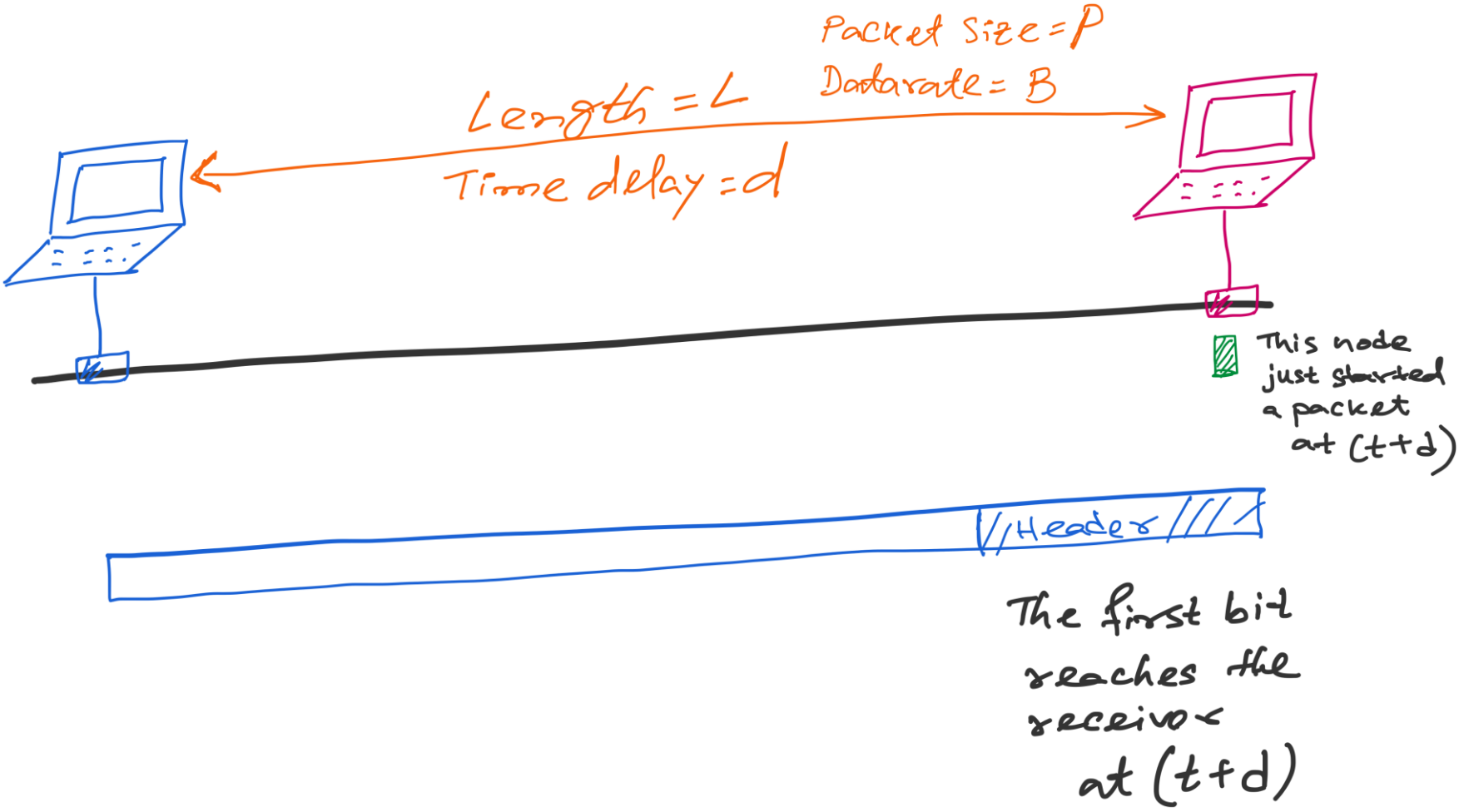
Preparing for the worst-case scenario of collision



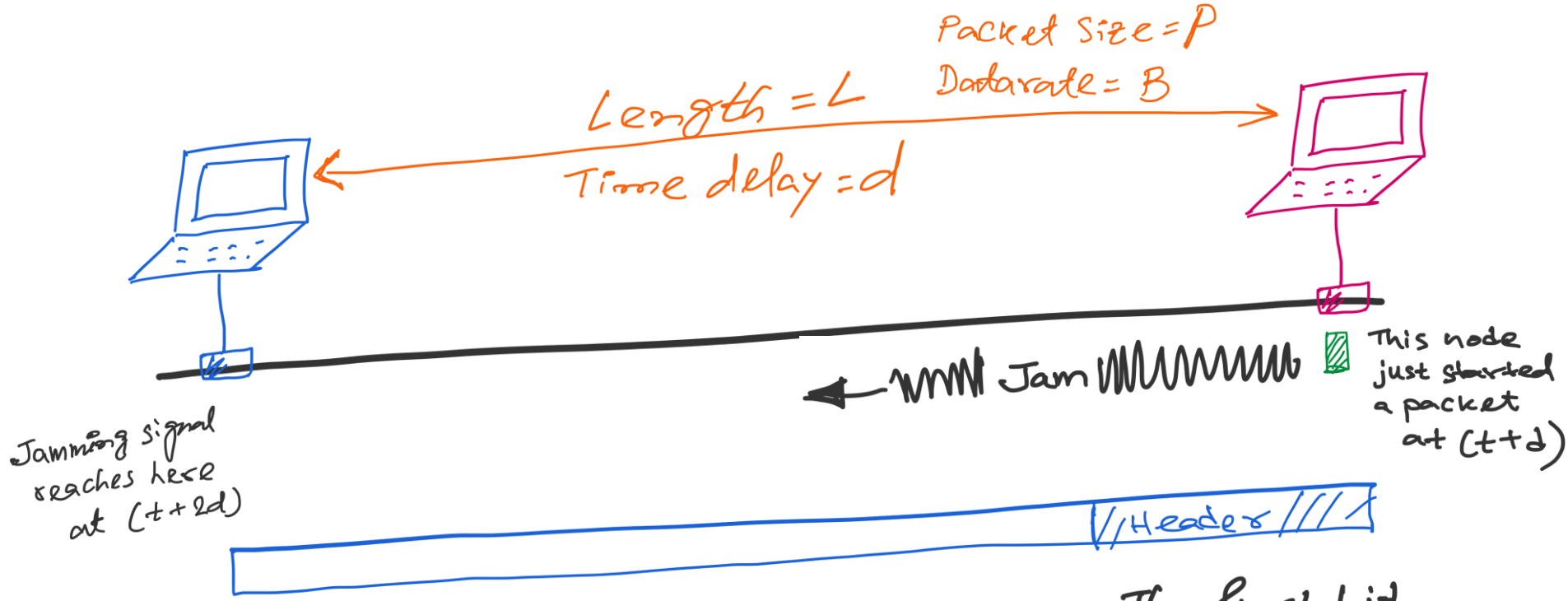
Preparing for the worst-case scenario of collision



Preparing for the worst-case scenario of collision

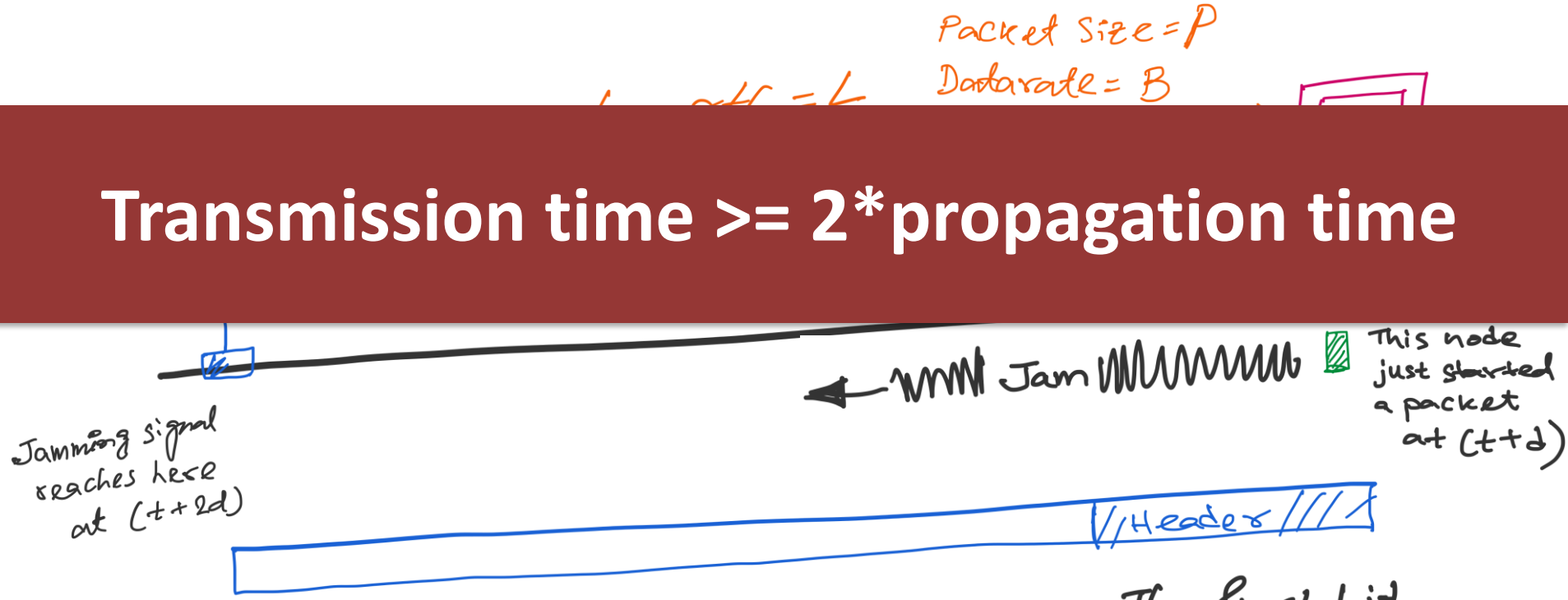


Preparing for the worst-case scenario of collision



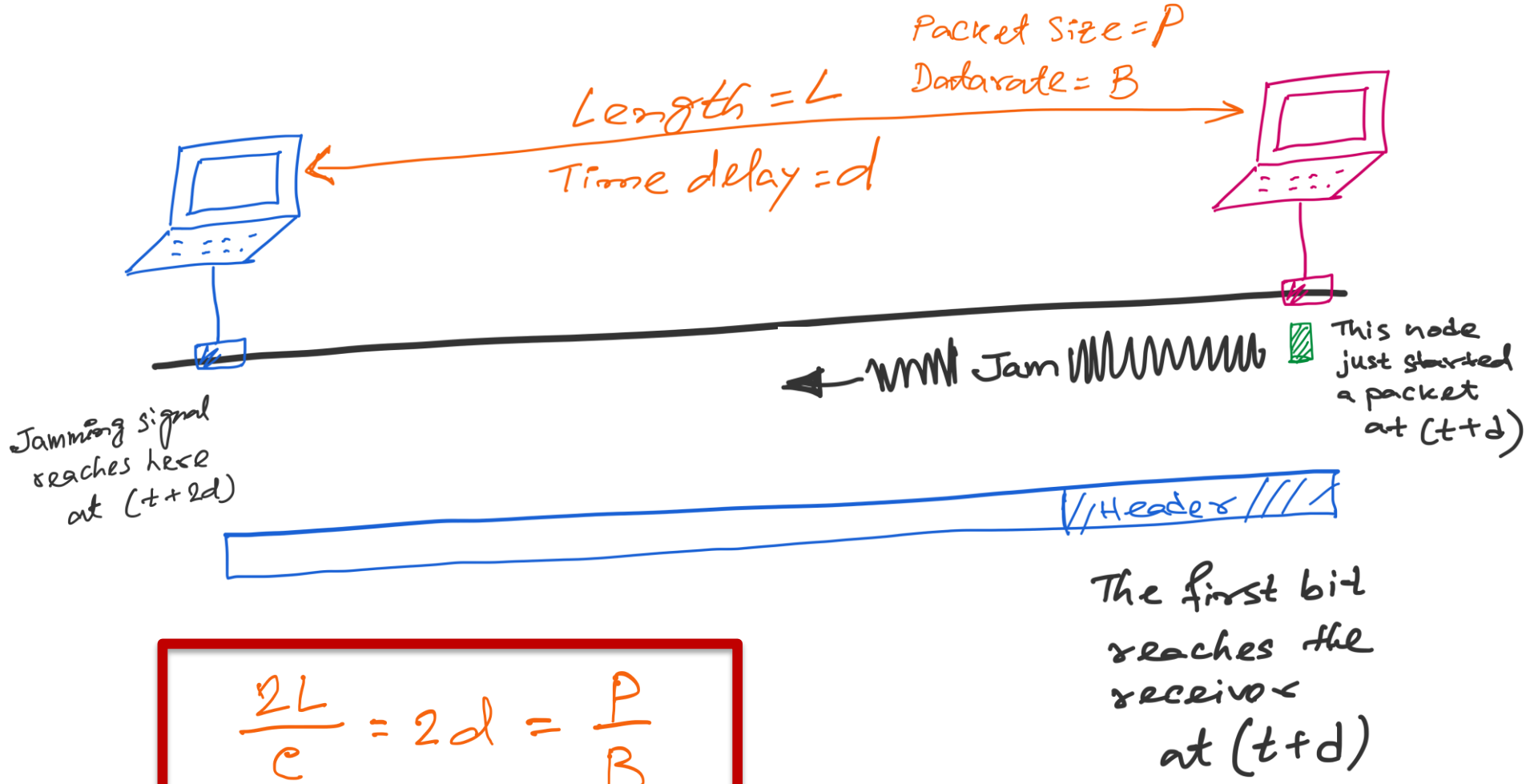
The packet should be at least for 2d seconds long so that the sender can get the notification of the collision (through the jamming signal)

Preparing for the worst-case scenario of collision



The packet should be at least for 2d seconds long so that the sender can get the notification of the collision (through the jamming signal)

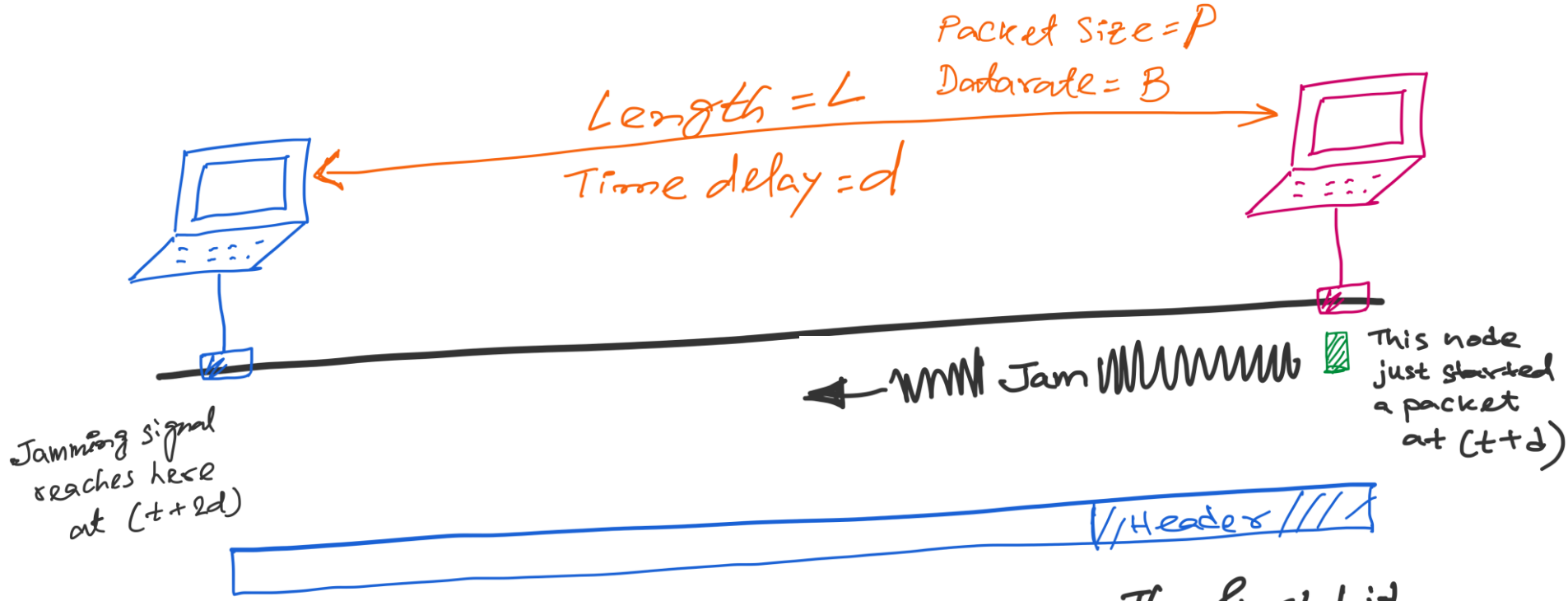
Preparing for the worst-case scenario of collision



$$\frac{2L}{c} = 2d = \frac{P}{B}$$

Formula for minimum packet size (P) or maximum length (L)

Preparing for the worst-case scenario of collision



$$\frac{2L}{C} = 2d = \frac{P}{B}$$

$$\frac{2L}{C} = 2d = \frac{P}{B}$$

C = Electrical signal in the cable (in copper, 2×10^8 m/s)

L = Maximum length of the link (meter)

P = Minimum frame size (bits)

B = Data rate (bits/sec)

Say, $B = 10\text{Mbps} = 10^7$ bits/sec

$P = 64$ bytes $= 512$ bits

$C = 2 \times 10^8$ m/sec.

$$\frac{2L}{C} = \frac{P}{B}$$

$$\therefore L = \frac{PC}{2B} = \frac{512 \times 2 \times 10^8}{2 \times 10^7}$$

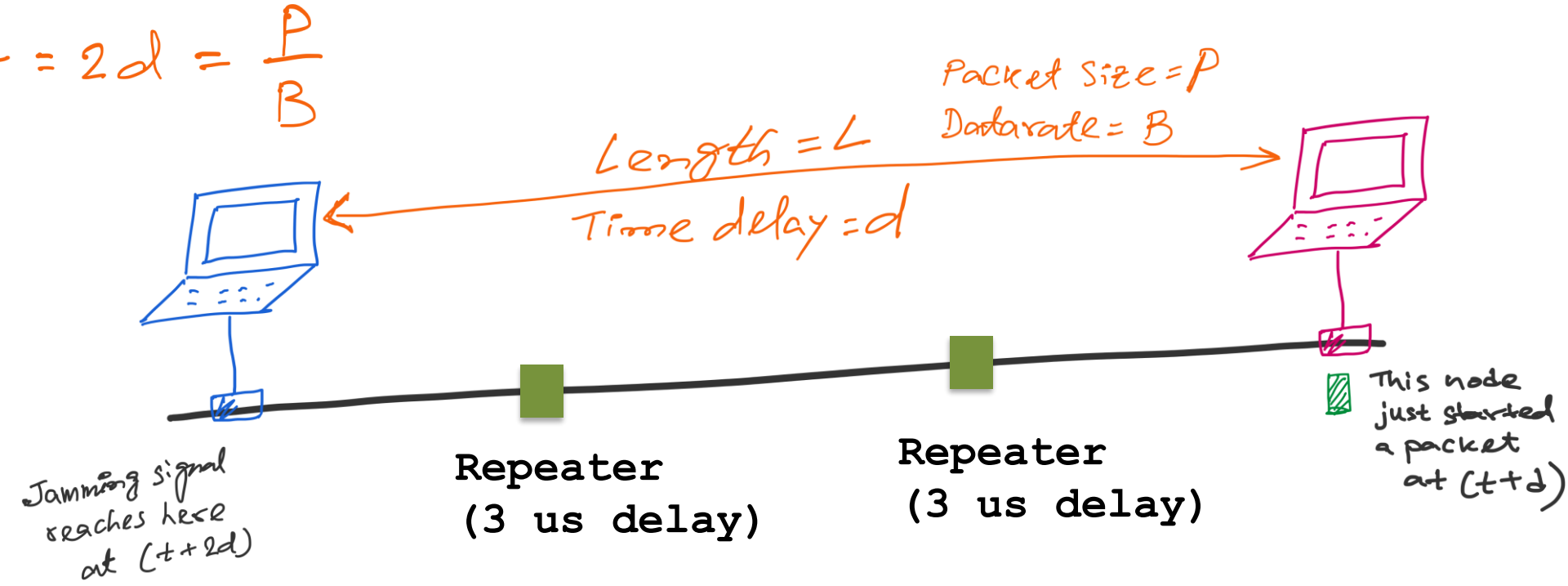
$$= 5120 \text{ meter}$$

$$\approx 5 \text{ km}$$

Maximum length of one segment of 10Base5 cable was 500 m.

To achieve 5km range, it will take 9 repeaters. Repeaters add ~3μs delay.

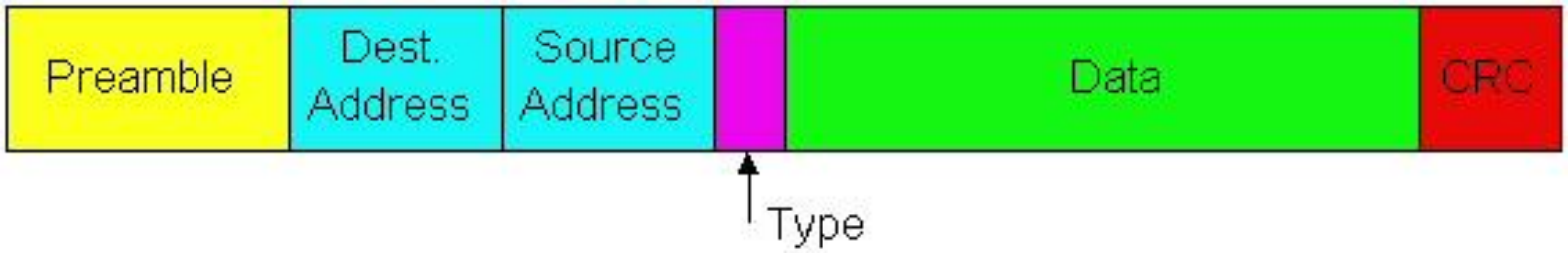
Preparing for the worst-case scenario of collision



$$\frac{P}{B} \geq 2 * \left(\frac{L}{C} + \text{Additional-one-way-delay} \right)$$

Ethernet Frame Structure

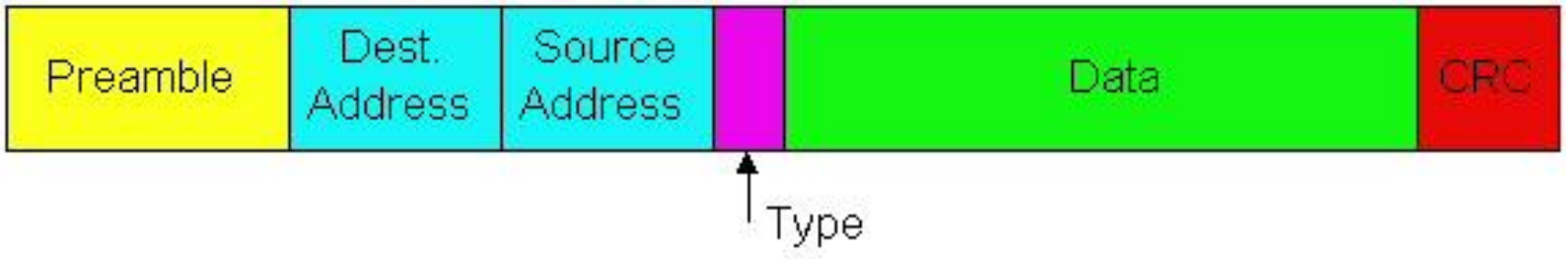
- Sending adapter encapsulates packet in frame



- Preamble: synchronization
  - Seven bytes with pattern 10101010, followed by one byte with pattern 10101011
  - Used to synchronize receiver, sender clock rates

Ethernet Frame Structure

- Addresses: source and destination MAC addresses
  - Adaptor passes frame to network-level protocol
    - If destination is local MAC address or broadcast address
  - Otherwise, adapter discards frame
- Type: indicates the higher layer protocol
  - Usually IP
  - But also Novell IPX, AppleTalk, …
- CRC: cyclic redundancy check



Unreliable, Connectionless Service

- Connectionless
  - No handshaking between send and receive adapter
- Unreliable
  - Receiving adapter doesn't send ACKs or NACKs
  - Packets passed to network layer can have gaps
  - Gaps can be filled by transport protocol (e.g., TCP)
  - Otherwise, the application will see the gaps

Star topology and collision-free Ethernet

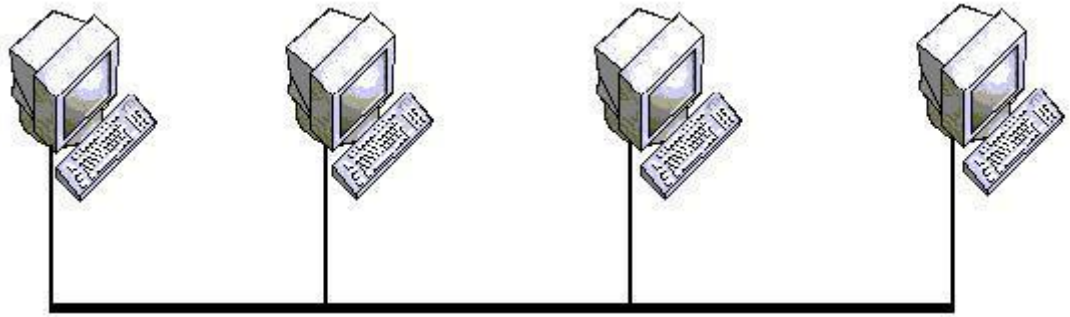
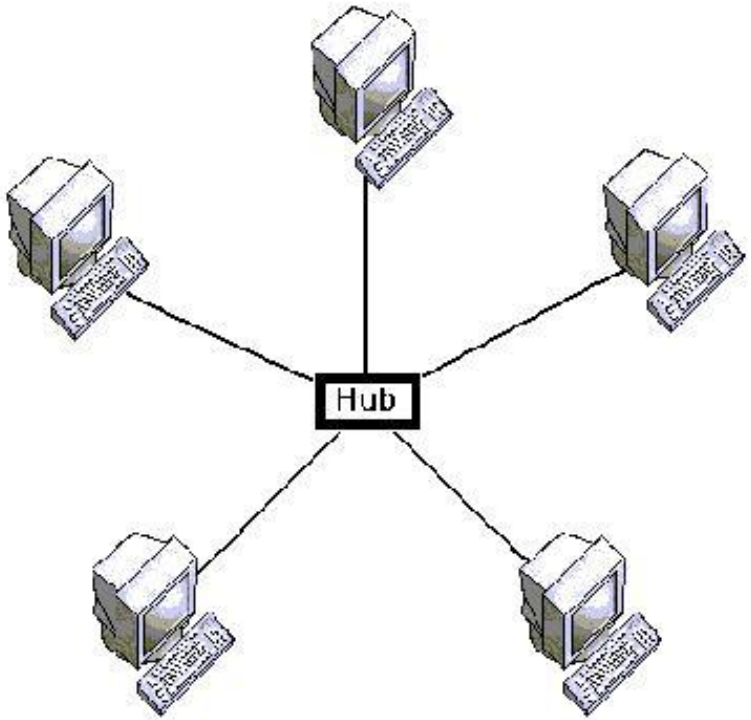


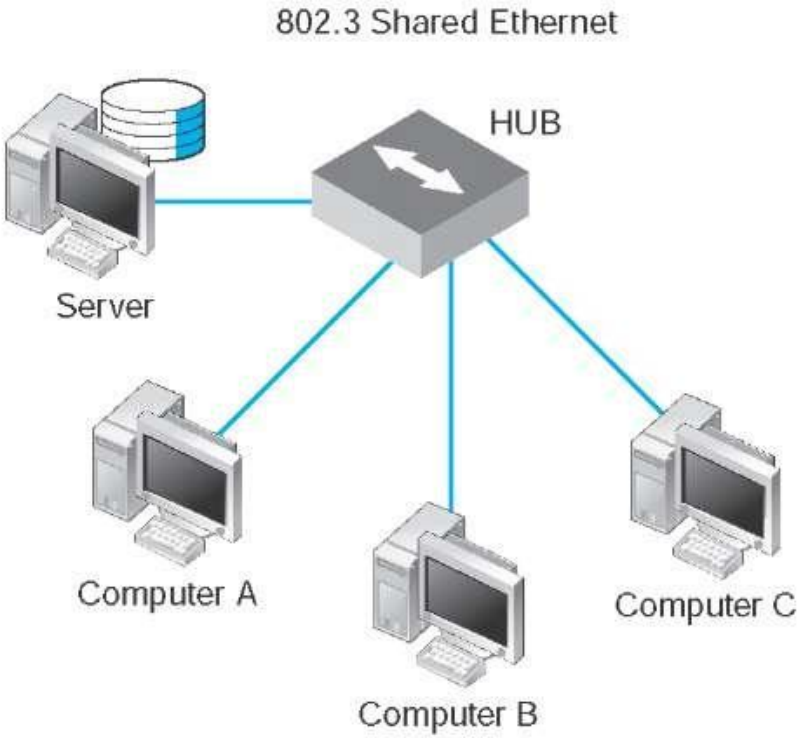
Figure 1: Bus topology

Bus topology



Star topology

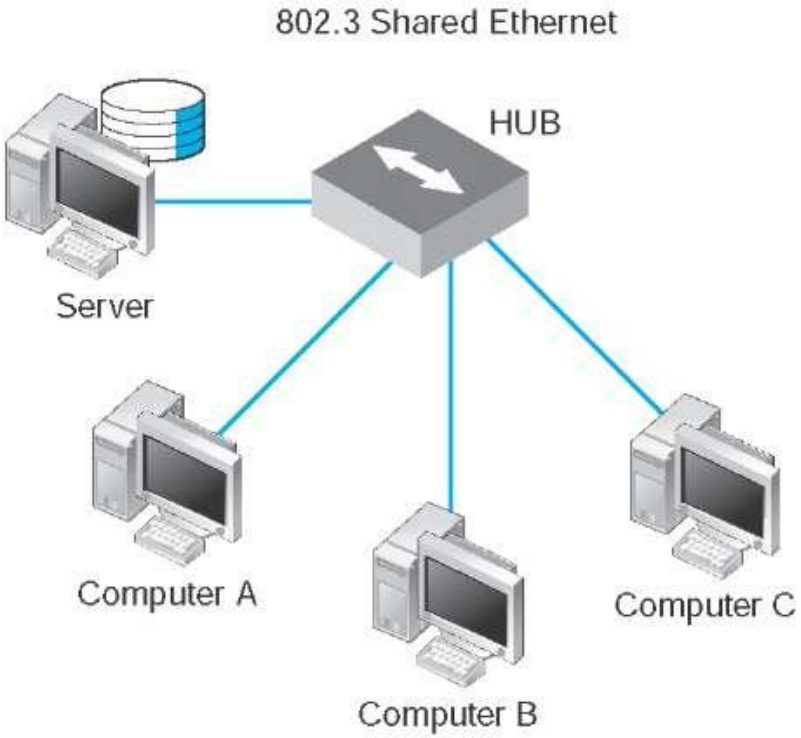
Star topology and collision-free Ethernet



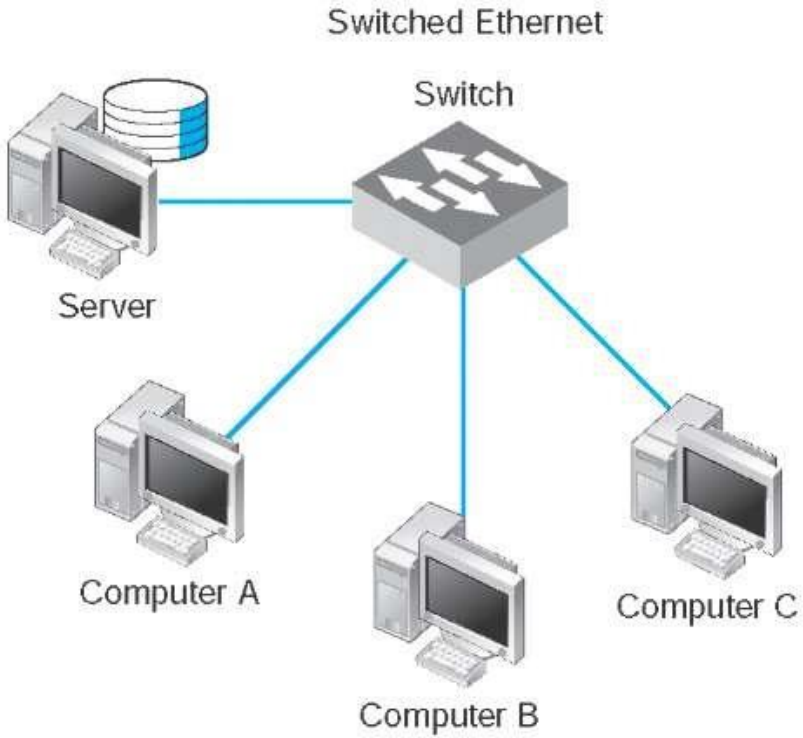
- **Same collision domain**

Star topology with hub

Star topology and collision-free Ethernet



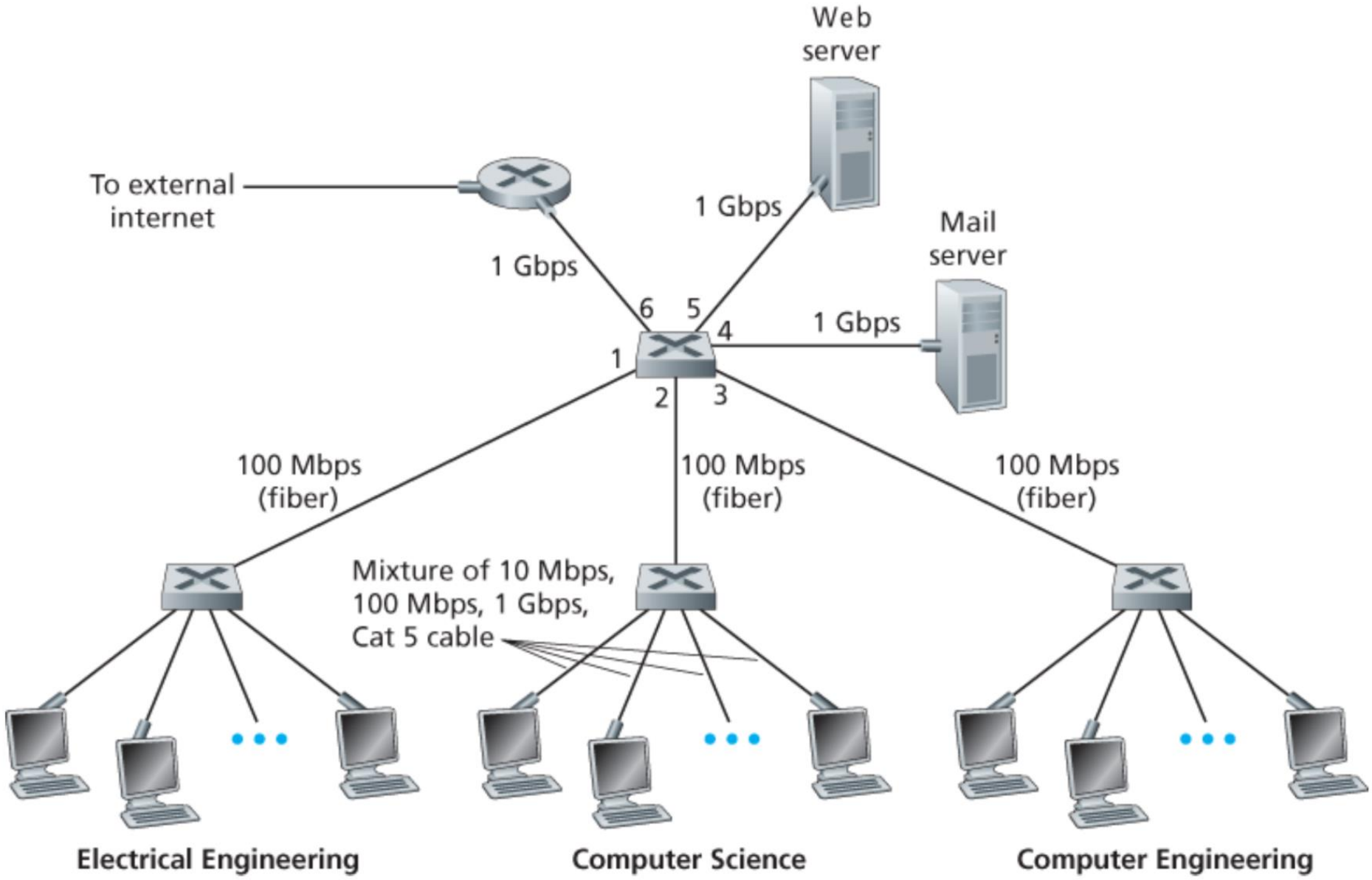
- Same collision domain



+ Separates the collision domain.
+ Buffers simultaneous packets sent to a host.

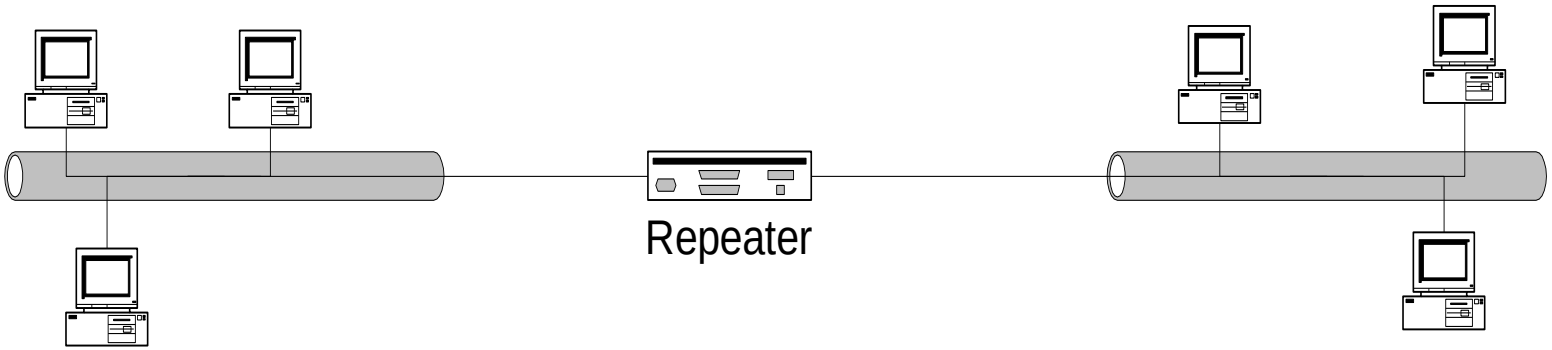
Star topology with hub and switch

Repeaters, Hubs, Bridges and Switches


Web server
To external internet
1 Gbps
1 Gbps
Mail server
1 Gbps
6
5
4
1
2
3
100 Mbps (fiber)
100 Mbps (fiber)
100 Mbps (fiber)
Mixture of 10 Mbps, 100 Mbps, 1 Gbps, Cat 5 cable
Electrical Engineering
Computer Science
Computer Engineering

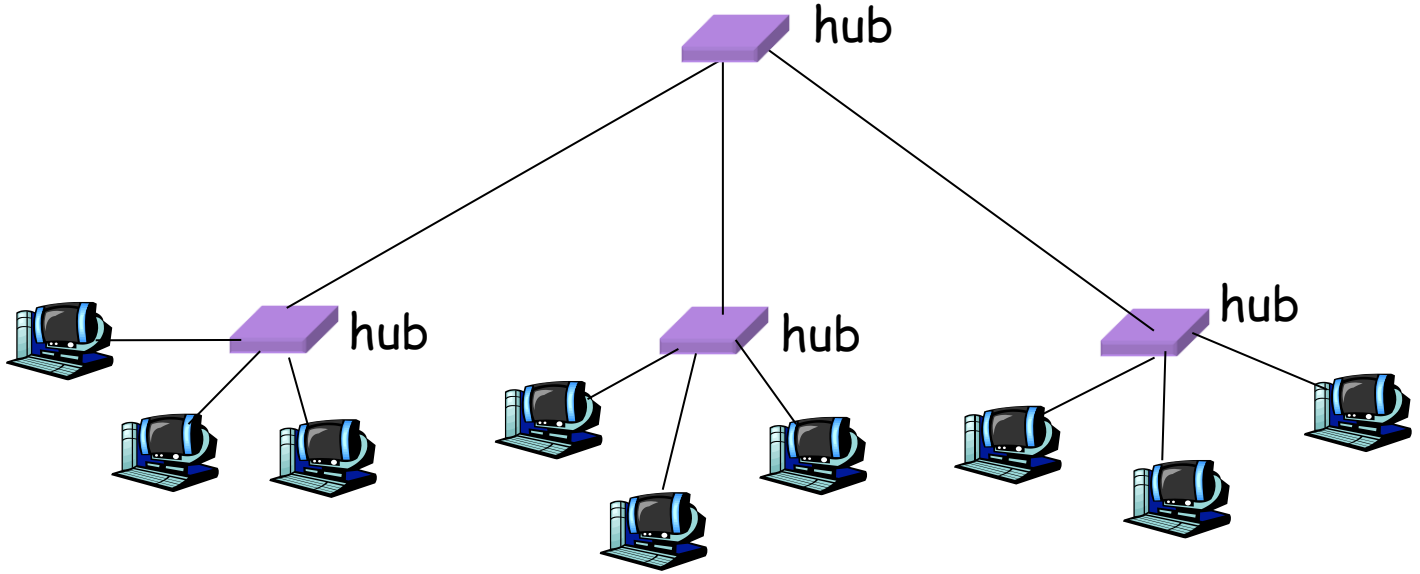
Physical Layer: Repeaters

- Distance limitation in local-area networks
  - Electrical signal becomes weaker as it travels
  - Imposes a limit on the length of a LAN
- Repeaters join LANs together
  - Analog electronic device
  - Continuously monitors electrical signals
  - Transmits an amplified copy

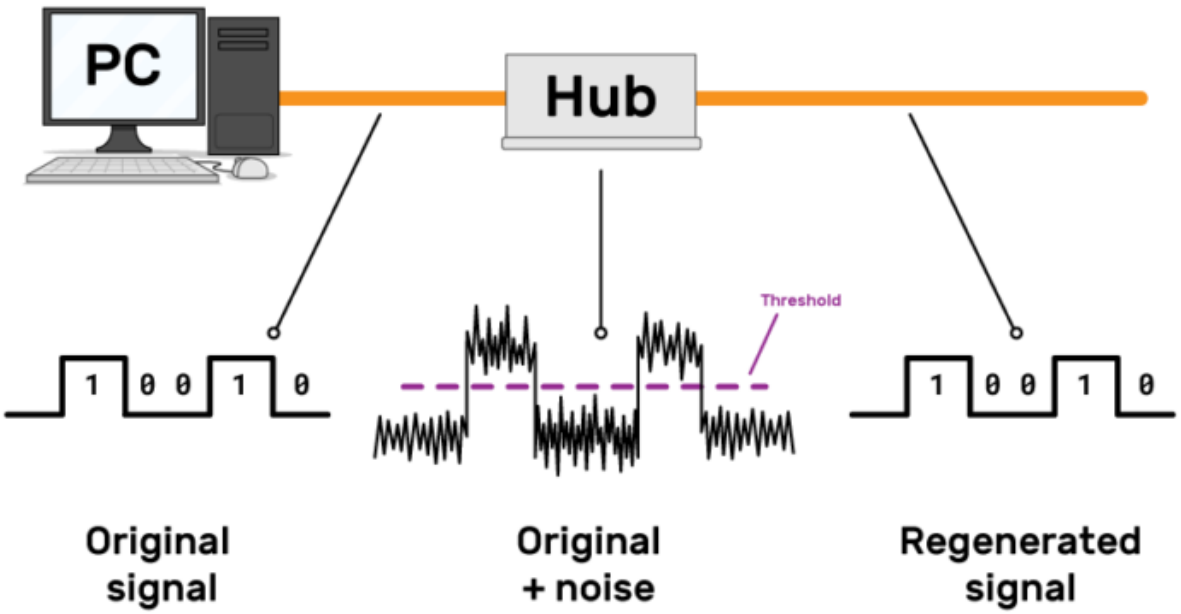


Physical Layer: Hubs

- Joins multiple input lines electrically
  - Designed to hold multiple line cards
  - Do not necessarily amplify the signal
- Very similar to repeaters
  - Also operates at the physical layer



Physical Layer: Hubs

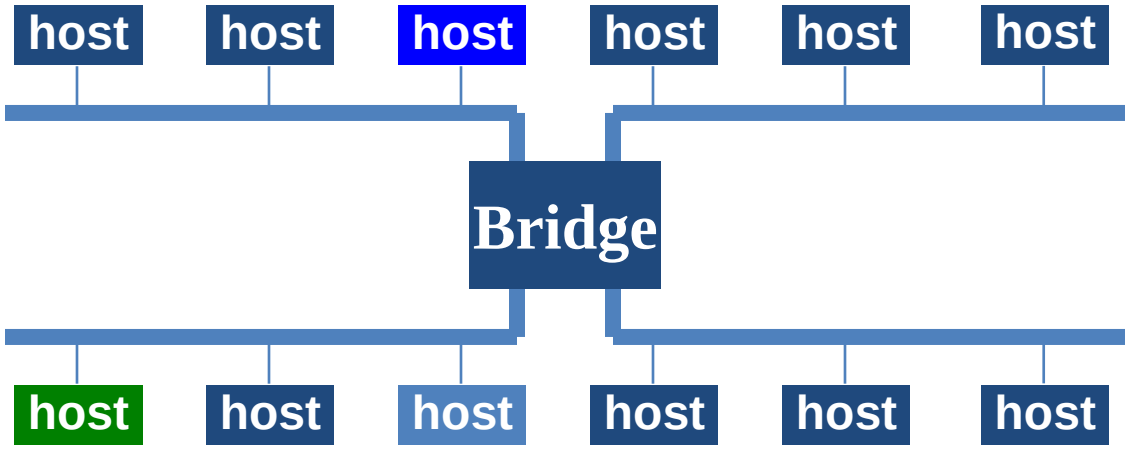


Limitations of Repeaters and Hubs

- One large shared link
  - Each bit is sent everywhere
  - So, aggregate throughput is limited
- Cannot support multiple LAN technologies
  - Does not buffer or interpret frames
  - Can't interconnect between different rates/formats
- Limitations on maximum nodes and distances
  - Shared medium imposes length limits
  - E.g., cannot go beyond 2500 meters on Ethernet

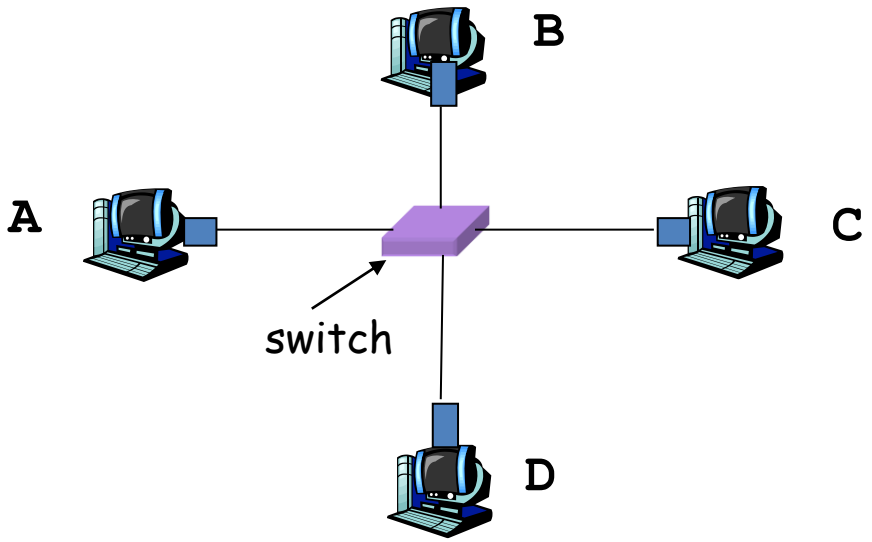
Link Layer: Bridges

- Connects two or more LANs at the link layer
  - Extracts destination address from the frame
  - Looks up the destination in a table
  - Forwards the frame to the appropriate segment
- Each segment can carry its own traffic



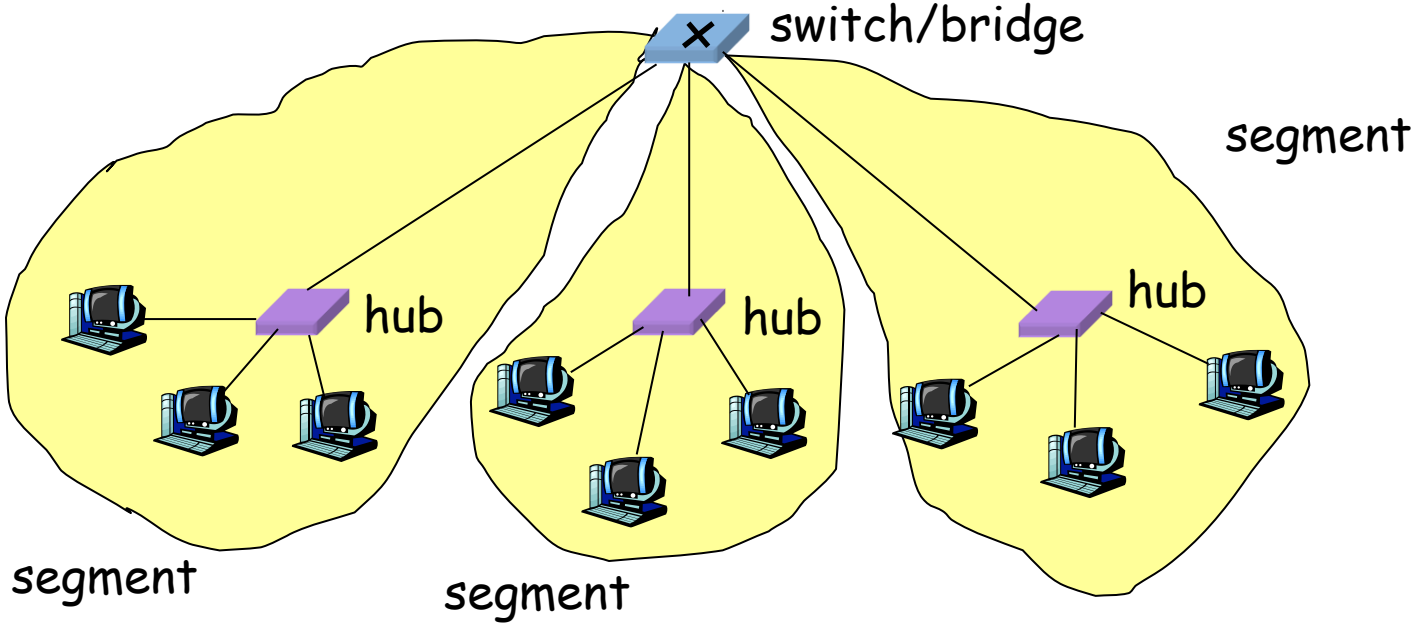
Link Layer: Switches

- Typically connects individual computers
  - A switch is essentially the same as a bridge
  - … though typically used to connect hosts
- Supports concurrent communication
  - Host A can talk to C, while B talks to D



Bridges/Switches: Traffic Isolation

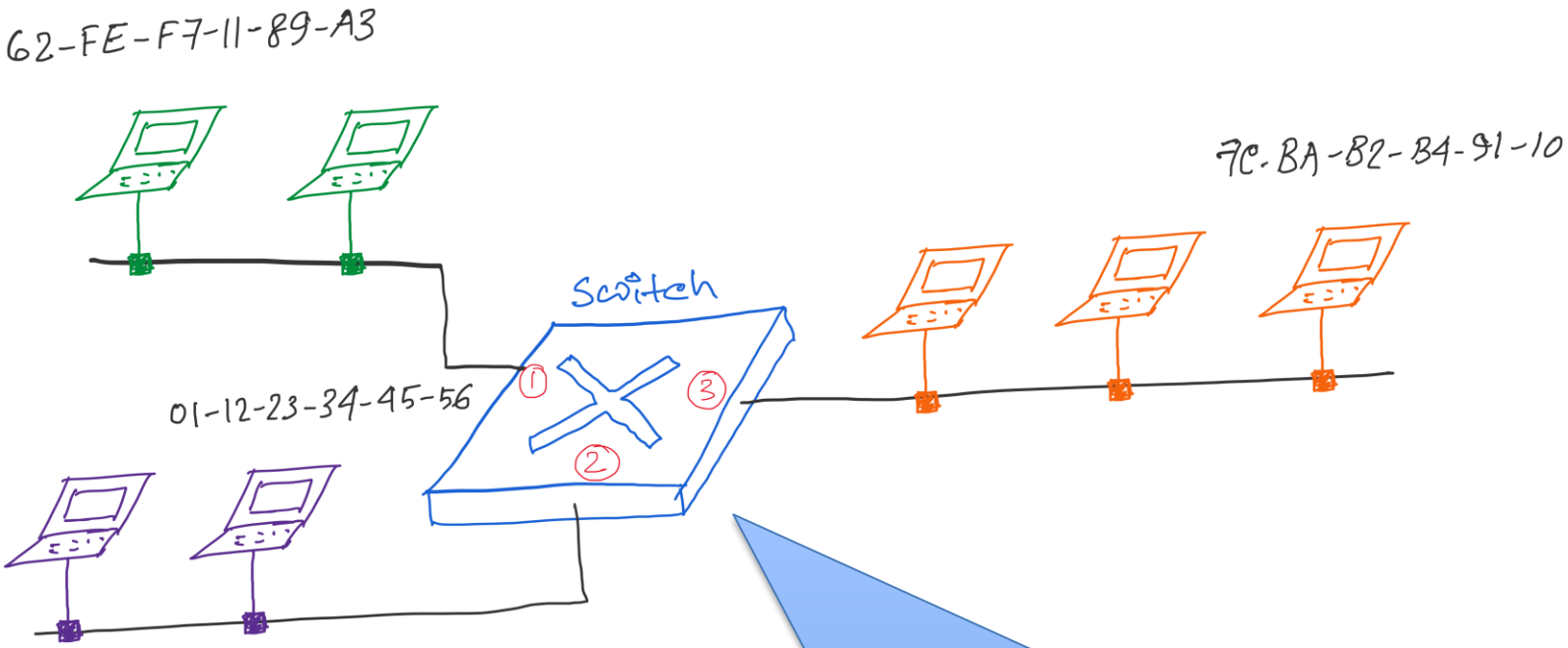
- Switch filters packets
  - Frame only forwarded to the necessary segments
  - Segments can support separate transmissions



Advantages Over Hubs/Repeaters

- Only forwards frames as needed
  - Avoid unnecessary load on segments
- Wider geographic span
  - Separate segments allow longer distances
- Improves privacy
  - Hosts can "snoop" traffic traversing their segment
  - … but not all the rest of the traffic
- Can join segments using different technologies

Traffic Isolation: Example

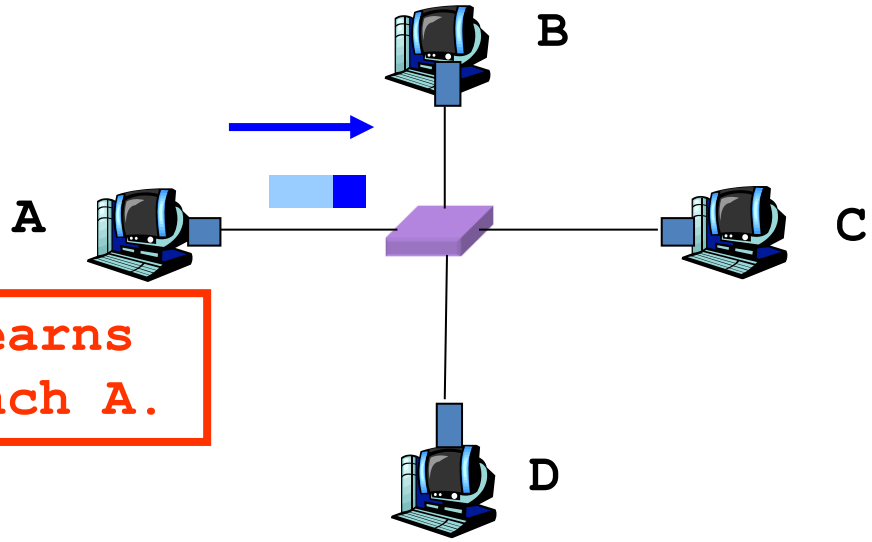


Address	Interface	Time
01-12-23-34-45-56	2	9:39
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
....	....	....

Switch table

Self Learning: Building the Table

- When a frame arrives
  - Inspect the *source* MAC address
  - Associate the address with the *incoming* interface
  - Store the mapping in the switch table
  - Use a timer to eventually forget the mapping



Switch learns how to reach A.

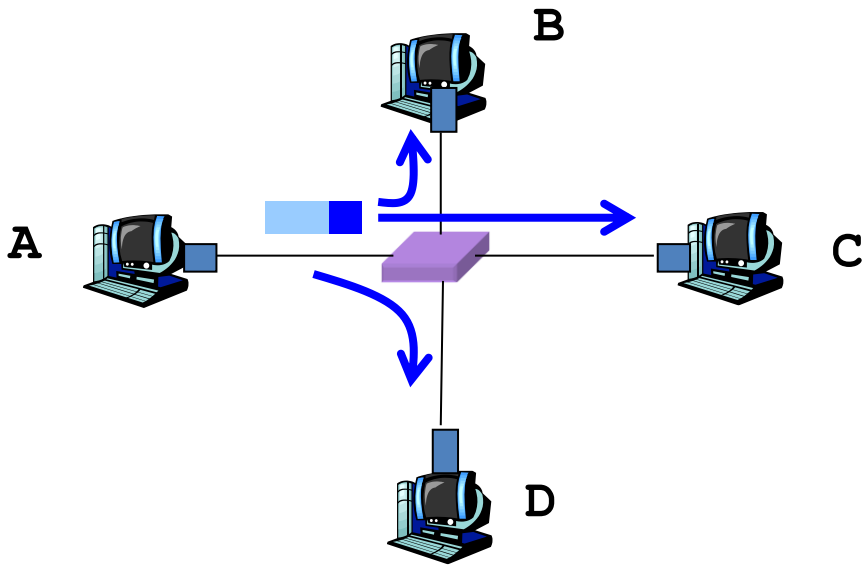
Self Learning: Handling Misses

- When frame arrives with unfamiliar destination

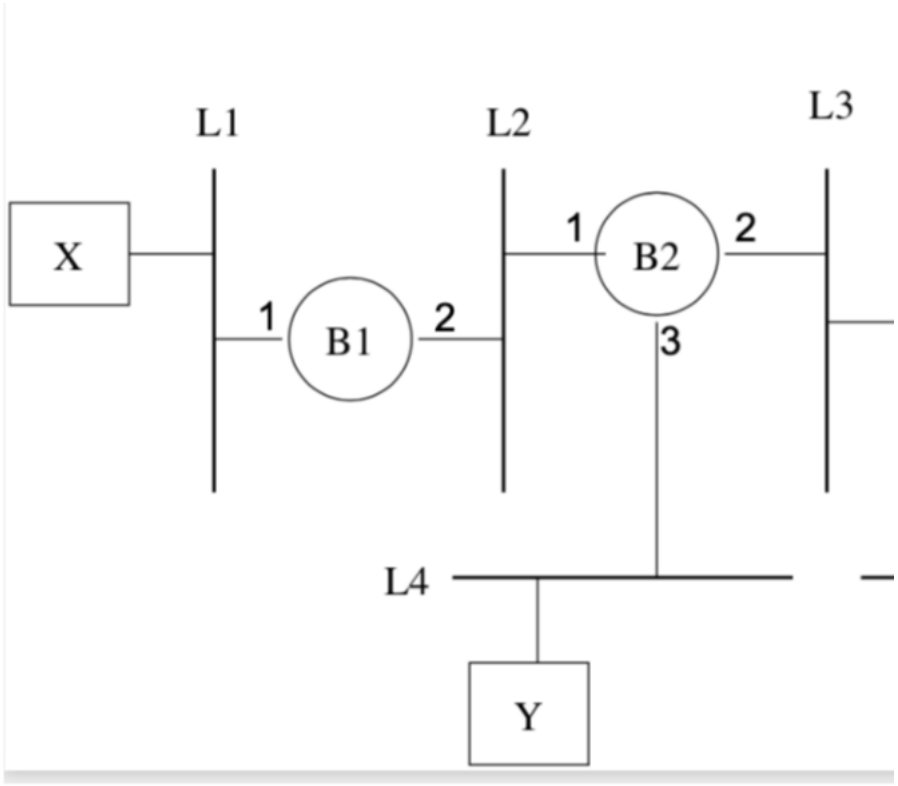
(i.e., the information is not present in the table)

  - Forward the frame out all of the interfaces
  - … except for the one where the frame arrived
  - Hopefully, this case won't happen very often!

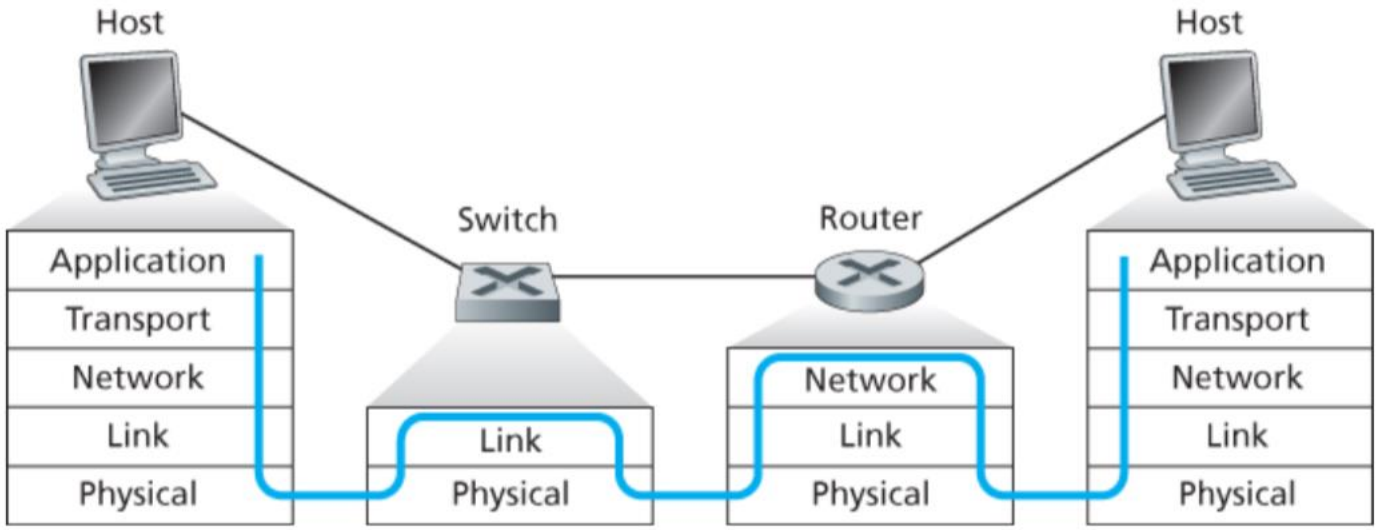
When in doubt, shout!



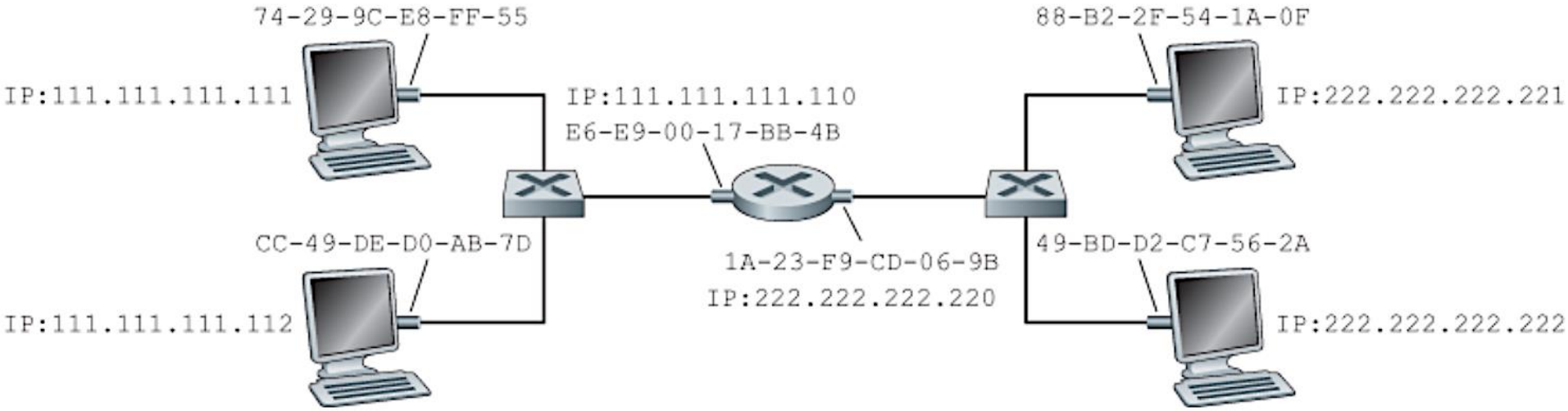
Problems related to learning-bridges/switches



Switch/Bridge vs Router



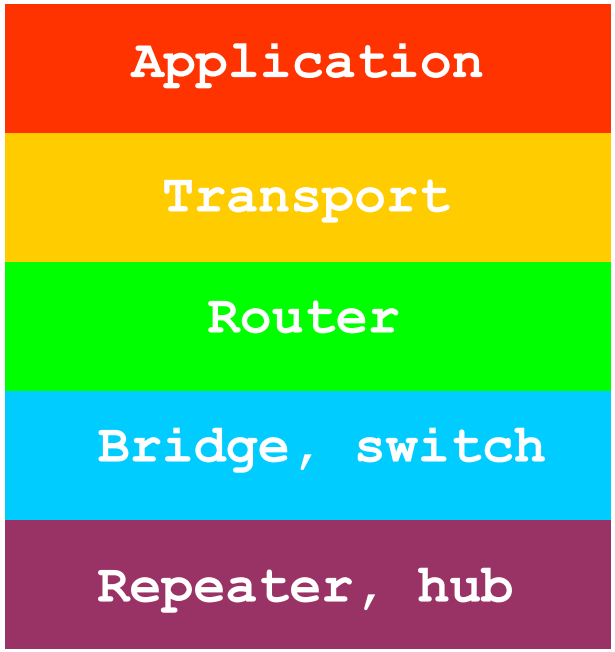
Problems related to learning-bridges/switches and routers

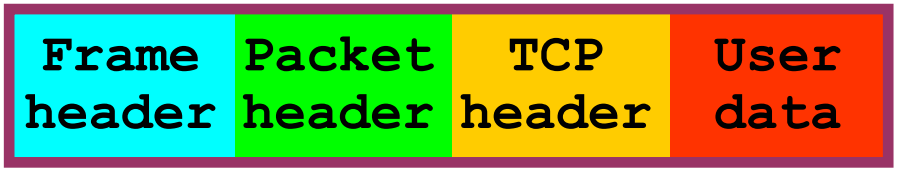


Problems related to learning-bridges/switches and routers

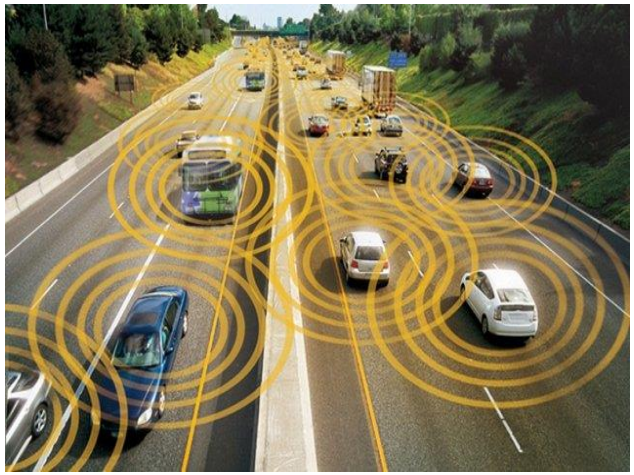
Summary: Multiple Layers

- Different devices switch different things
  - Network layer: packets (routers)
  - Link layer: frames (bridges and switches)
  - Physical layer: electrical signals (repeaters and hubs)









Wireless Networks

Widespread Deployment

- Worldwide cellular subscribers
  - 1993: 34 million
  - 2005: more than 2 billion
  - 2009: more than 4 billion

    > landline subscribers

- Wireless local area networks
  - Wireless adapters built into laptops, tablets, & phones
  - More than 220,000 known WiFi locations in 134 countries
  - Probably many, many more (e.g., home networks, corporate networks, …)

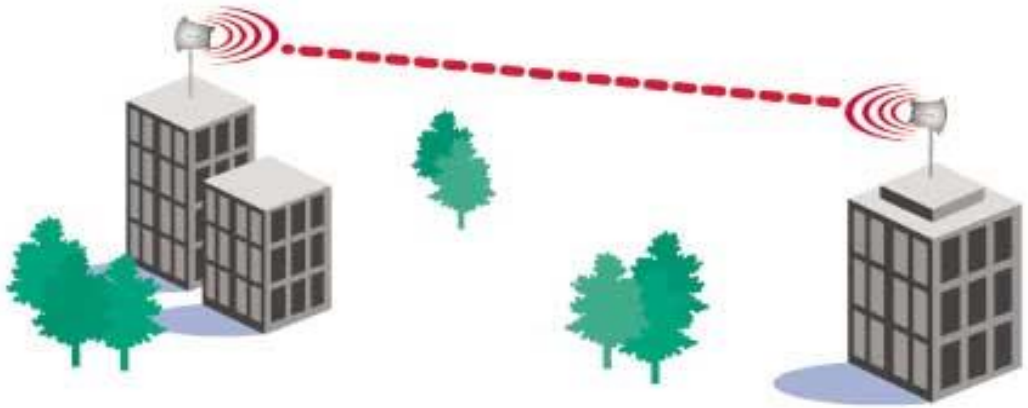
Wireless Links

Wireless Properties

- Interference / bit errors
  - More sources of corruption compared to wired
- Multipath propagation
  - Signal does not travel in a straight line
- Broadcast medium
  - All traffic to everyone
- Power trade-offs
  - Important for power constrained devices

Wireless Links: High Bit Error Rate

- Decreasing signal strength
  - Disperses as it travels greater distance
  - Attenuates as it passes through matter

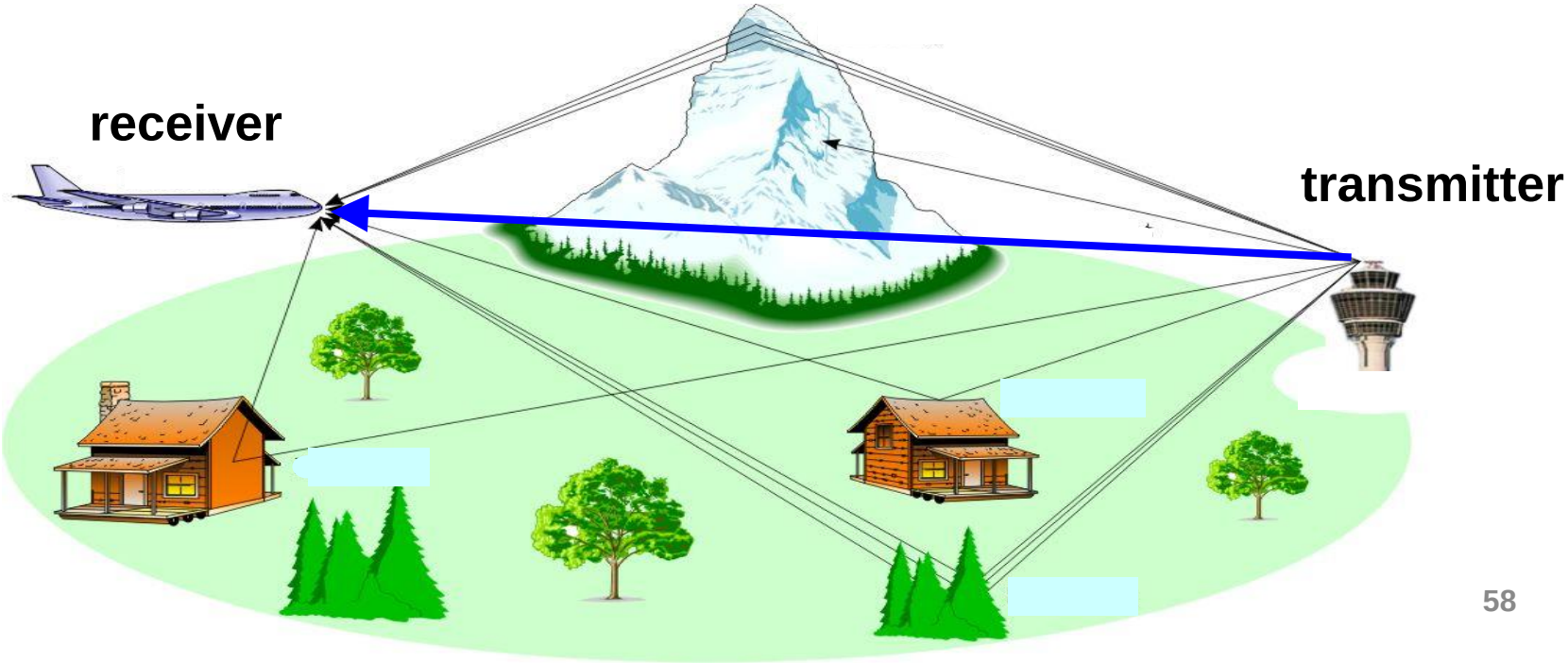


Wireless Links: High Bit Error Rate

- Interference from other sources
  - Radio sources in same frequency band
  - E.g., 2.4 GHz wireless phone interferes with 802.11b wireless LAN
  - Electromagnetic noise (e.g., microwave oven)

Wireless Links: High Bit Error Rate

- Multi-path propagation
  - Electromagnetic waves reflect off objects
  - Taking many paths of different lengths
  - Causing blurring of signal at the receiver

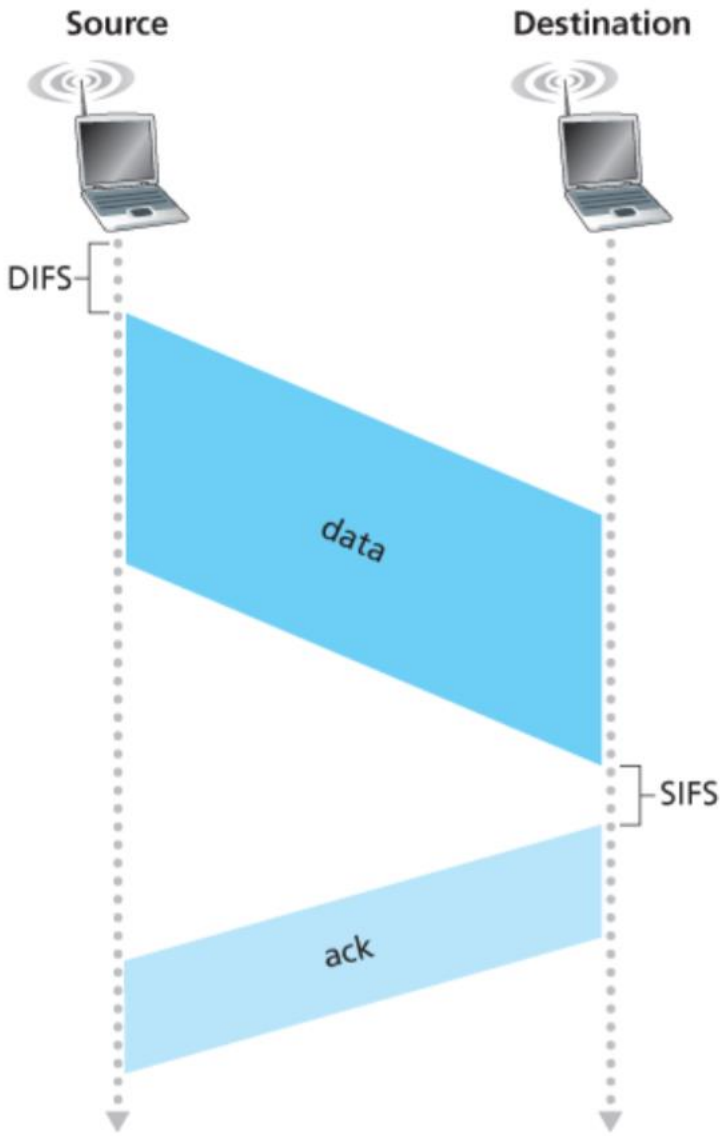


Dealing With Bit Errors

- Wireless vs. wired links
  - Wired: most loss is due to congestion
  - Wireless: higher, time-varying bit-error rate

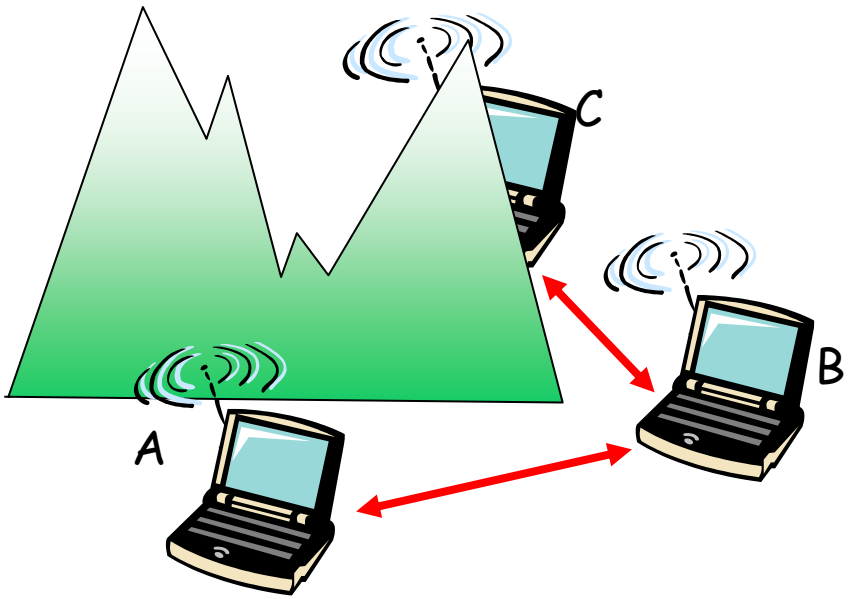
- Dealing with high bit-error rates
  - Sender could increase transmission power
    - Requires more energy (bad for battery-powered hosts)
    - Creates more interference with other senders
  - Stronger error detection and recovery
    - More powerful error detection/correction codes
    - Link-layer retransmission of corrupted frames

Link layer ACK



Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: hidden terminal problem

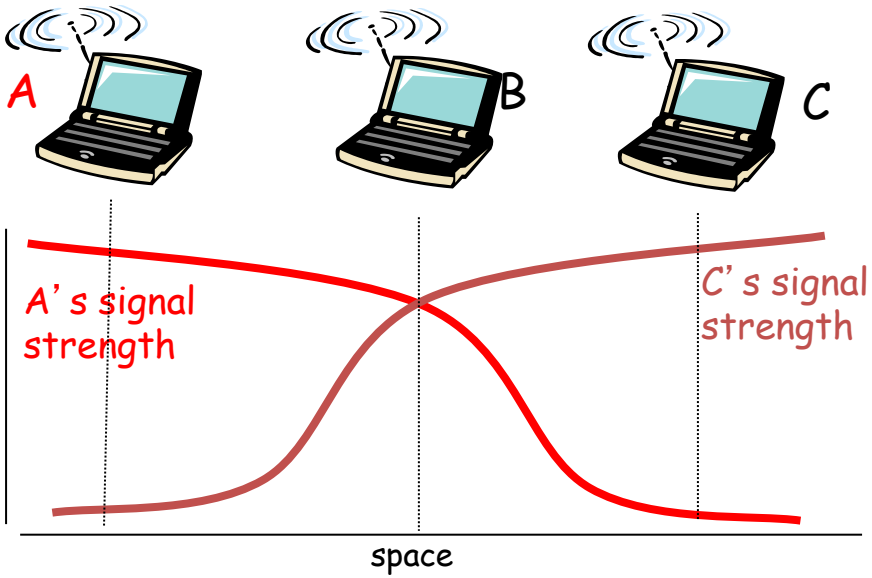


- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

So, A and C are unaware of their interference at B

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: fading over distance



- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

So, A and C are unaware of their interference at B

Example Wireless Link Technologies

- Data networks
  - 802.15.1 (Bluetooth): 2.1 Mbps – 10 m
  - 802.11b (WiFi): 5-11 Mbps – 100 m
  - 802.11a and g (WiFi): 54 Mbps – 100 m
  - 802.11n (WiFi): 200 Mbps – 100 m
  - 802.16 (WiMax): 70 Mbps – 10 km
- Cellular networks, outdoors
  - 2G: 56 Kbps
  - 3G: 384 Kbps
  - 3G enhanced (“4G”): 4 Mbps
  - LTE
  - 5G

Example Wireless Link Technologies

- Data networks
  - 802.15.1 (Bluetooth): 2.1 Mbps – 10 m
  - 802.11b (WiFi): 5-11 Mbps – 100 m
  - 802.11a and g (WiFi): 54 Mbps – 100 m
  - 802.11n (WiFi): 200 Mbps – 100 m
  - 802.16 (WiMax): 70 Mbps – 10 km
- Cellular networks, outdoors
  - 2G: 56 Kbps
  - 3G: 384 Kbps
  - 3G enhanced ("4G"): 4 Mbps
  - LTE
  - 5G

WiFi: IEEE 802.11 Wireless LANs

A quick comparison of the different Wifi generations is given in the table below:

Standard	Other Name	Available Year	Single-stream Speed (via highest channelwidth)	Operating Channels	Freqyency Bands	Status
802.11b	–	1999	11 Mbps	20 MHz	2.4 GHz	obsolete
802.11ba	–	2000	54 Mbps	20 MHz	5GHz	obsolete
802.11g	–	2003	54 Mbps	20 MHz	2.4GHz	obsolete
802.11n or Wireless N	Wifi 4	2009	150 Mbps	20 HMHz / 40 MHz	2.4 GHz and 5 GHz	Legacy
802.11ac	Wifi 5	2012	433 Mbps	20 HMHz / 40 MHz / 80 MHz	5GHz	Mainstream
802.11ad	–	2015	Up to 7 Gbps	2.16 GHz	60GHz	Limited use
802.11ax	Wifi 6	2019	1200 Mbps	20 HMHz / 40 MHz / 80 MHz / 160 MHz	2.4 GHz and 5 GHz	Latest

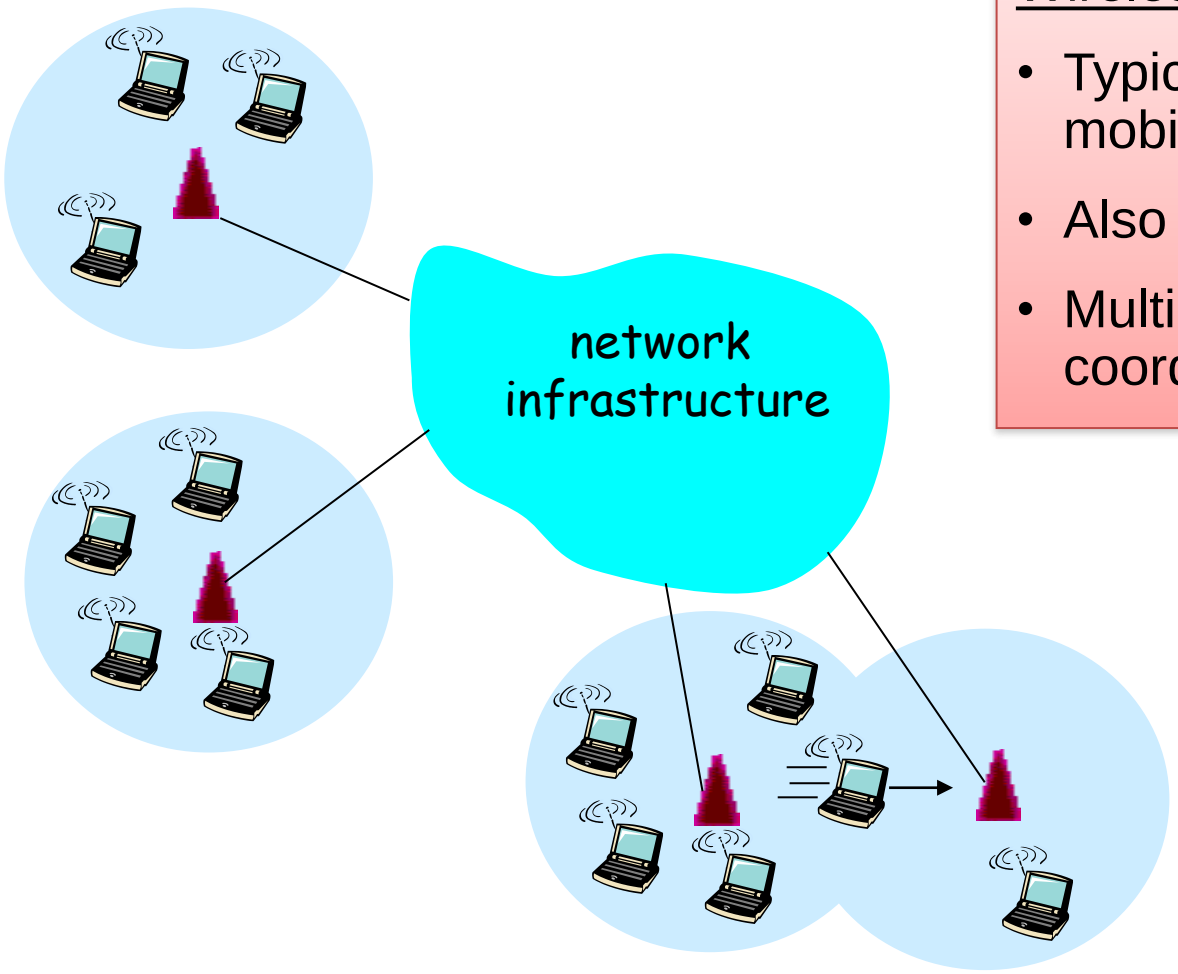
WiFi: IEEE 802.11 Wireless LANs

1. LAN Architecture
2. MAC protocol
3. Frame structure
4. Advanced features

WiFi: IEEE 802.11 Wireless LANs

1. LAN Architecture
2. MAC protocol
3. Frame structure
4. Advanced features

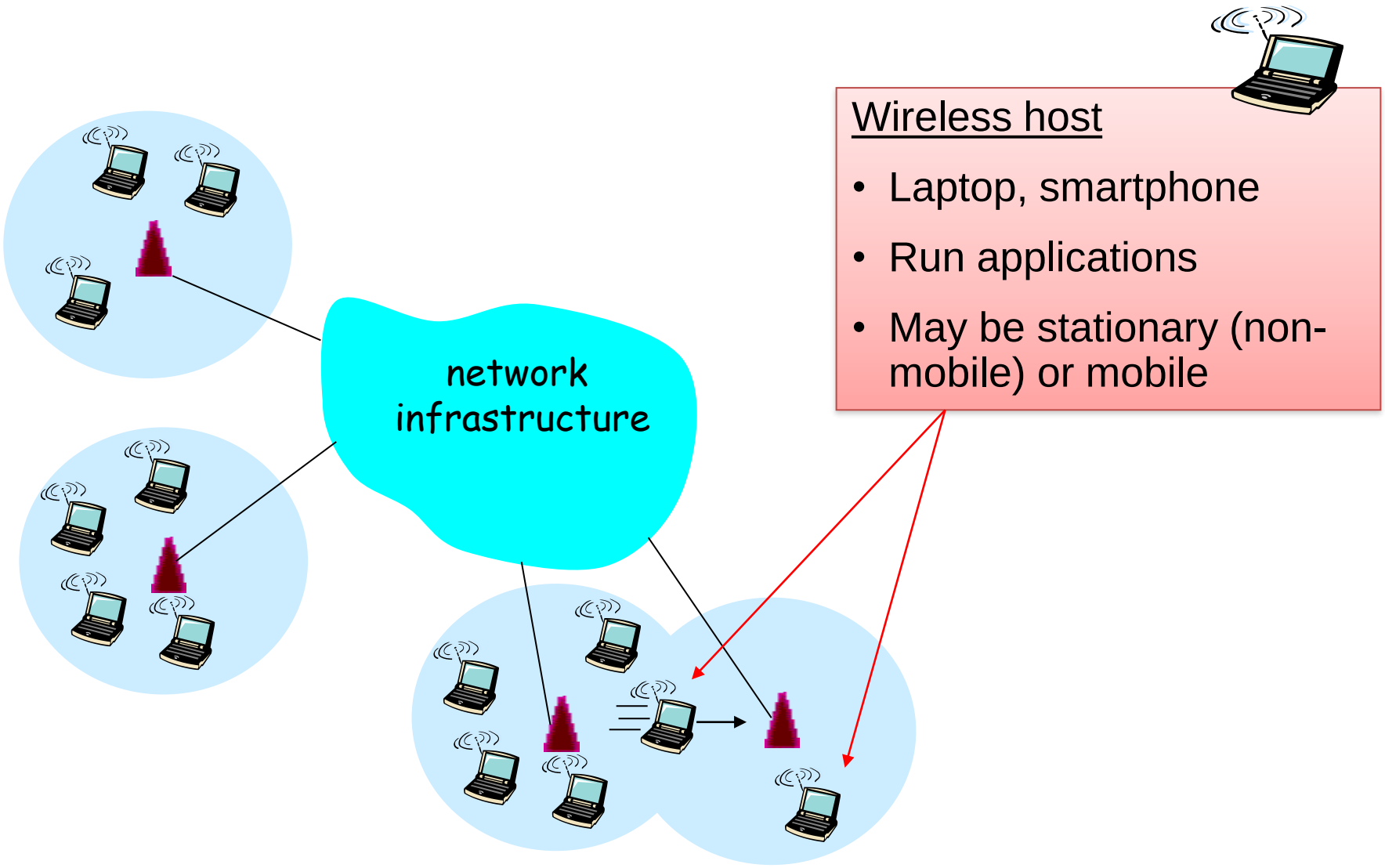
Wireless Network: Wireless Link



Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access

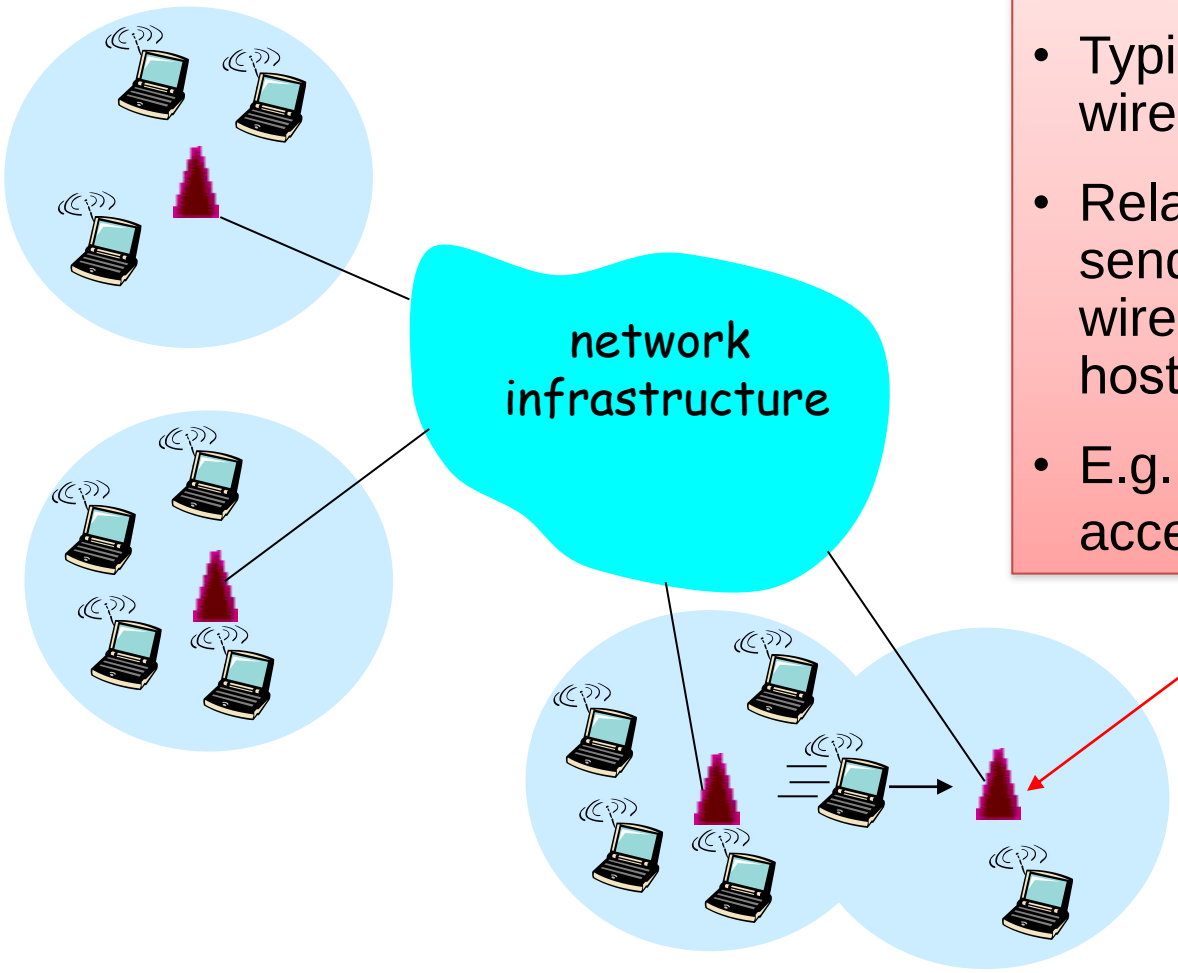
Wireless Network: Wireless Hosts



Wireless host

- Laptop, smartphone
- Run applications
- May be stationary (non-mobile) or mobile

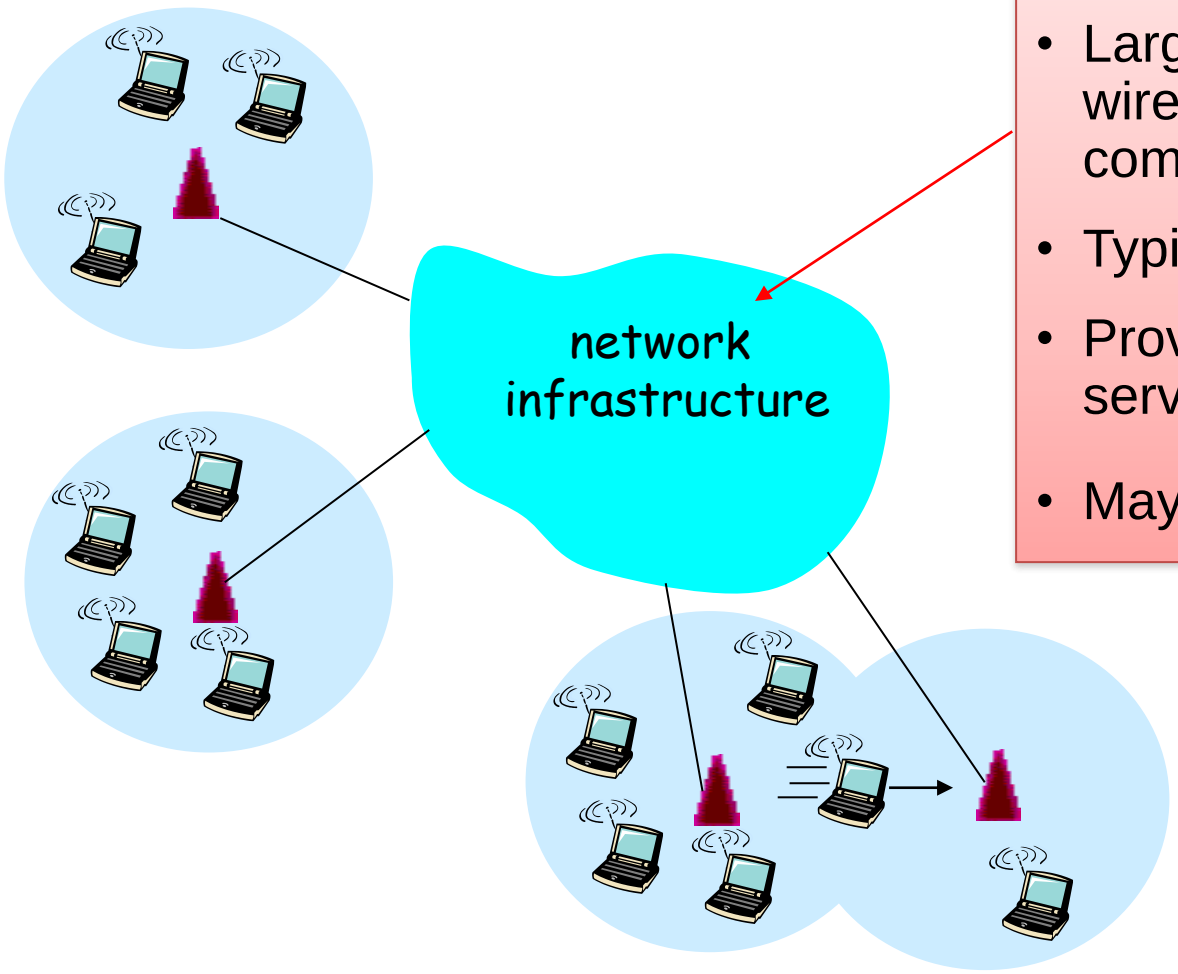
Wireless Network: Base Station



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

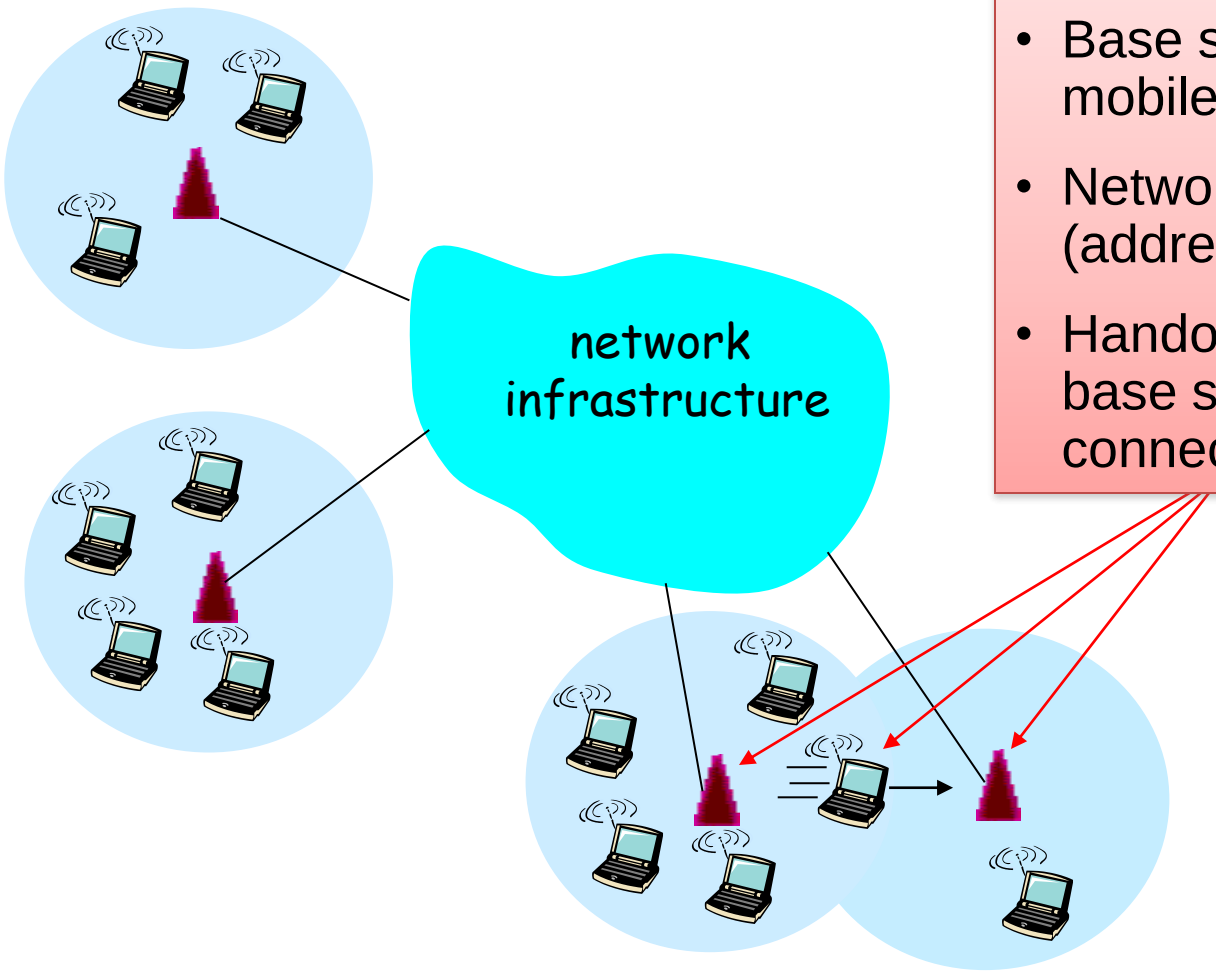
Wireless Network: Infrastructure



Network infrastructure

- Larger network with which a wireless host wants to communicate
- Typically a wired network
- Provides traditional network services
- May not always exist

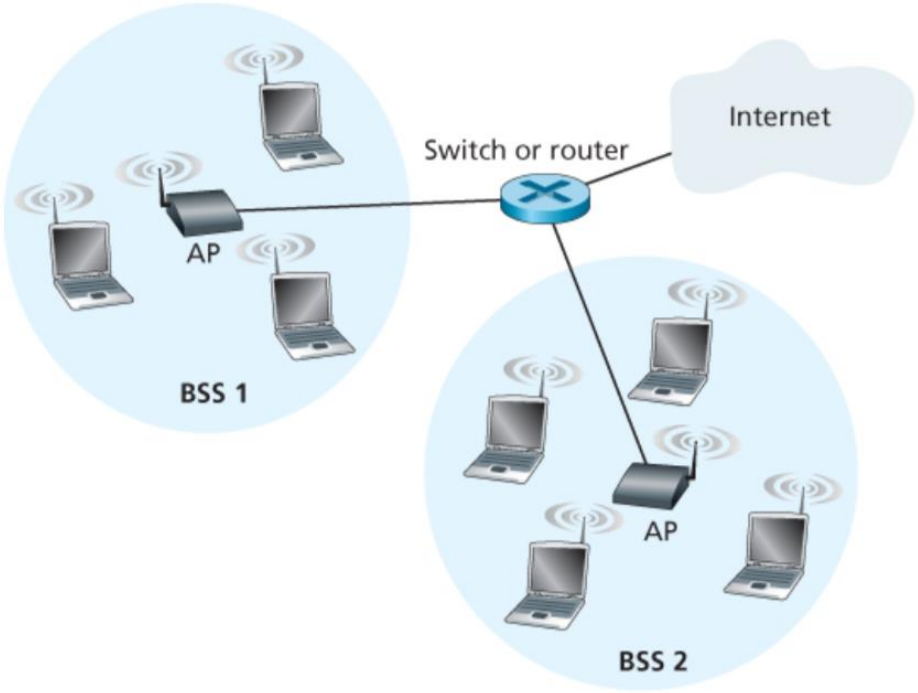
Infrastructure Mode (APs)



Infrastructure mode

- Base station connects mobiles into wired network
- Network provides services (addressing, routing, DNS)
- Handoff: mobile changes base station providing connection to wired network

802.11 LAN Architecture

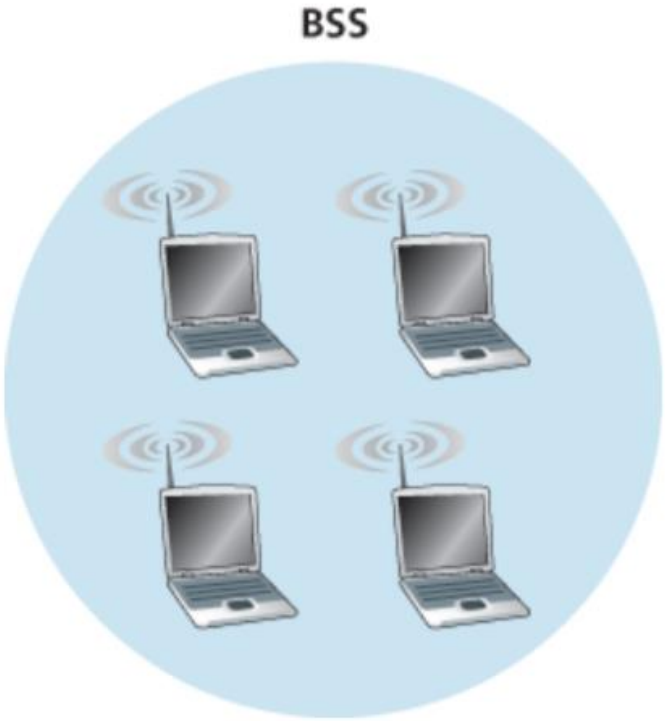


- Access Point (AP)
  - Base station that communicates with the wireless hosts
- Basic Service Set (BSS)
  - Coverage of one AP
  - AP acts as the master
  - Identified by a "network name" known as an SSID

SSID: Service Set Identifier

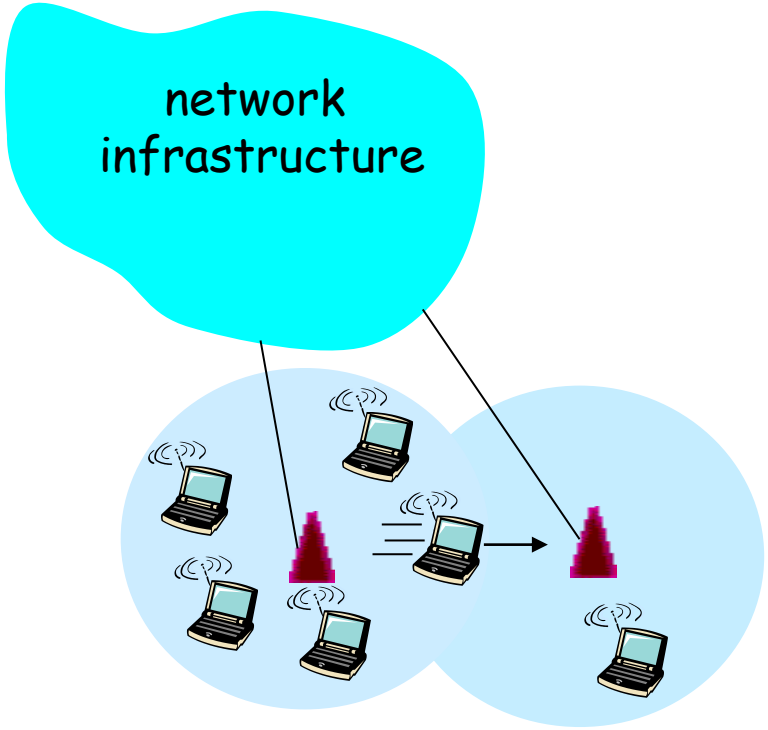
(1) Infrastructure wireless LAN

802.11 LAN Architecture



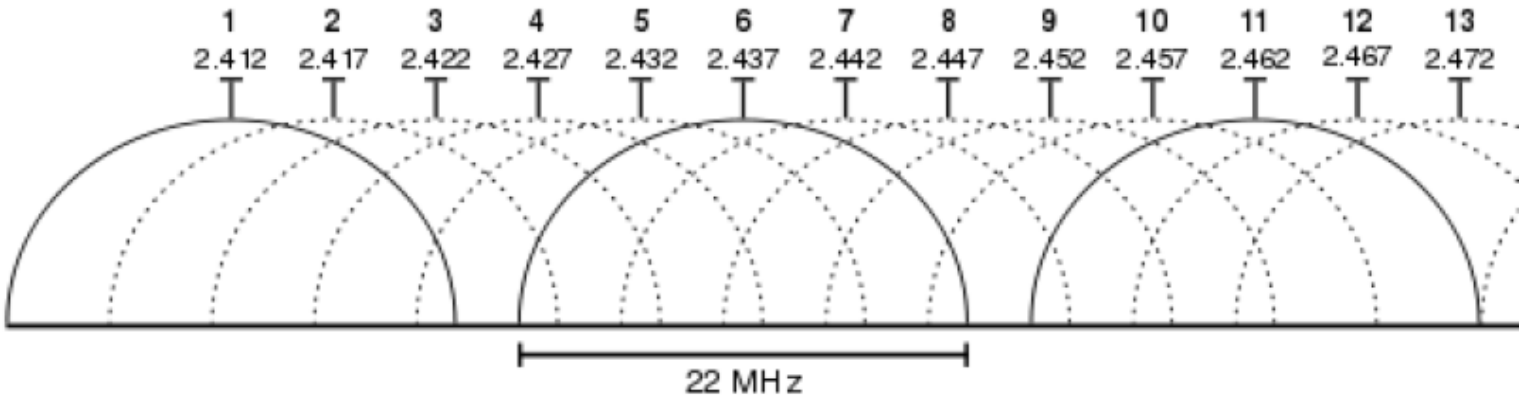
(2) Ad hoc wireless LAN

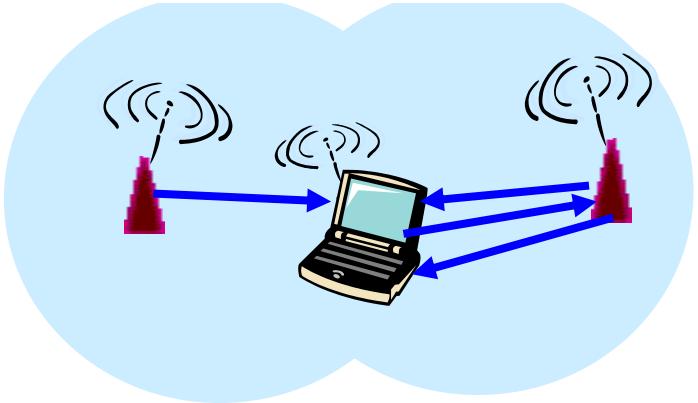
Channels and Association



Channels and Association

- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP

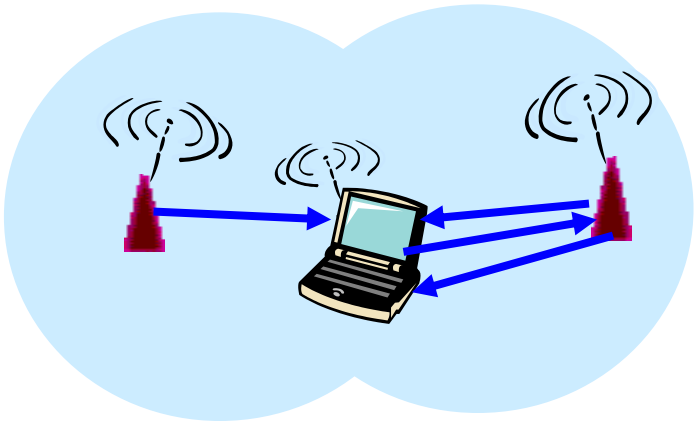




- Beacon frames from APs
- Associate request from host
- Association response from AP

Channels and Association

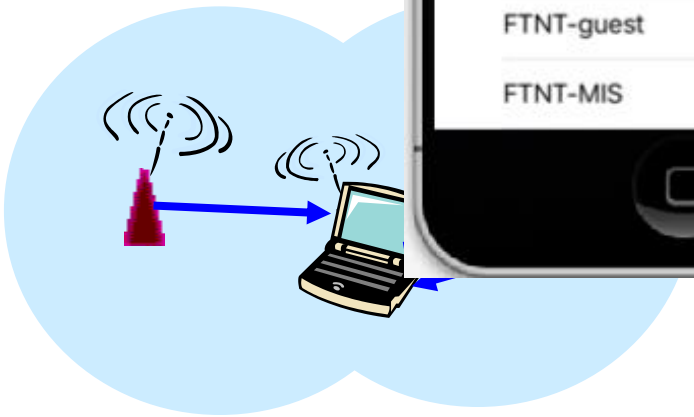
- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP
- Access points send periodic beacon frames
  - Containing AP's name (SSID) and MAC address
  - Host scans channels, listening for beacon frames
  - Host selects an access point to associate with



- Beacon frames from APs
- Associate request from host
- Association response from AP

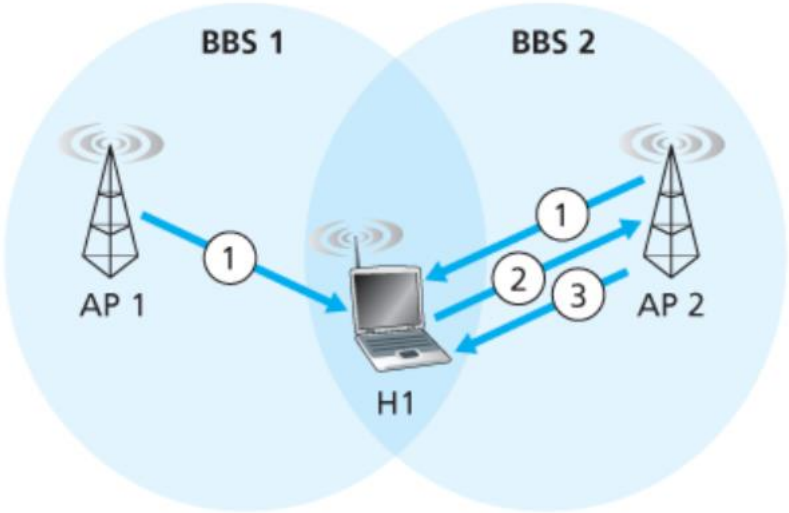
Channels and Association

- Multiple chann quencies
  - Network admi quency for AP
  - Interference if eighboring AP
- Access points s on frames
  - Containing AP AC address
  - Host scans cha eacon frames
  - Host selects ar ciate with



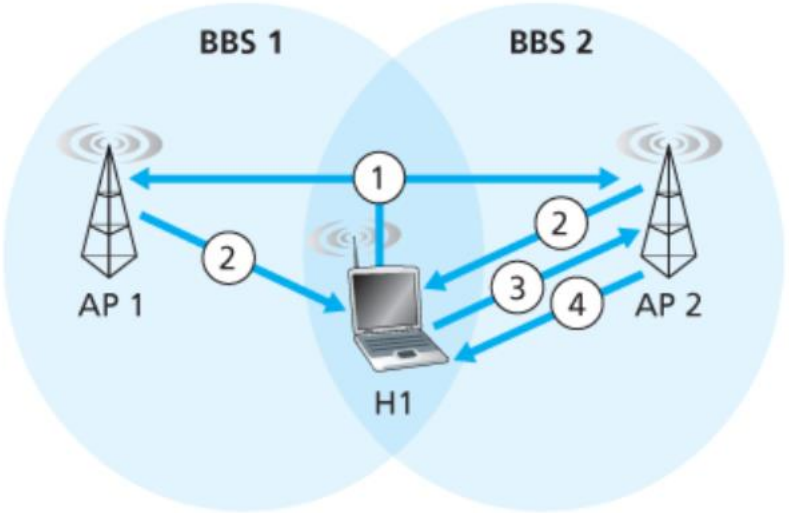
on frames from APs
ciate request from host
ciation response from AP

Scanning: Passive and active



a. Passive scanning

1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1

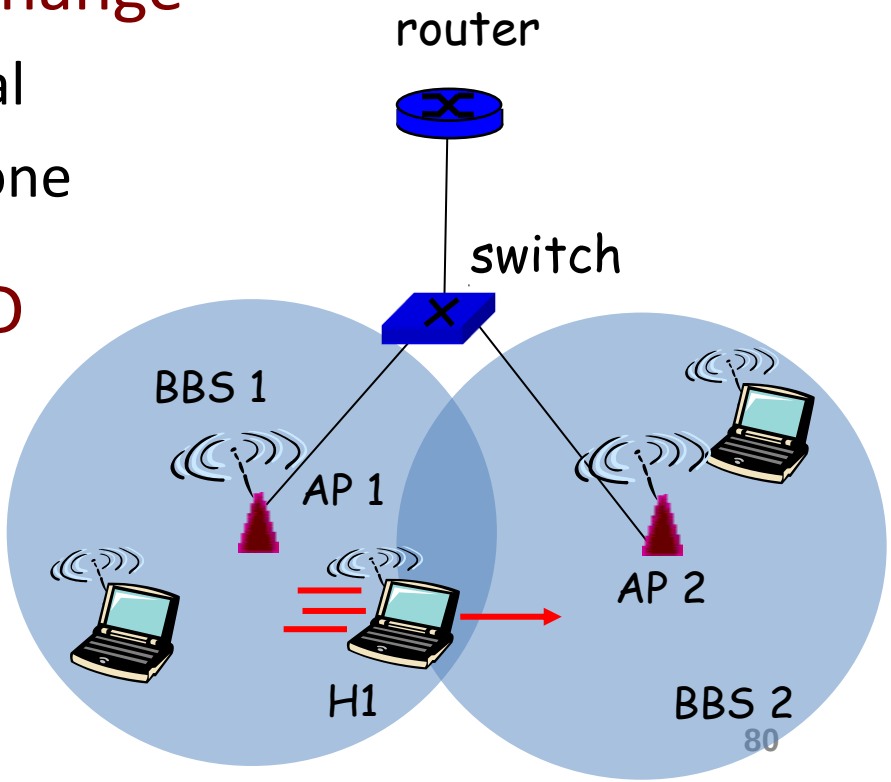


a. Active scanning

1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Mobility Within the Same Subnet

- H1 remains in same IP subnet
  - IP address of the host can remain same
  - Ongoing data transfers can continue uninterrupted
- H1 recognizes the need to change
  - H1 detects a weakening signal
  - Starts scanning for stronger one
- Changes APs with same SSID
  - H1 disassociates from one
  - And associates with other
- Switch learns new location
  - Self-learning mechanism

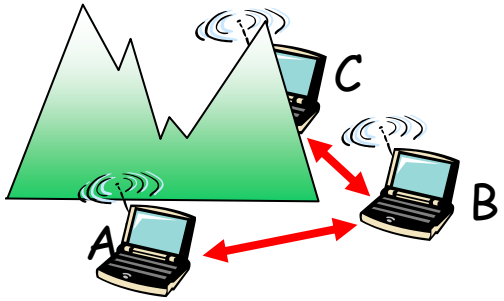


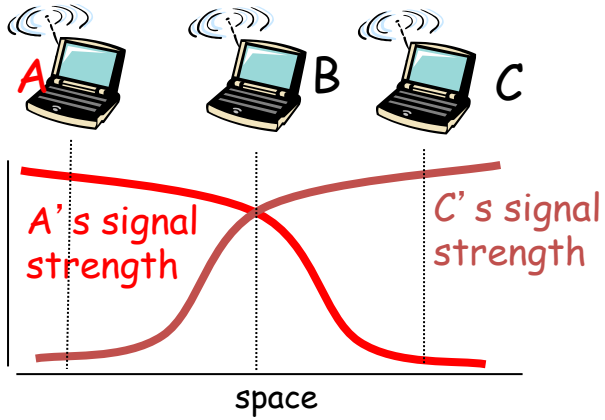
WiFi: IEEE 802.11 Wireless LANs

1. LAN Architecture
2. MAC protocol
3. Frame structure
4. Advanced features

CSMA: Carrier Sense, Multiple Access

- Multiple access: channel is shared medium
  - Station: wireless host or access point
  - Multiple stations may want to transmit at same time
- Carrier sense: sense channel before sending
  - Station doesn't send when channel is busy
  - To prevent collisions with ongoing transfers
  - But, detecting ongoing transfers isn't always possible





CSMA/CA: Collision Avoidance (CA), Not Collision Detection (CD)

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again

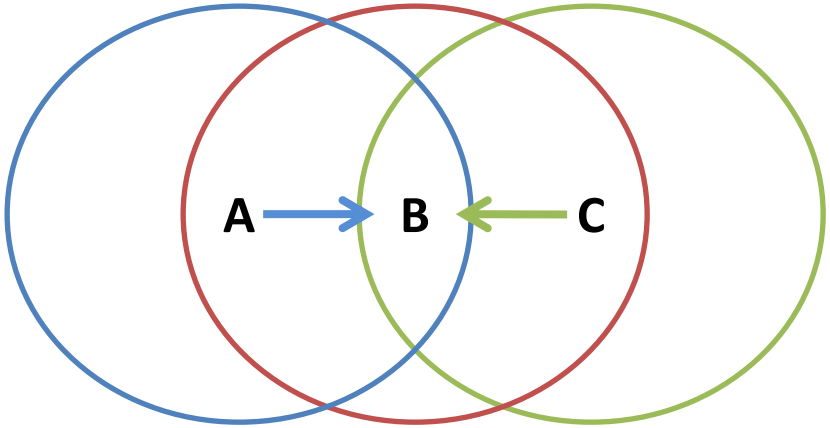
CSMA/CA: Collision Avoidance (CA), Not Collision Detection (CD)

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again
- Problem #1: cannot detect all collisions
  - Hidden terminal problem
  - Fading

CA: Collision Avoidance, Not Detection

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again
- Problem #1: cannot detect all collisions
  - Hidden terminal problem
  - Fading
- Problem #2: Can not listen while sending
  - Strength of received signal is much smaller
  - Expensive to build hardware that detects collisions
- So, 802.11 does collision avoidance, not detection

Hidden Terminal Problem

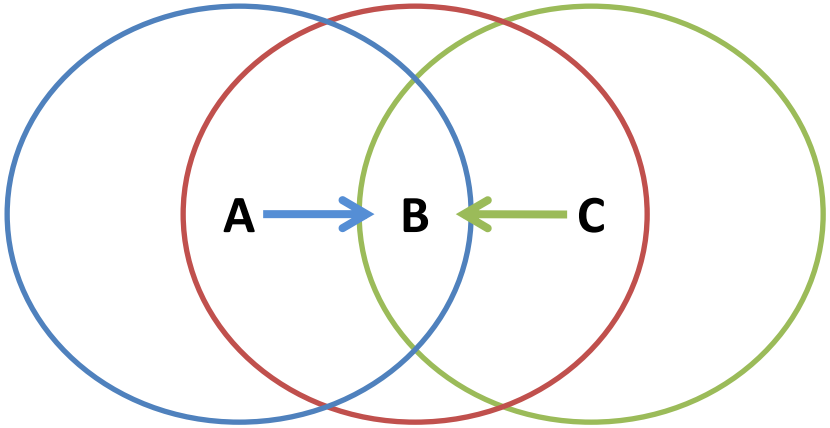


- A and C can't see each other, both send to B
- Occurs since 802.11 relies on physical carrier sensing, which is susceptible to hidden terminal problem

Virtual carrier sensing

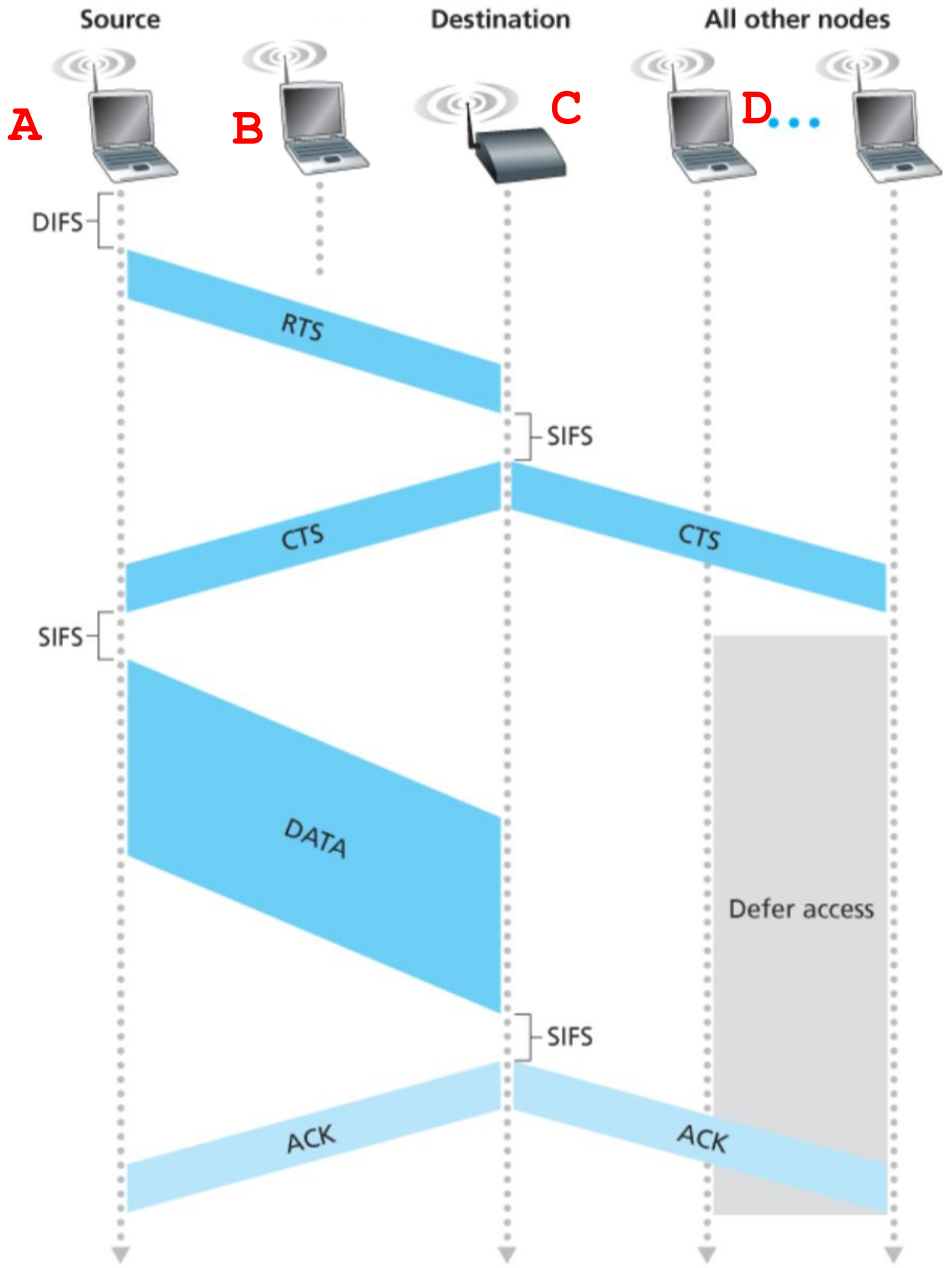
- First exchange control frames before transmitting data
  - Sender issues "Request to Send" (RTS), incl. length of data
  - Receiver responds with "Clear to Send" (CTS)
- If sender sees CTS, transmits data (of specified length)
- If other node sees CTS, will idle for specified period
- If other node sees RTS but not CTS, free to send

Hidden Terminal Problem

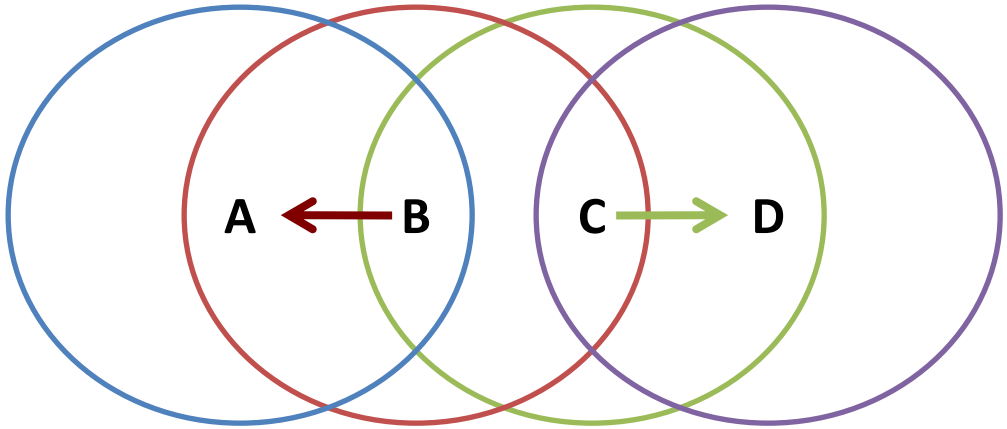


- A and C can't see each other, both send to B
- RTS/CTS can help
  - Both A and C would send RTS that B would see first
  - B only responds with one CTS (say, echo'ing A's RTS)
  - C detects that CTS doesn't match and won't send

Virtual carrier sensing (RTS-CTS)



Exposed Terminal Problem



- B sending to A, C wants to send to D
- As C receives B's packets, carrier sense would prevent it from sending to D, even though wouldn't interfere
- RTS/CTS can help
  - C hears RTS from B, but not CTS from A
  - C knows it's transmission will not interfere with A
  - C is safe to transmit to D

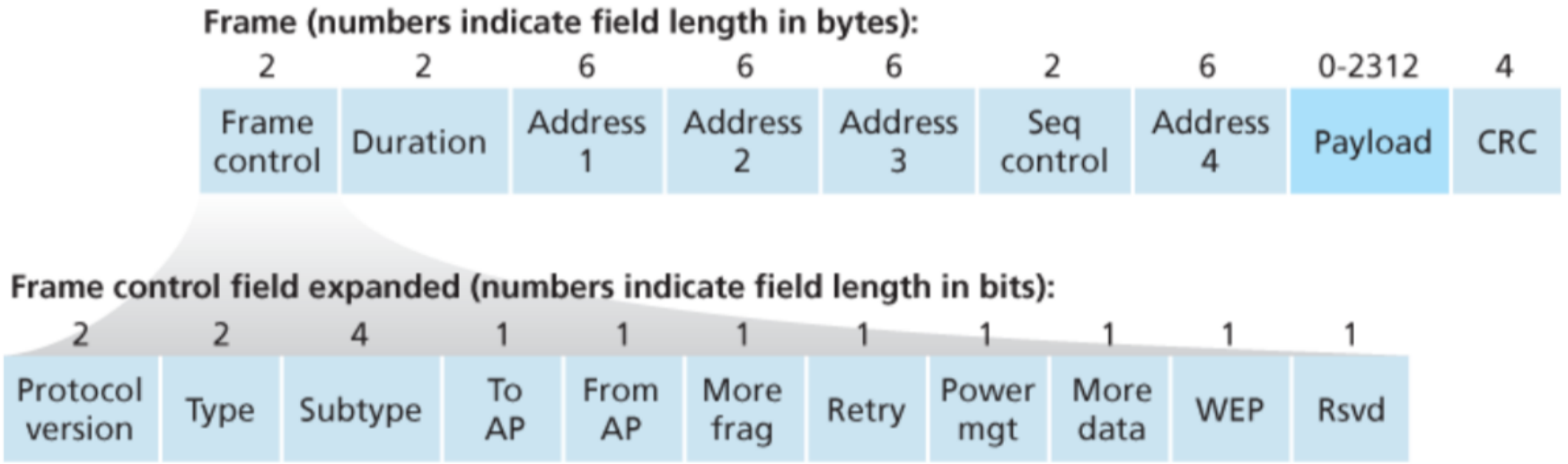
Impact on Higher-Layer Protocols

- Wireless and mobility change path properties
  - Wireless: higher packet loss, not from congestion
  - Mobility: transient disruptions, and changes in RTT
- Logically, impact should be minimal …
  - Best-effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- But, performance definitely *is* affected
  - TCP treats packet loss as a sign of congestion
  - TCP tries to estimate the RTT to drive retransmissions
  - TCP does not perform well under out-of-order packets
- Internet not designed with these issues in mind

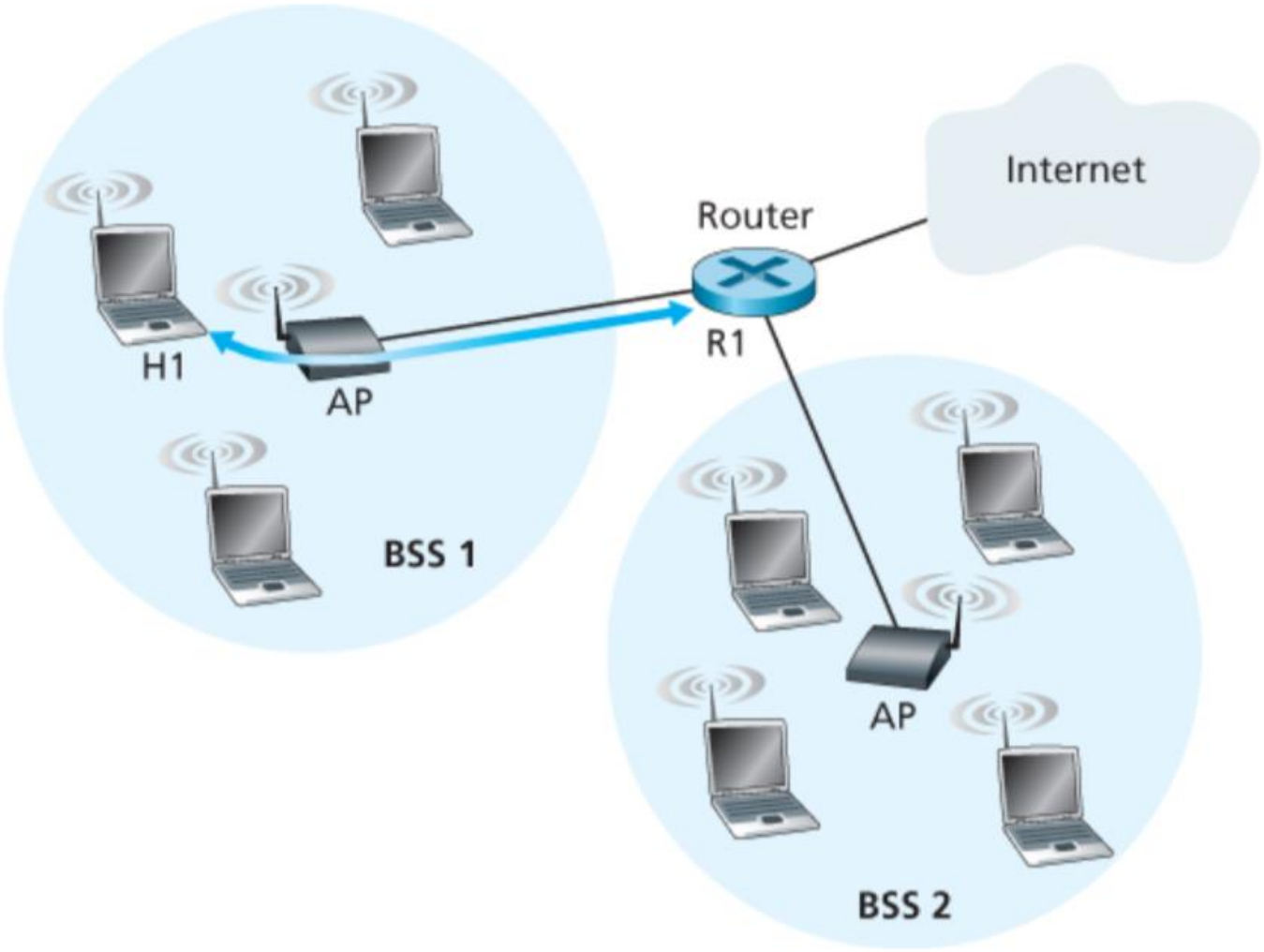
WiFi: IEEE 802.11 Wireless LANs

1. LAN Architecture
2. MAC protocol
3. Frame structure
4. Advanced features

WiFi: IEEE 802.11 Frame

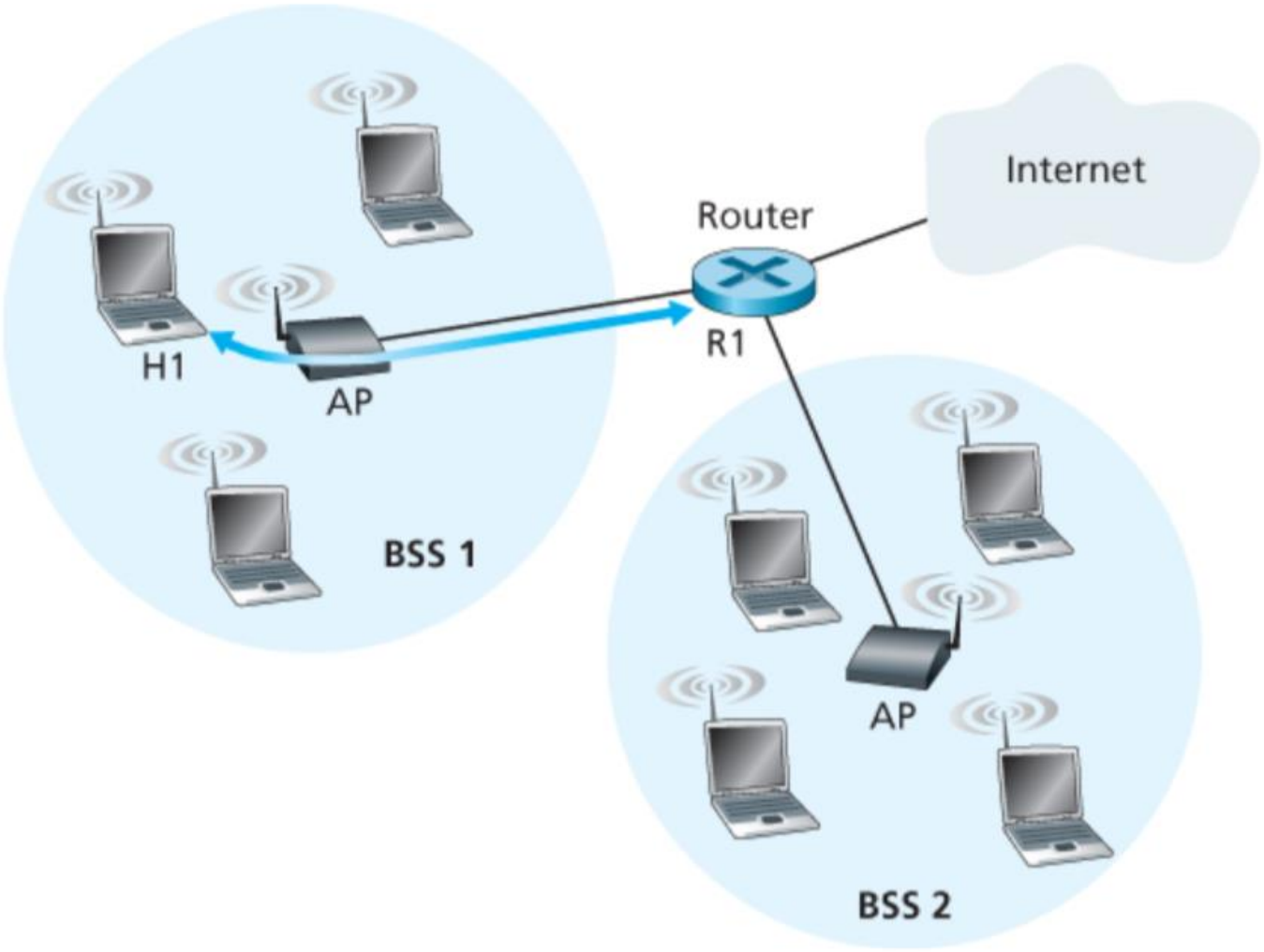


802.11 Frame: The secret of Address-3



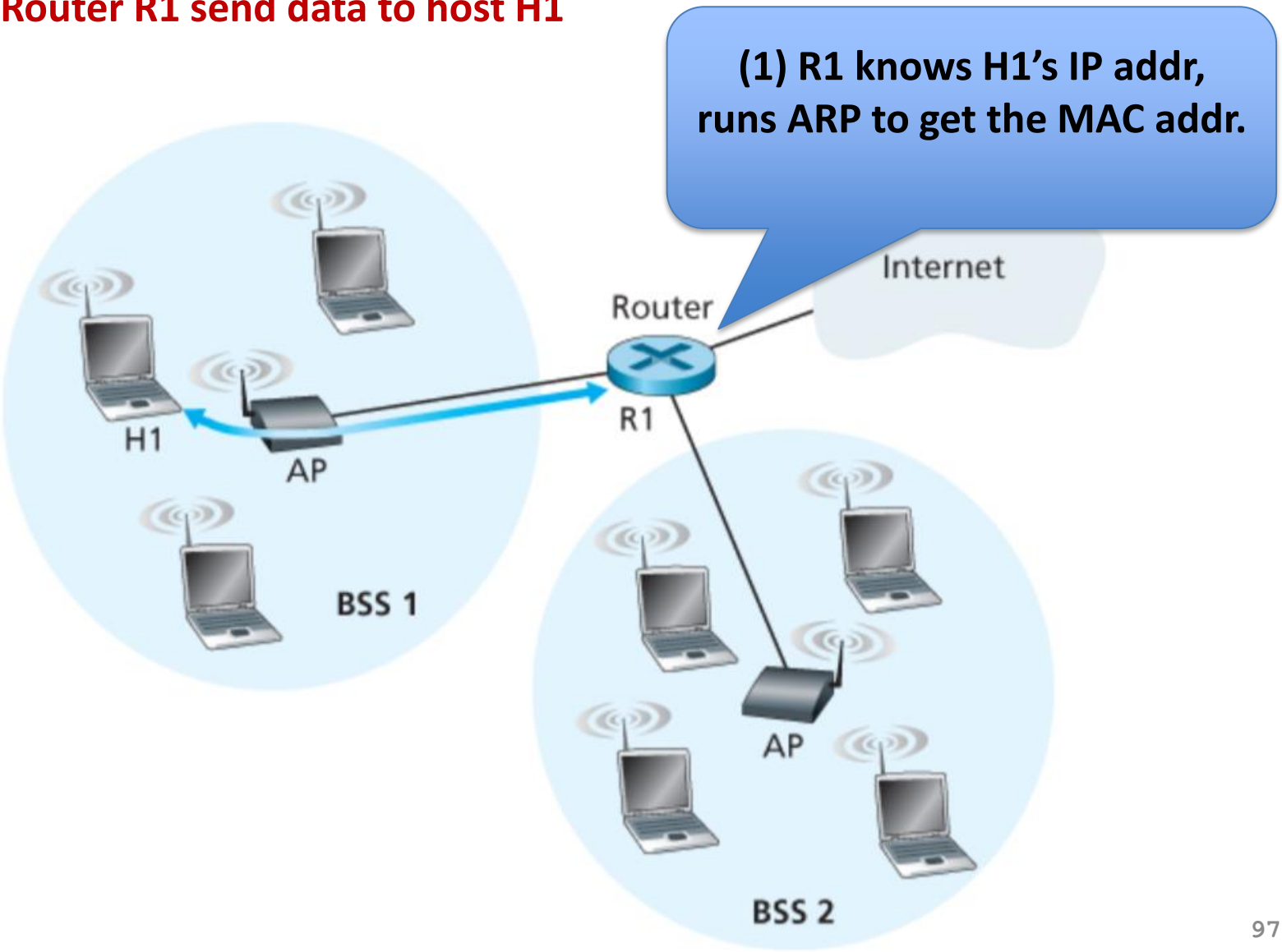
802.11 Frame: The secret of Address-3

Case 1: Router R1 send data to host H1



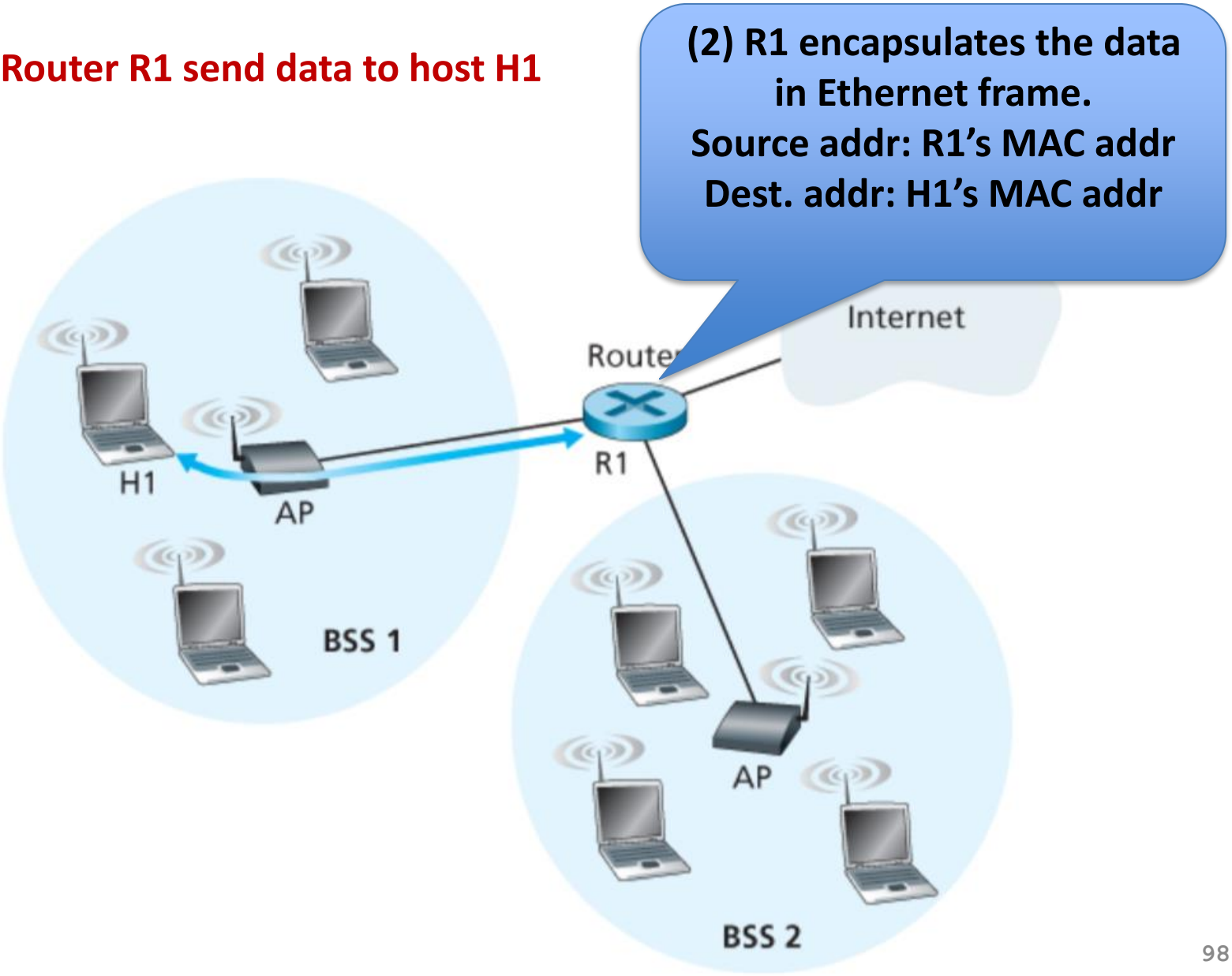
802.11 Frame: The secret of Address-3

Case 1: Router R1 send data to host H1



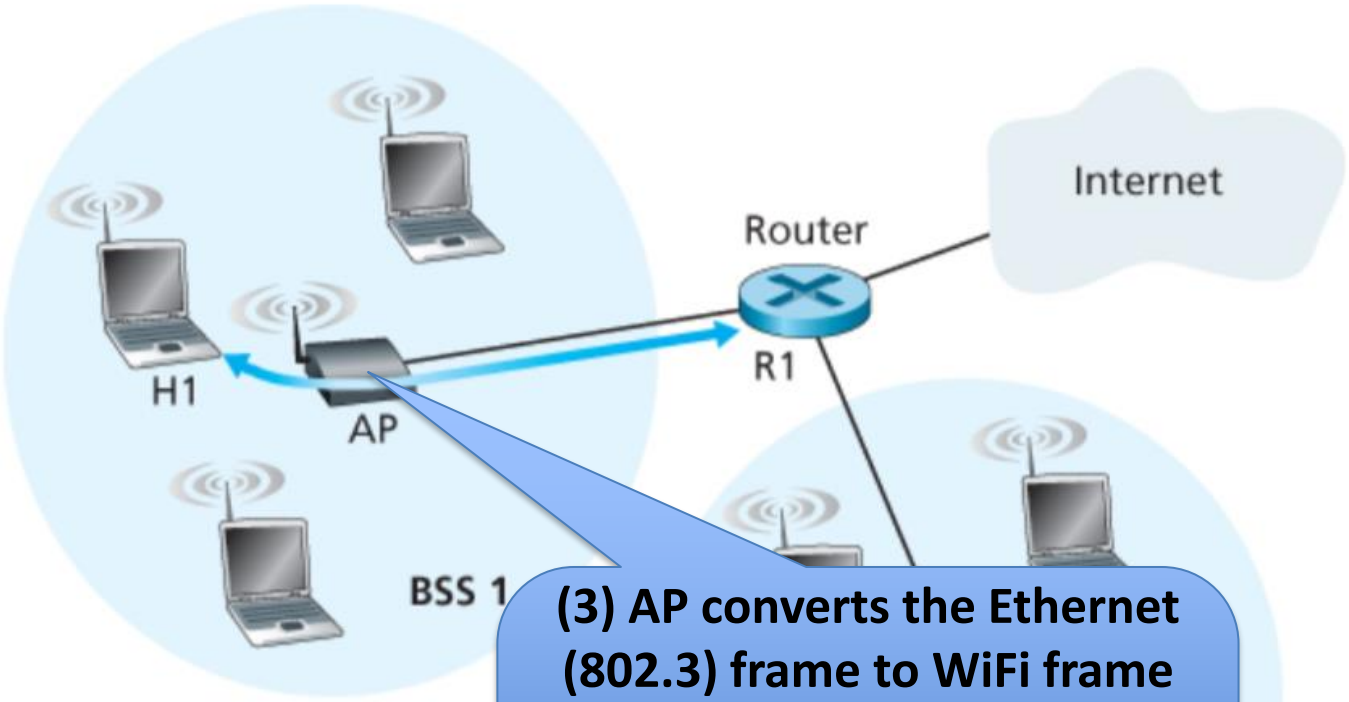
802.11 Frame: The secret of Address-3

Case 1: Router R1 send data to host H1



802.11 Frame: The secret of Address-3

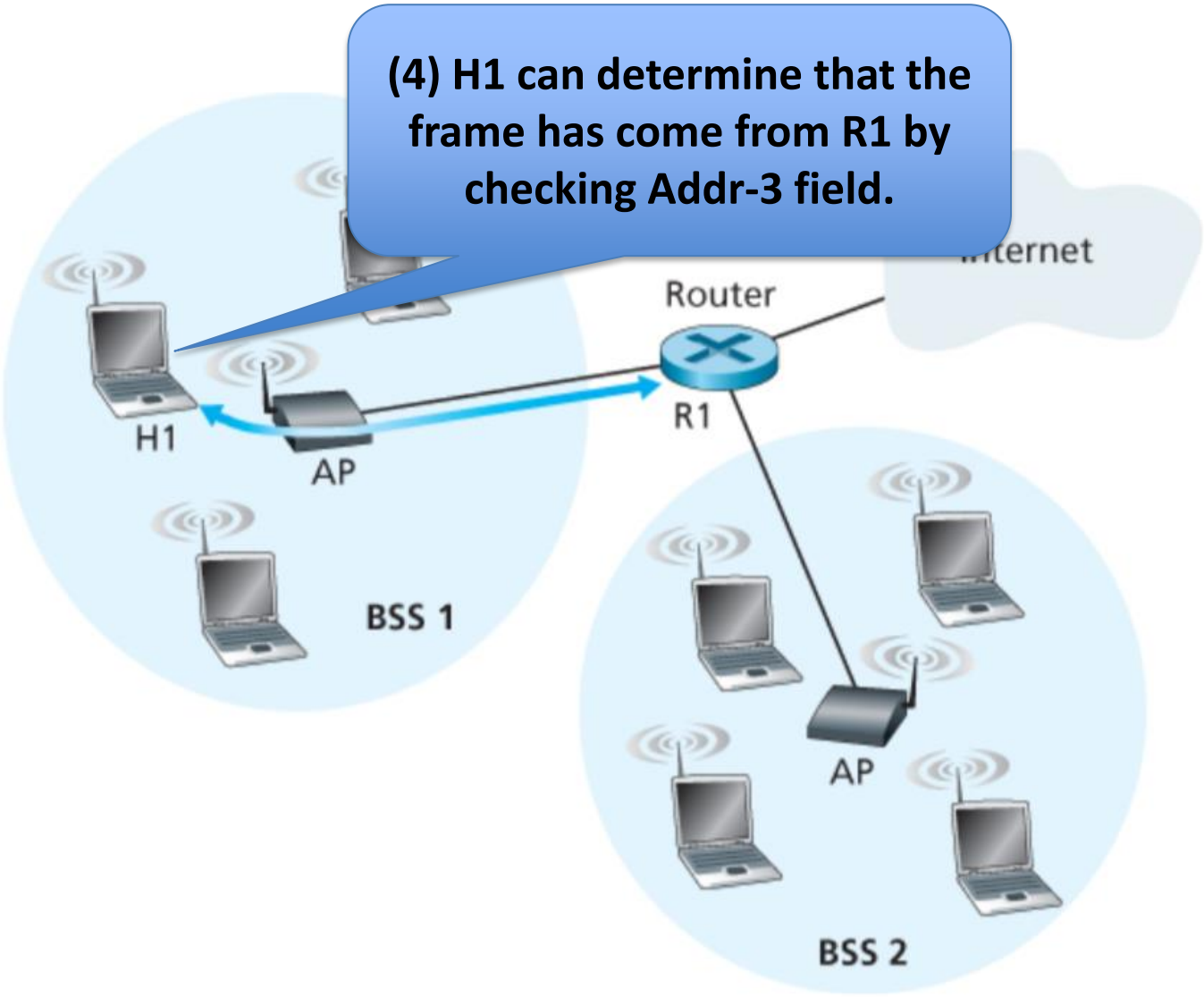
Case 1: Router R1 send data to host H1



(3) AP converts the Ethernet (802.3) frame to WiFi frame (802.11).
Addr 1: H1's MAC addr
Addr 2: AP's MAC addr
Addr 3: R1's MAC addr

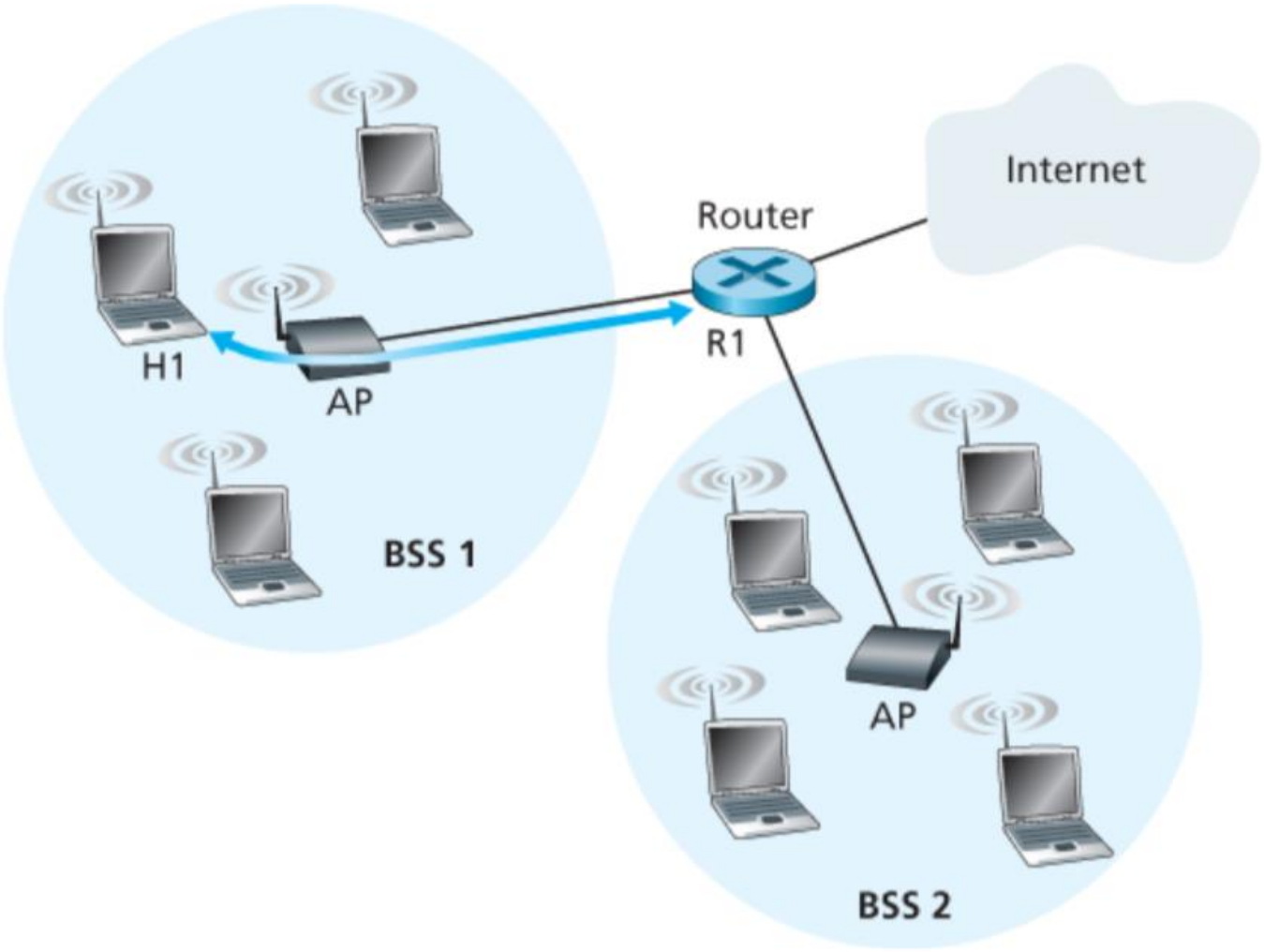
802.11 Frame: The secret of Address-3

Case 1: Router R1 send data to host H1



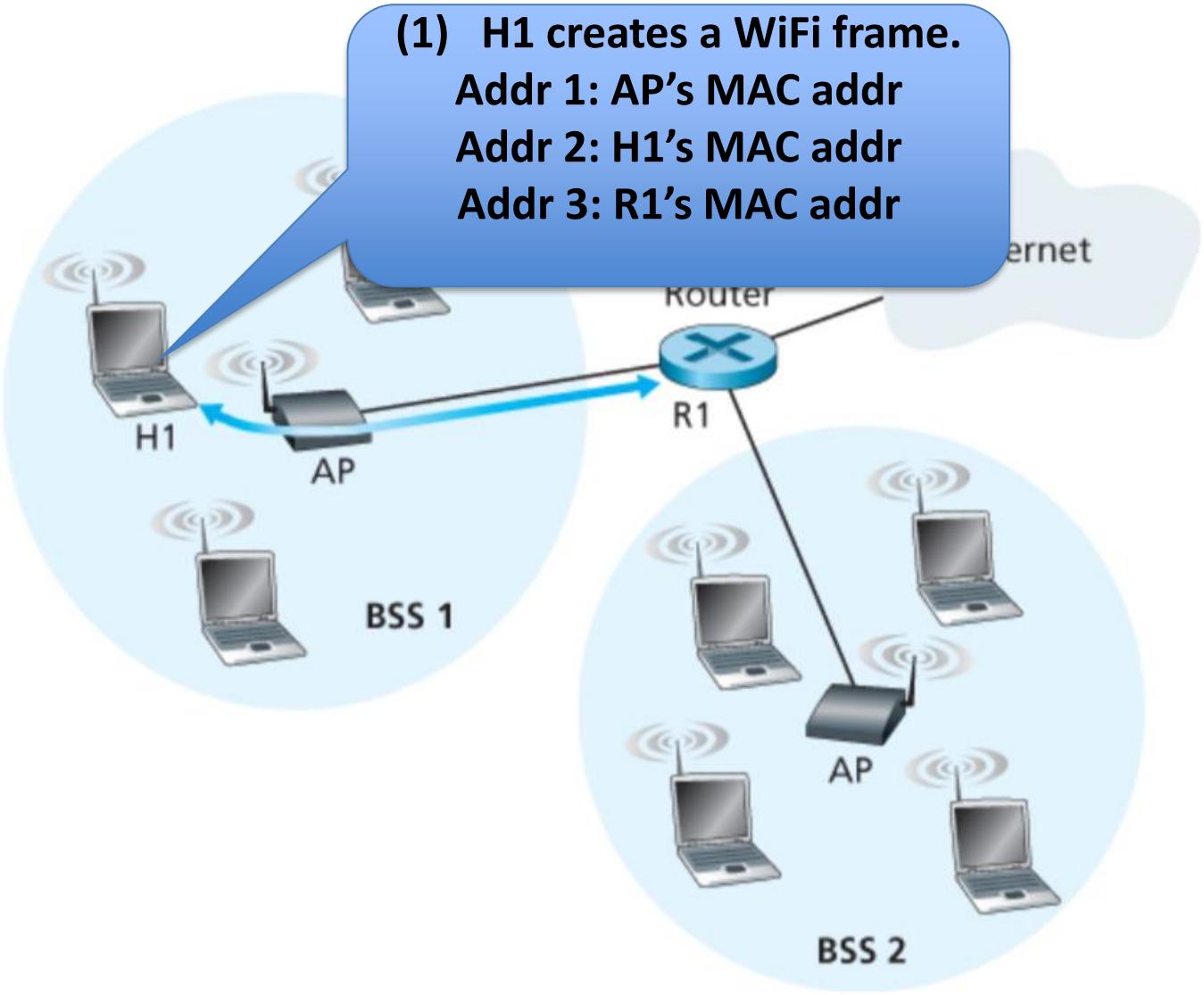
802.11 Frame: The secret of Address-3

Case 2: Host H1 responds by sending packet to Router R1



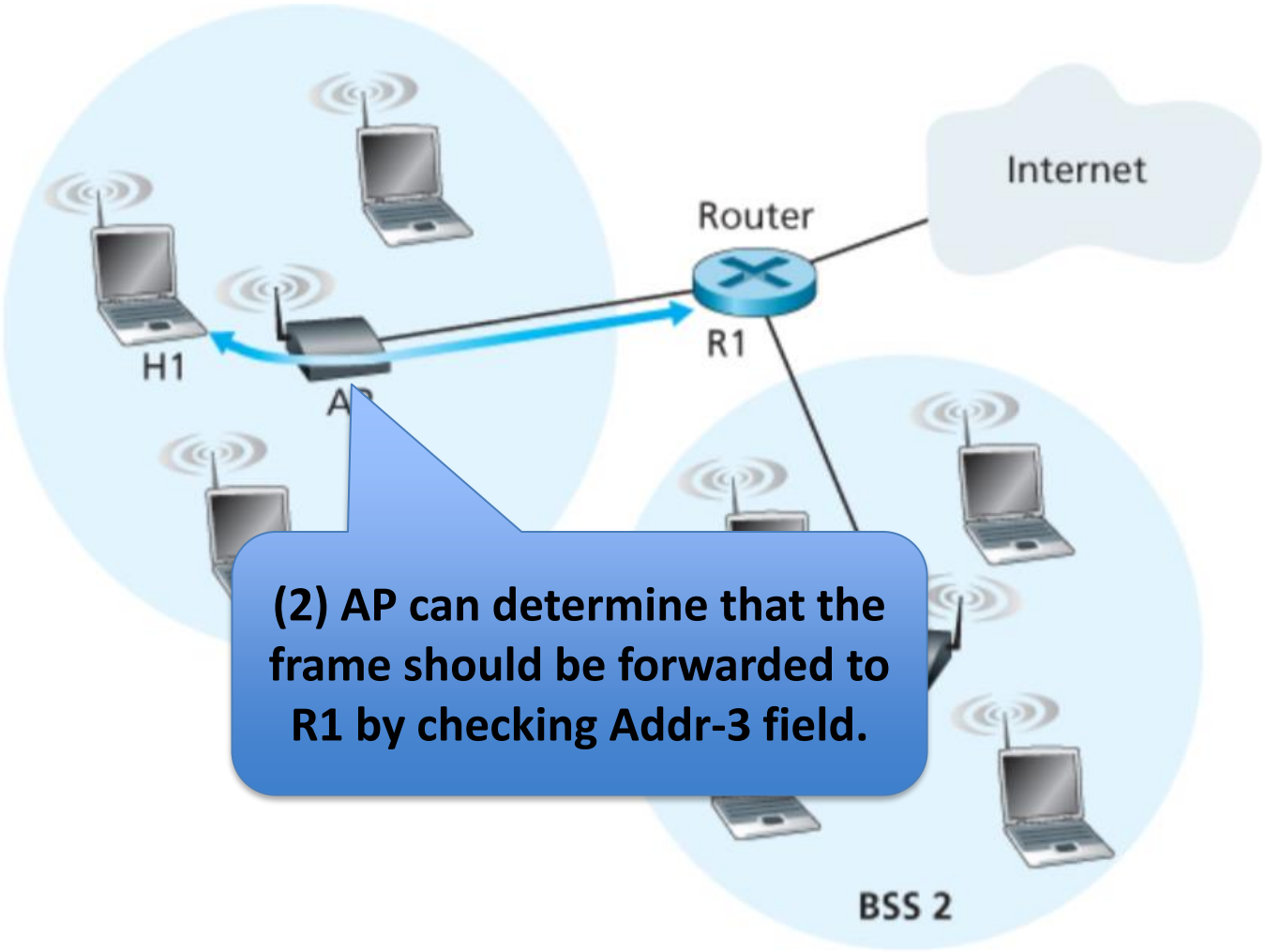
802.11 Frame: The secret of Address-3

Case 2: Host H1 responds by sending packet to Router R1



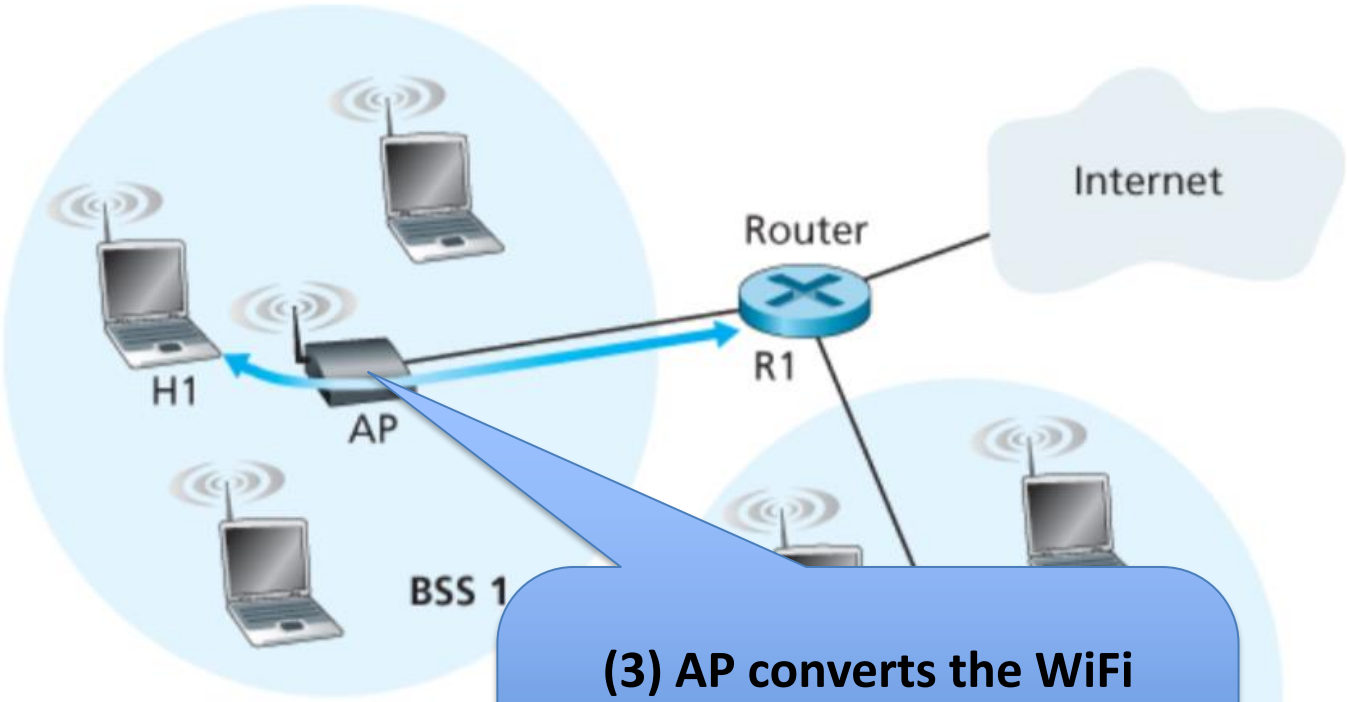
802.11 Frame: The secret of Address-3

Case 2: Host H1 responds by sending packet to Router R1



802.11 Frame: The secret of Address-3

Case 2: Host H1 responds by sending packet to Router R1



(3) AP converts the WiFi (802.11) frame to Ethernet frame (802.3).
Source addr : H1's MAC addr
Dest. addr : R1's MAC addr

WiFi: IEEE 802.11 Wireless LANs

1. LAN Architecture
2. MAC protocol
3. Frame structure
4. Advanced features

WiFi: Advanced features

1) Rate adaptation

2) Power management

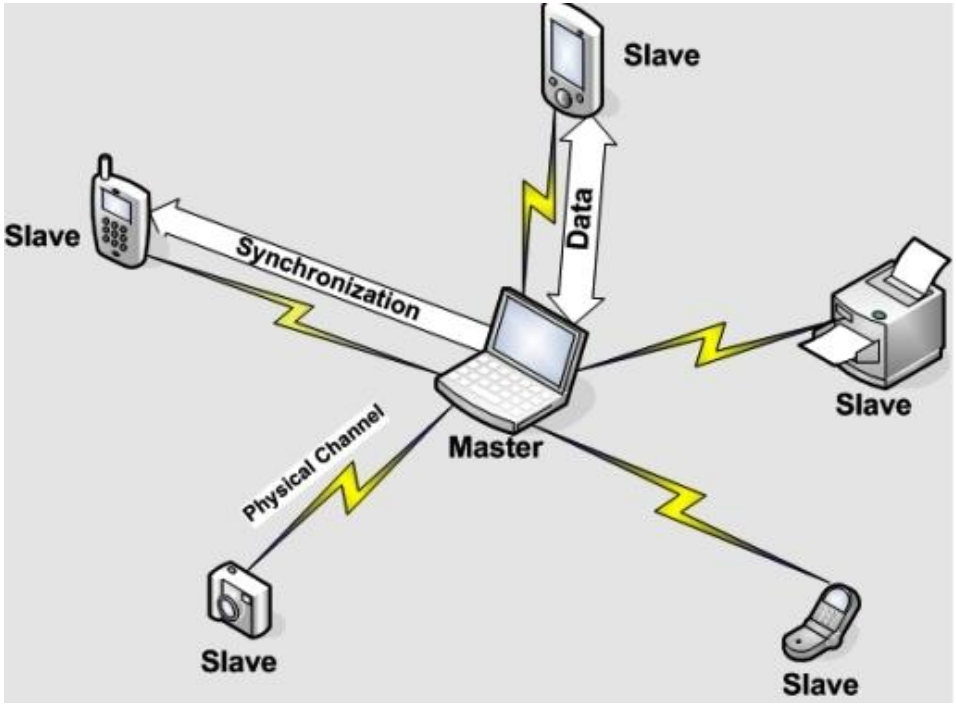
Bluetooth: 802.15.1 “personal-area-networks”

Wireless Personal Area Networks "WPANs"

WPANs address communication needs within personal operating space < 10m

IEEE 802.15.3 is chartered with creating a high rate WPAN standard that provides for low power, low cost, short range solutions targeted to consumer digital imaging and multimedia applications

Bluetooth piconets



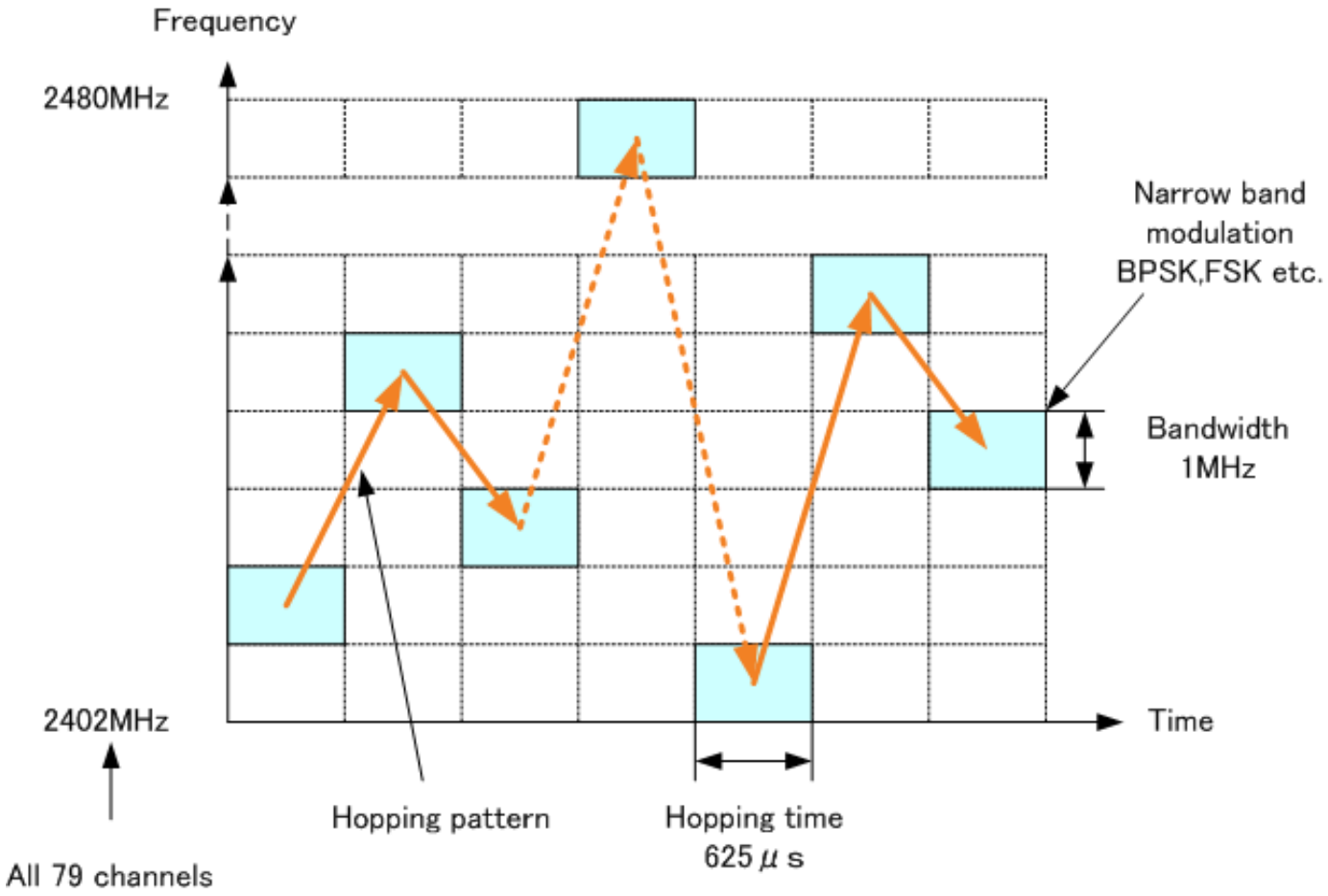
- 1 master, up to 7 “slave” devices; 225 “parked” devices
- Operates on unlicensed wireless spectrum
  - How to prevent interference?

PHY: Spread Spectrum – Frequency Hopping

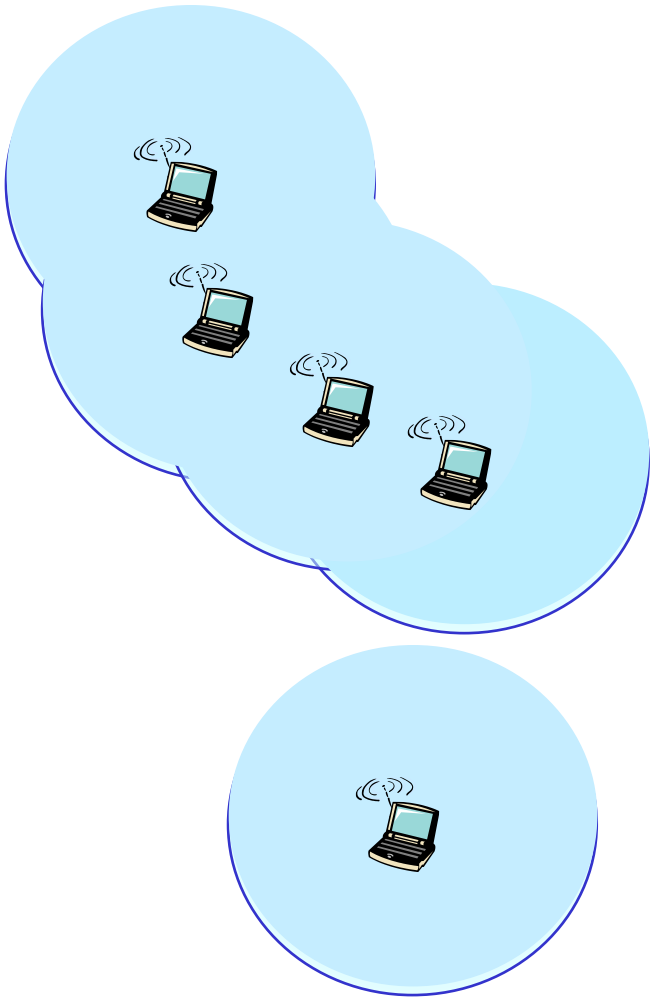
- Nodes rapidly jump between frequencies
- Sender and receiver coordinated in jumps
  - How coordinate? Pseudorandom number generator, with shared input known to sender/receiver
- If randomly collide with other transmitted, only for short period before jump again

- Bluetooth
  - 79 frequencies, on each frequency for 625 microseconds
  - Each channel also uses TDMA, with each frame taking 1/3/5 consecutive slots.
  - Only master can start in odd slot, slave only in response

PHY: Spread Spectrum – Frequency Hopping



Ad-Hoc Networks



Ad hoc mode

- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes self-organize and route among themselves
- Can create multi-hop wireless networks, instead of a wired backend

Infrastructure vs. Ad Hoc

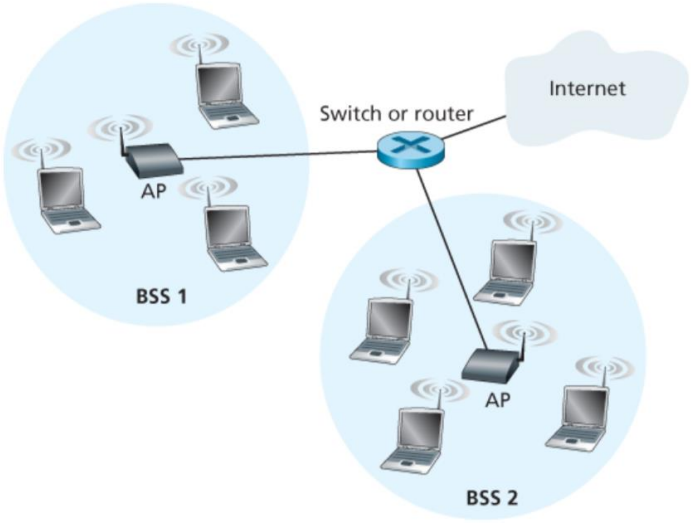
- Infrastructure mode
  - Wireless hosts are associated with a base station
  - Traditional services provided by the connected network
  - E.g., address assignment, routing, and DNS resolution
- Ad hoc networks
  - Wireless hosts have no infrastructure to connect to
  - Hosts themselves must provide network services
- Similar in spirit to the difference between
  - Client-server communication
  - Peer-to-peer communication

Delay Tolerant Networking

- Nodes can both route and store
  - Next hop is available, forward
  - Otherwise, store packets
- Useful for data collection with no time limit
  - e.g., sensors in the field
- Analogous to email
  - Hold onto packets until another hop can take it from you
  - Eventually reach its destination

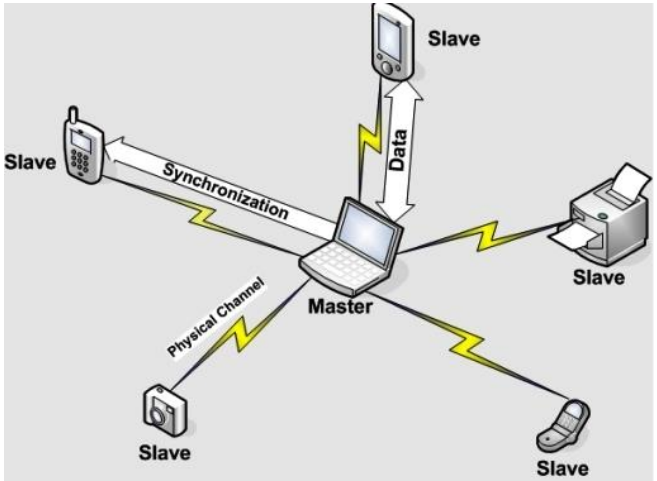
Conclusions

- Wireless
  - Already a major way people connect to the Internet
  - Gradually becoming more than just an access network
- Mobility
  - Today's users tolerate disruptions as they move
  - … and applications try to hide the effects
  - Tomorrow's users expect seamless mobility
- Challenges the design of network protocols
  - Wireless breaks the abstraction of a link, and the assumption that packet loss implies congestion
  - Mobility breaks association of address and location
  - Higher-layer protocols don't perform as well



802.11 LAN

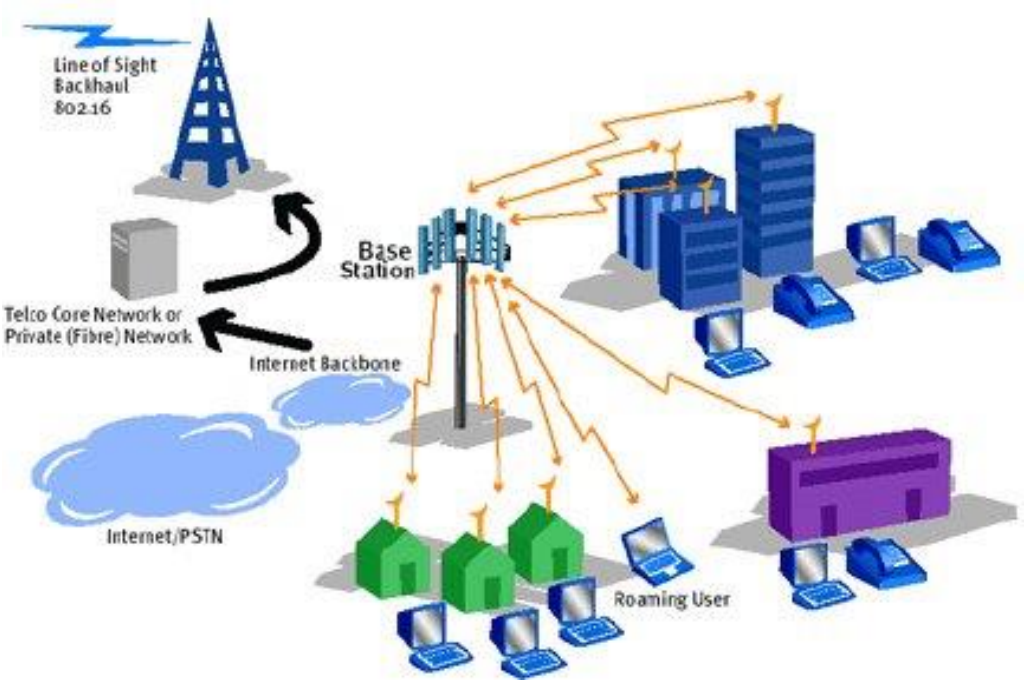
802.15 PAN



Wide-Area Wireless Network: WiMAX

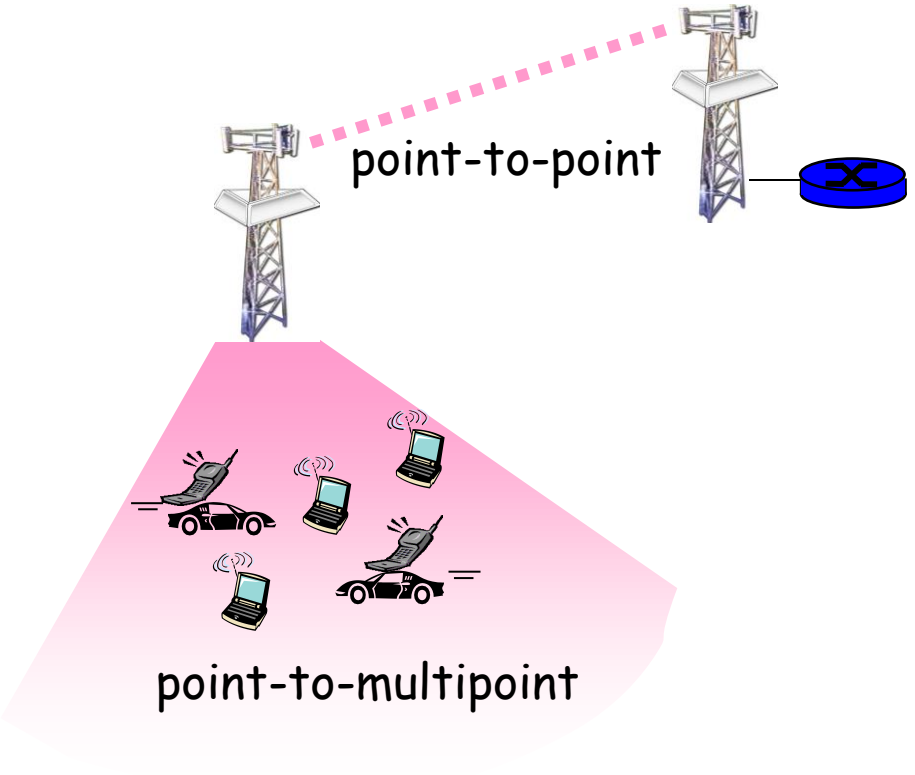
(Worldwide Interoperability for Microwave Access)

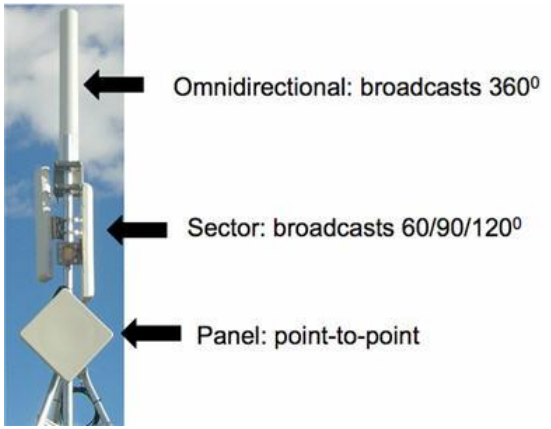
802.16 Metropolitan Area Network (MAN)



802.16: WiMAX

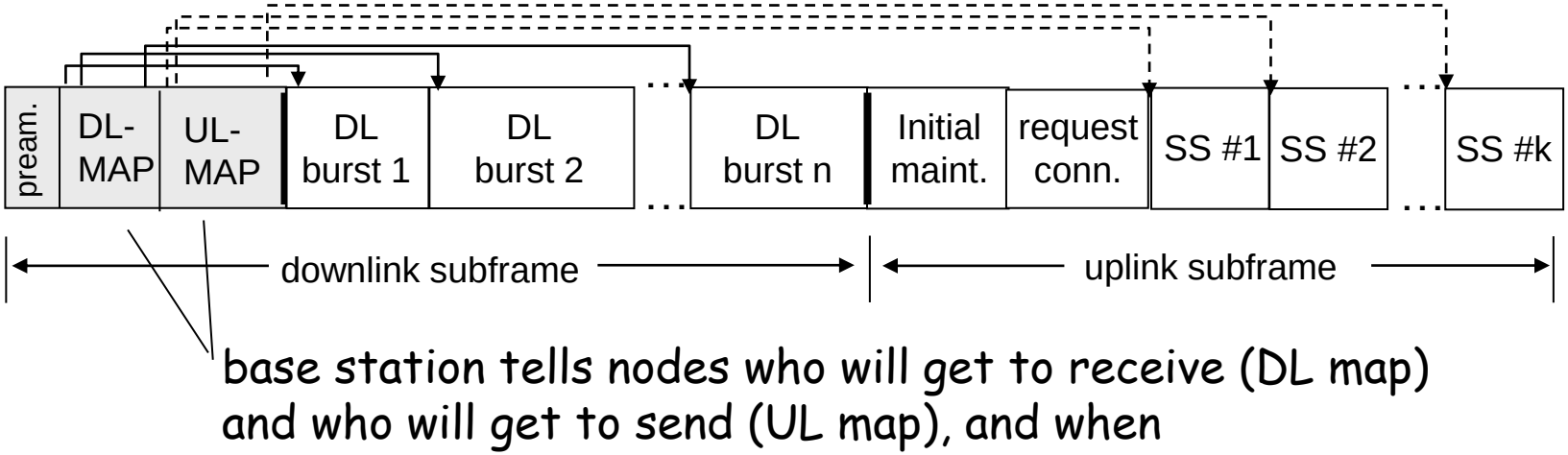
- like 802.11: base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11:
  - range ~ 6 miles (“city rather than coffee shop”)





802.16: WiMAX: downlink, uplink scheduling

- transmission frame
  - down-link subframe: base station to node
  - uplink subframe: node to base station



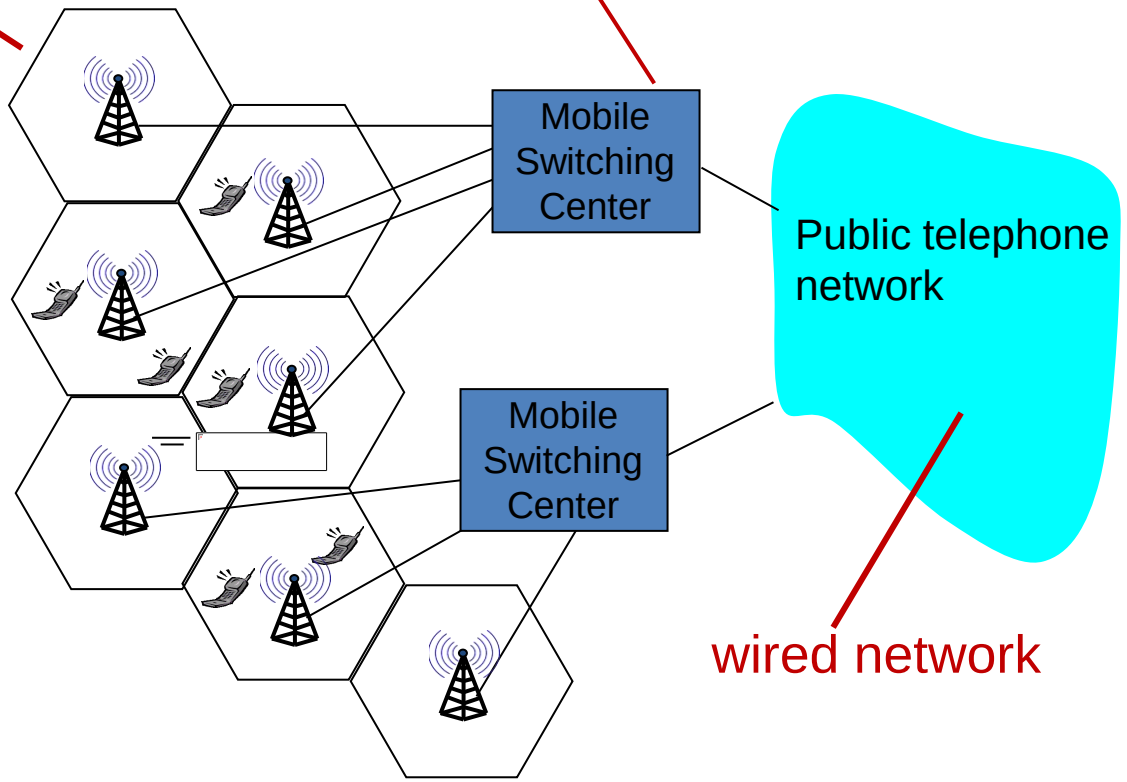
- WiMAX standard provide mechanism for scheduling, but not scheduling algorithm

Cellular Networks

Components of cellular network architecture

MSC
- connects cells to wired tel. net.
- manages call setup
- handles mobility

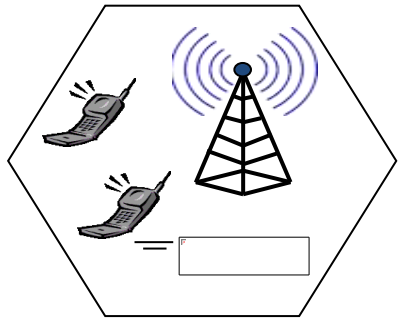
cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS

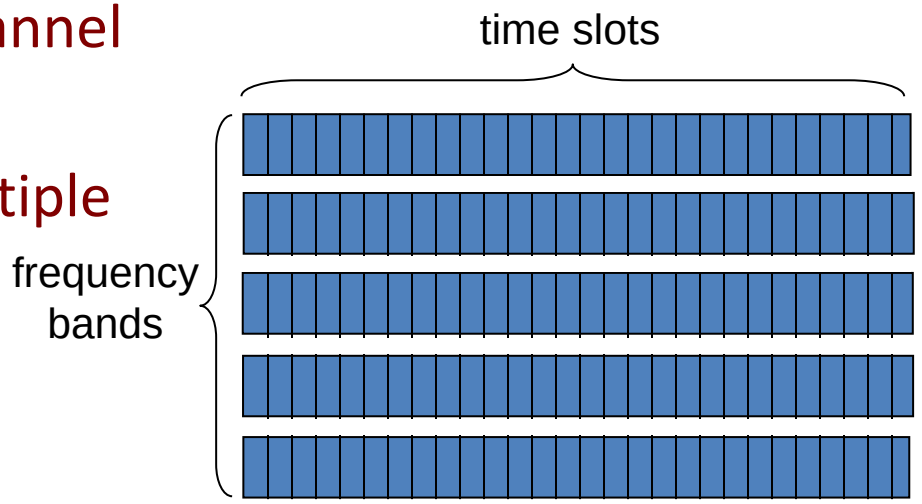


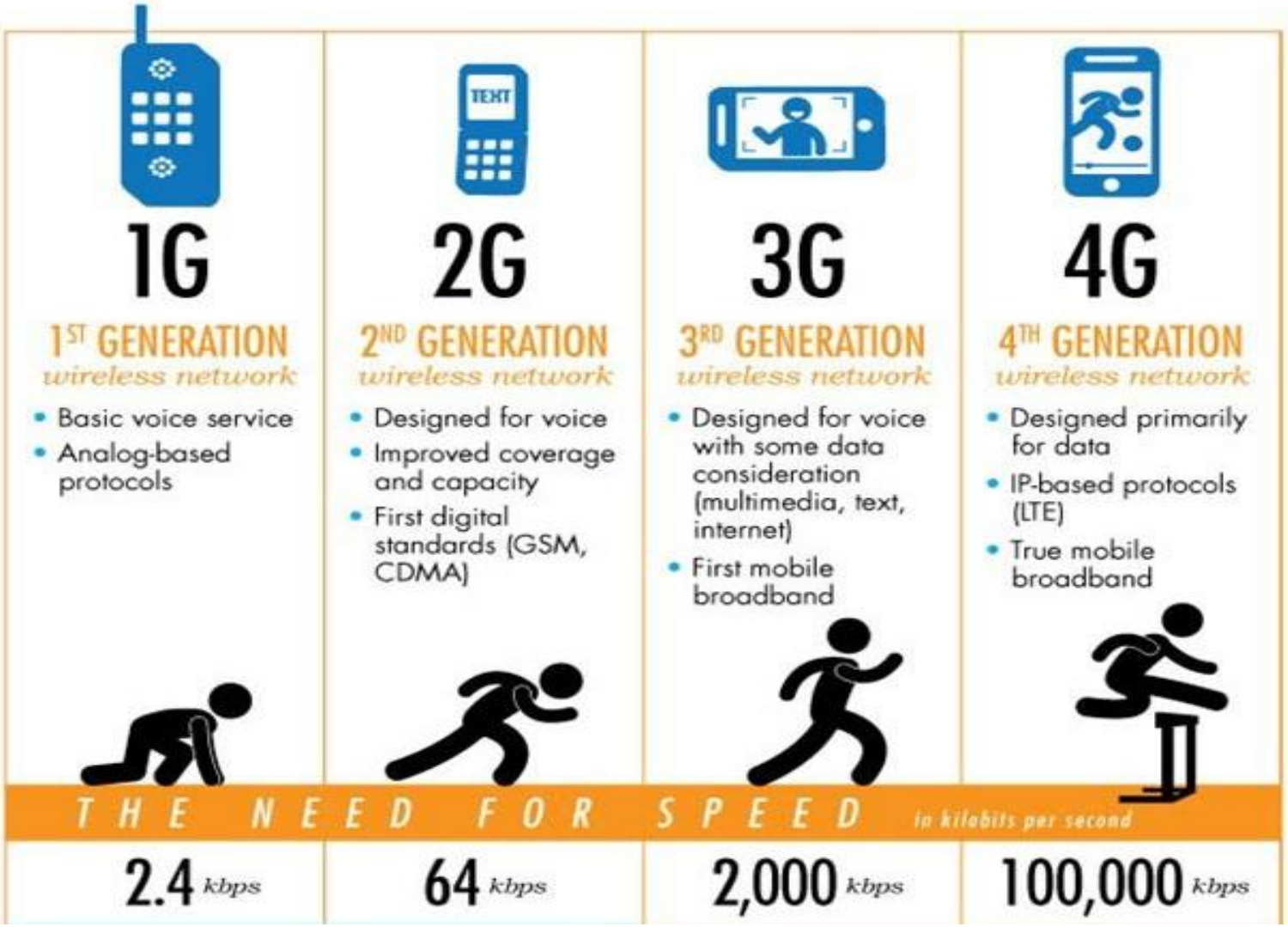
Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

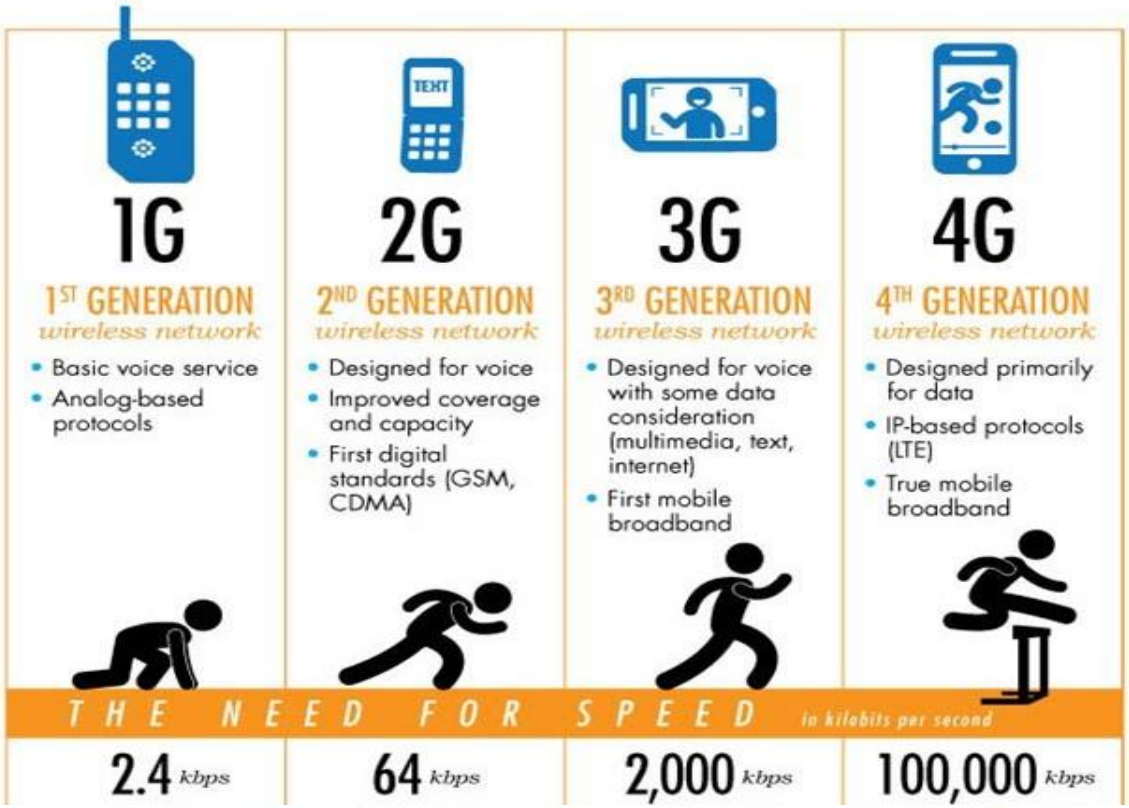
- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access







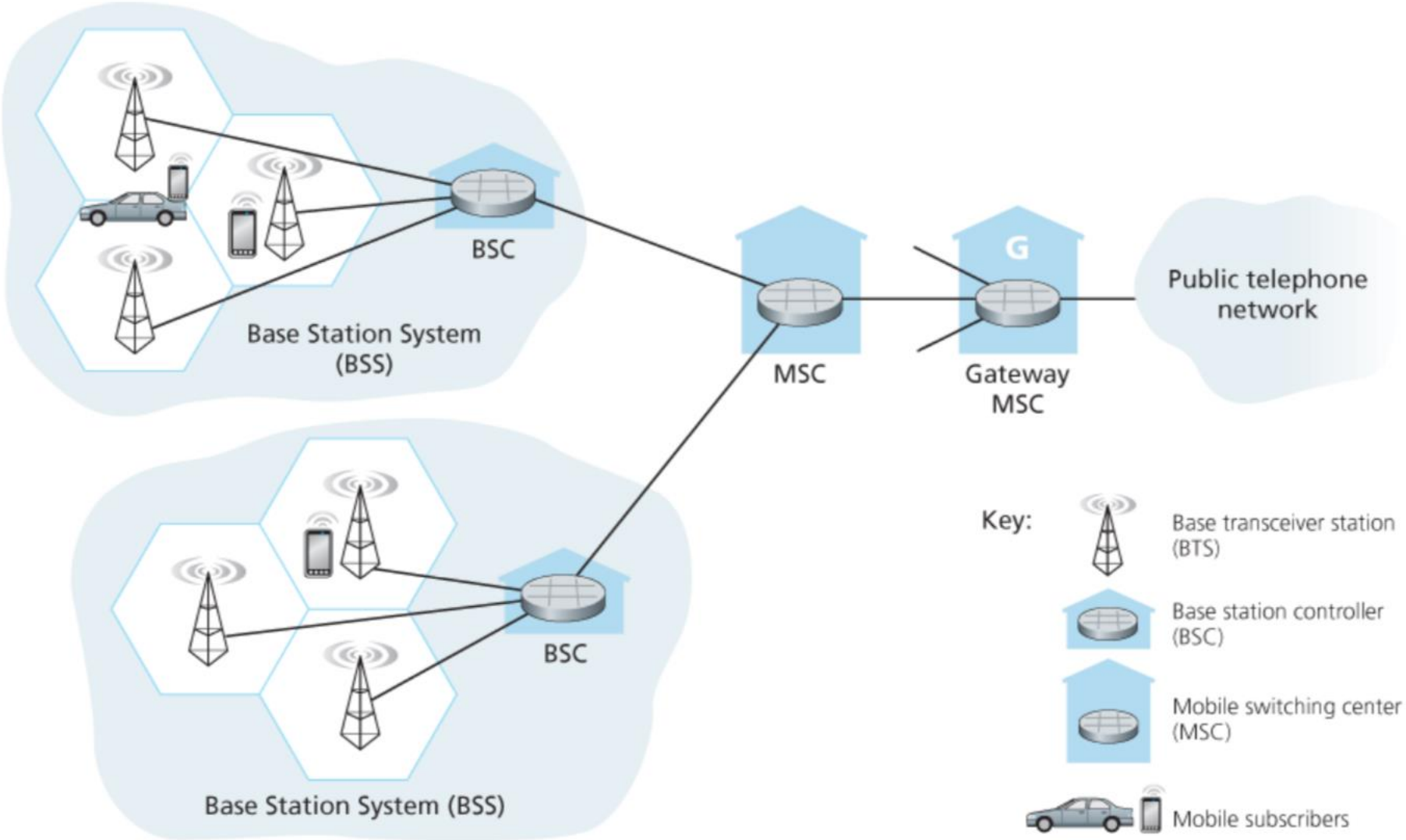
Picture1: https://www.brandsynario.com/the-evolution-of-gs-generation-networks/



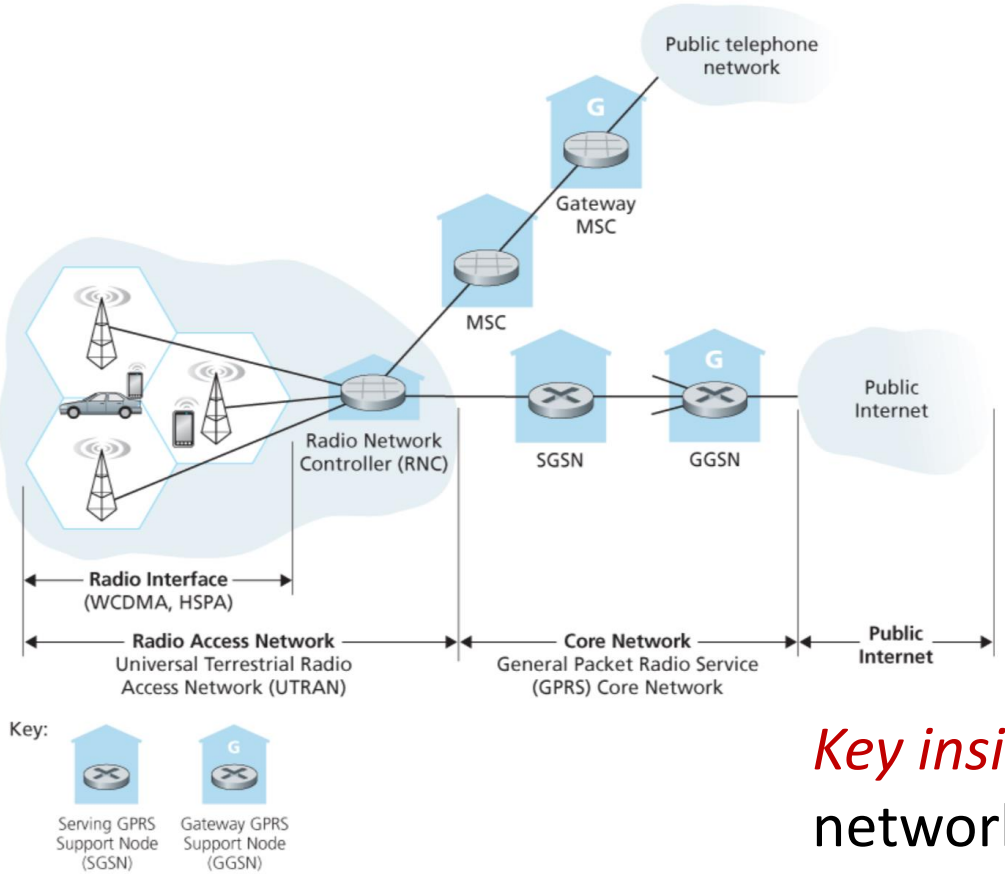
Tech. Generation	Year	Standard	Speed	Supports
1G (analog)	1980	AMPS, TACS, C-450	2 kbps	Voice only
2G	1990	GSM, CDMA	64 kbps	SMS
2.5G	2000	GPRS	110 kbps	MMS
2.75G	2003	EDGE	135 kbps	WAP
3G	2002	UMTS, WCDMA	144 kbps - 2 Mbps	Video call
3.5G	2010	HSPA	5.76 Mbps - 56 Mbps	Multimedia
3.75G	2010	HSPA+, HSPAP	28 Mbps - 168 Mbps	Multimedia
4G	2010	LTE	100 Mbps - 300 Mbps	Streaming video
4.5G	2015	LTE+	100 Mbps - 1 Gbps	VoIP
5G	2020	???	1 Gbps - 20 Gbps	WWWW, IoT

Picture1: https://www.brandsynario.com/the-evolution-of-gs-generation-networks/
Picture2: http://kaaale.blogspot.com/2019/02/the-evolution-of-cellular-mobile.html

2G (voice) network architecture



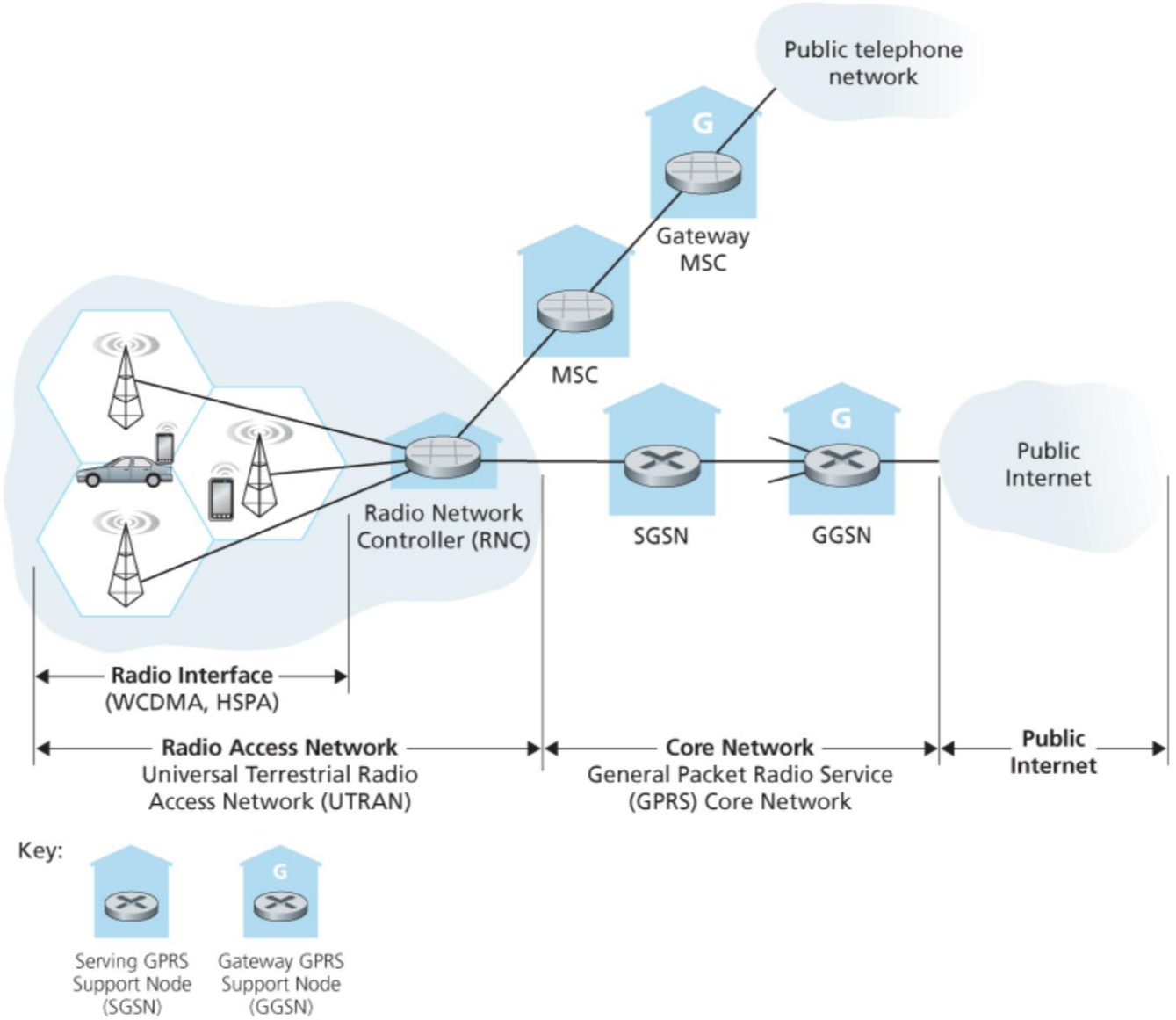
3G (voice+data) network architecture



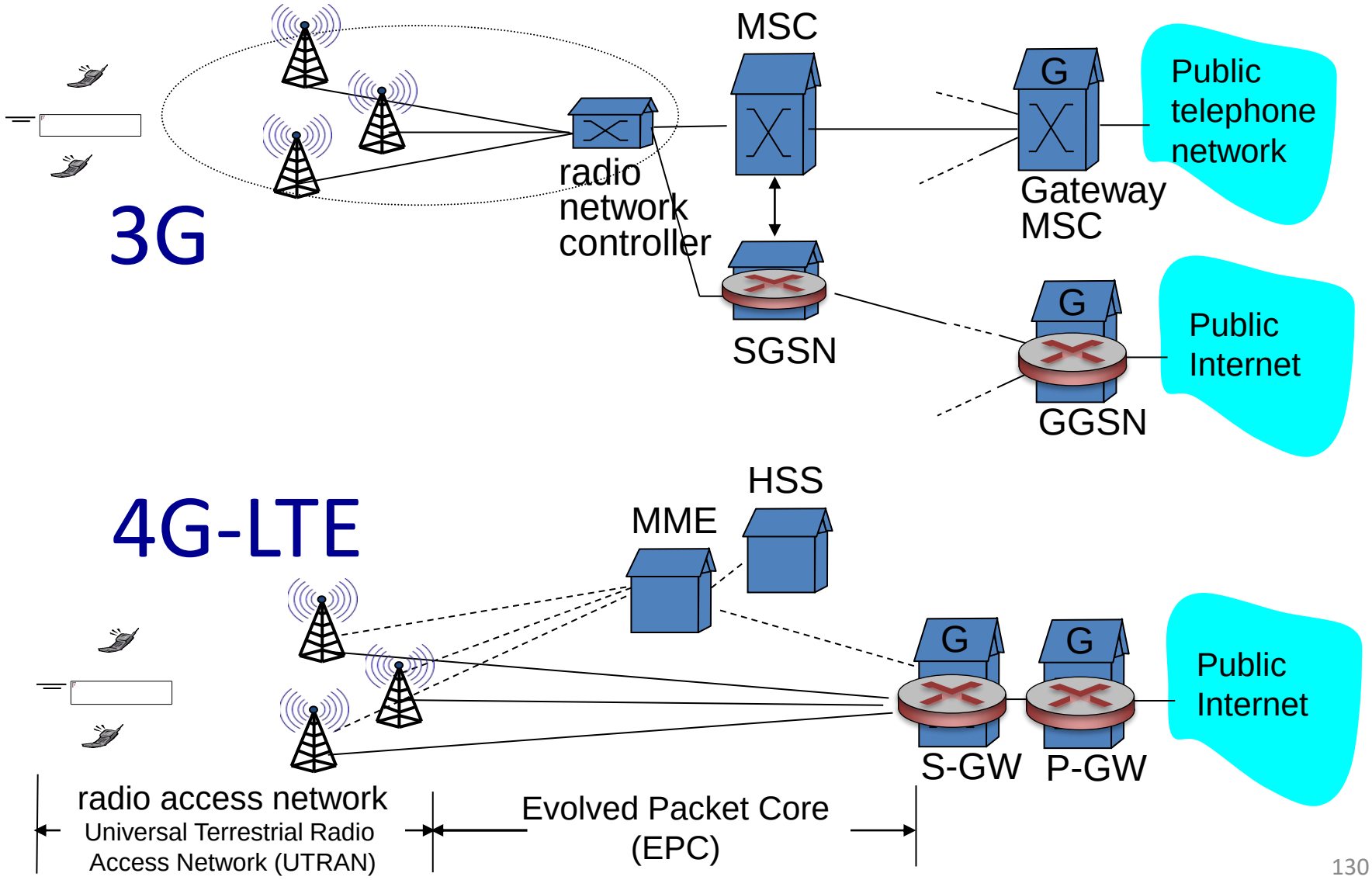
Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

- voice network *unchanged* in core
- data network operates in parallel

3G (voice+data) network architecture

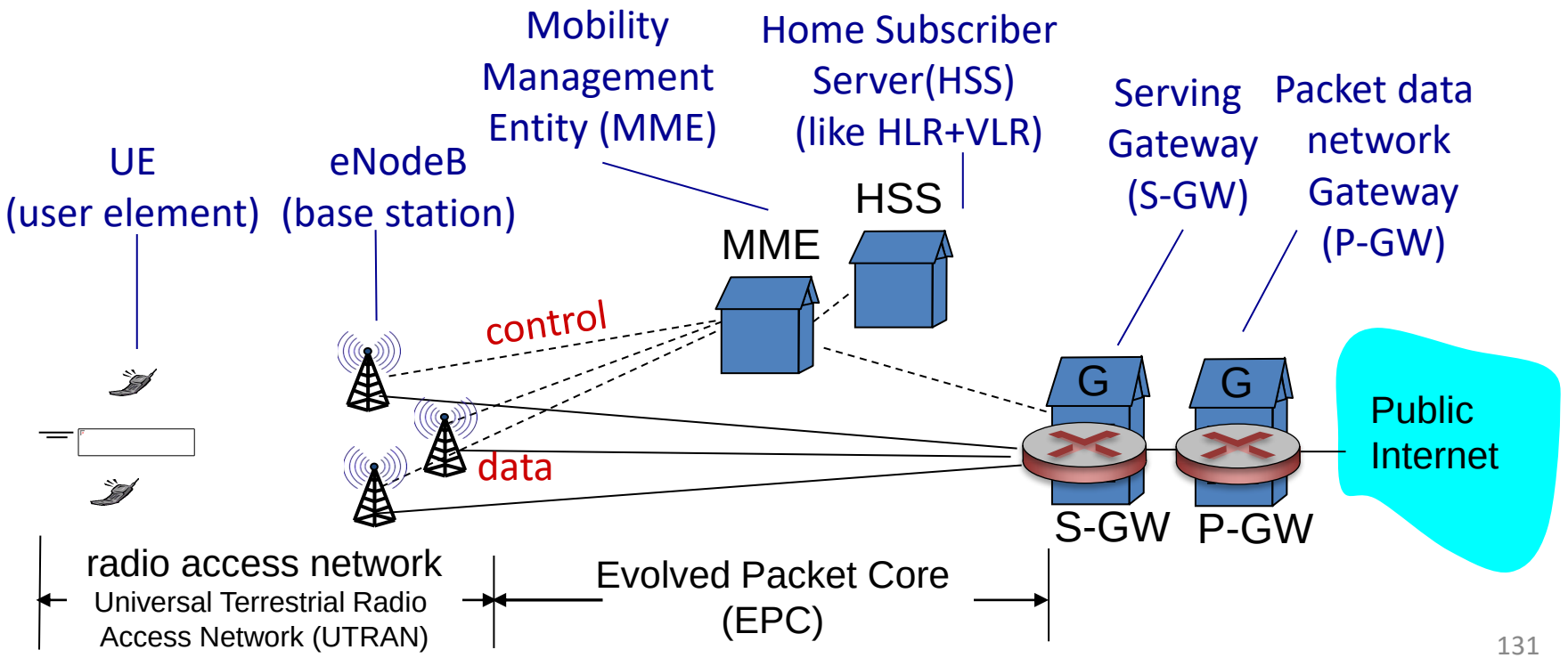


3G versus 4G LTE network architecture

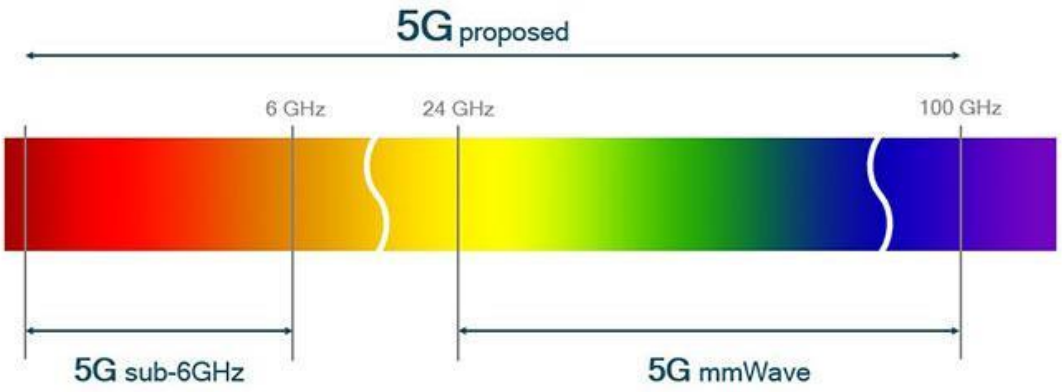


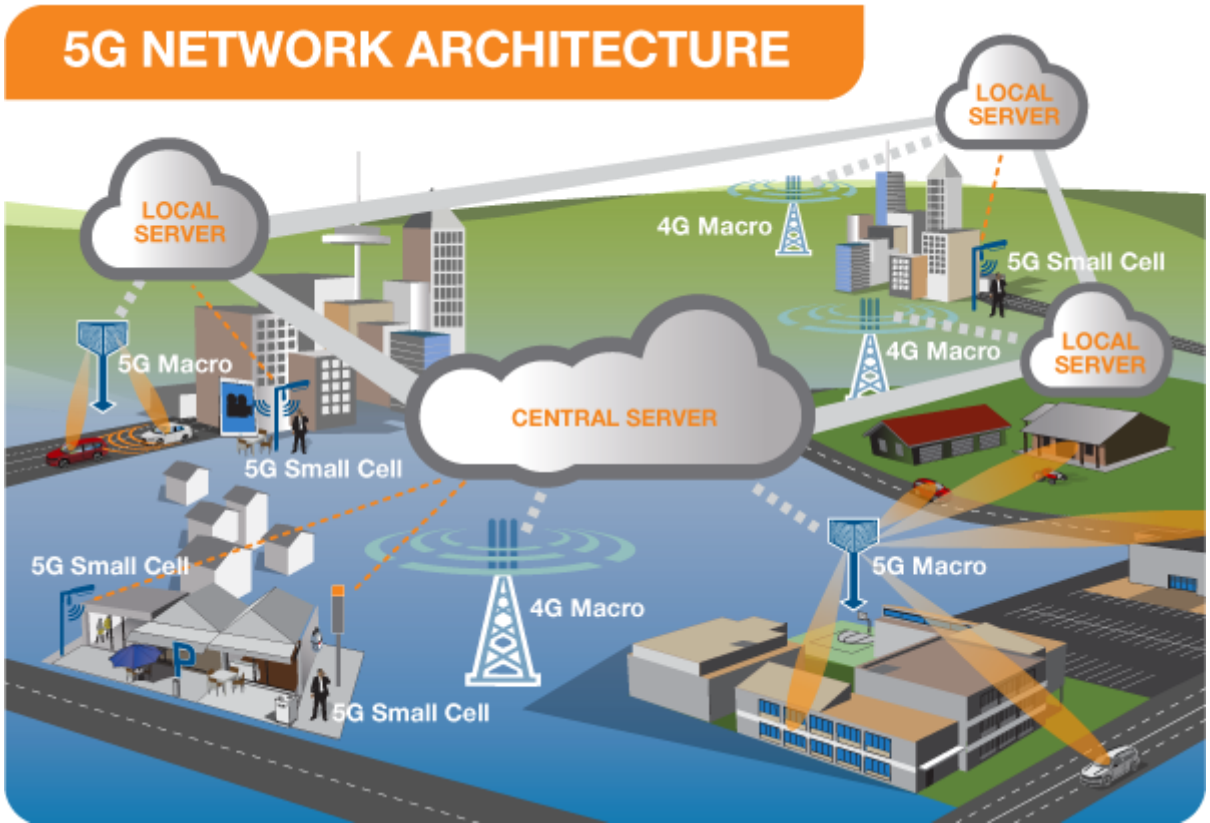
4G: differences from 3G

- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- no separation between voice and data – all traffic carried over IP core to gateway



5G cellular networks

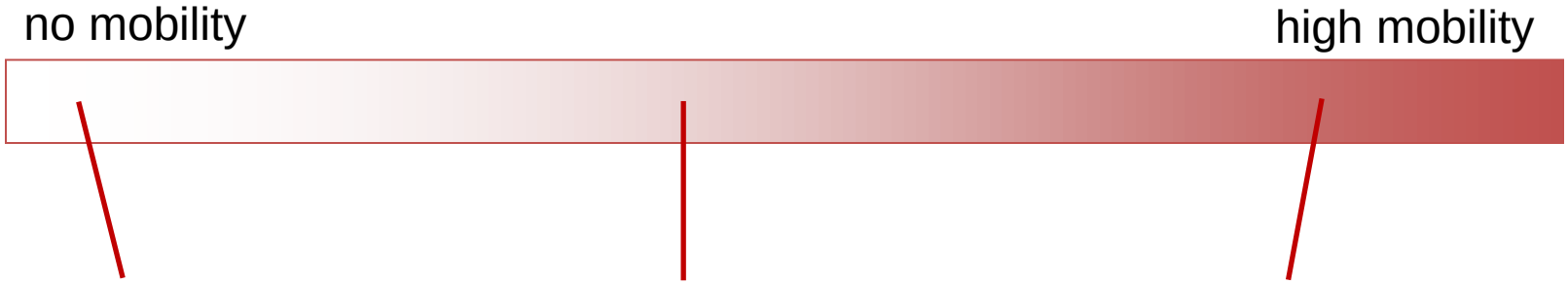




Mobility in Wireless Networks

What is mobility?

- spectrum of mobility, from the *network* perspective:



mobile wireless user, using same access point

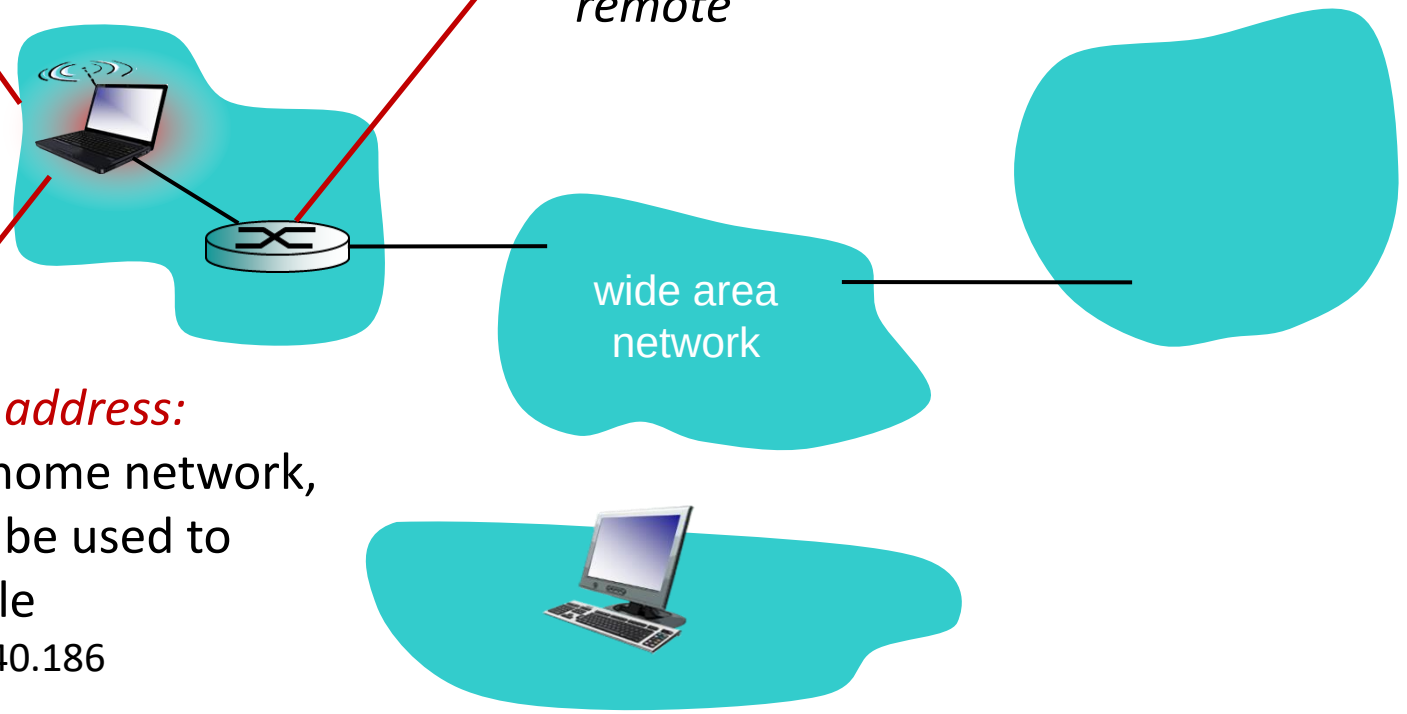
mobile user, connecting/ disconnecting from network using DHCP.

mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)

Mobility: vocabulary

home network: permanent "home" of mobile
(e.g., 128.119.40/24)

home agent: *entity that will perform mobility functions on behalf of mobile, when mobile is remote*



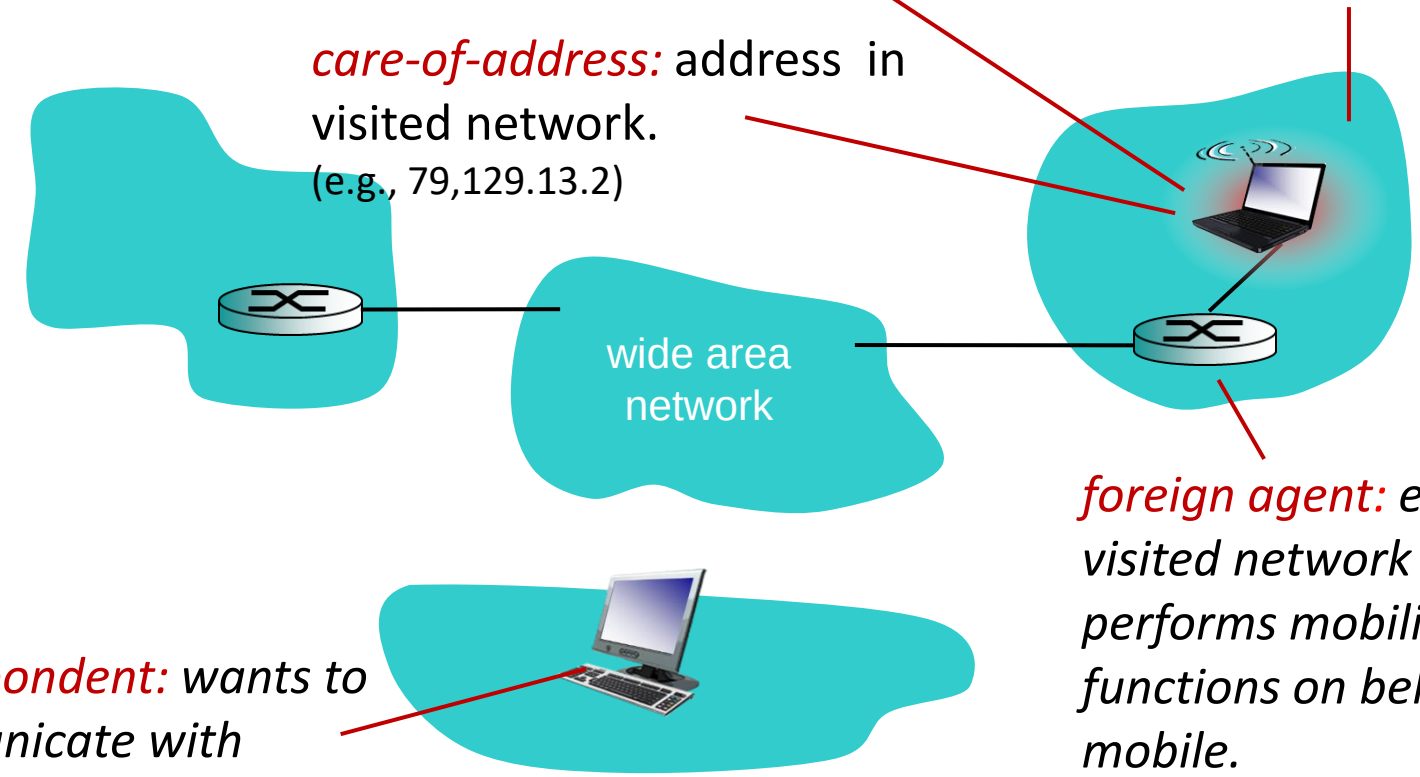
permanent address:
address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

Mobility: more vocabulary

permanent address: remains constant (e.g., 128.119.40.186)

visited network: network in which mobile currently resides (e.g., 79.129.13/24)

care-of-address: address in visited network. (e.g., 79,129.13.2)



foreign agent: *entity in visited network that performs mobility functions on behalf of mobile.*

correspondent: *wants to communicate with mobile*

Mobility: approaches

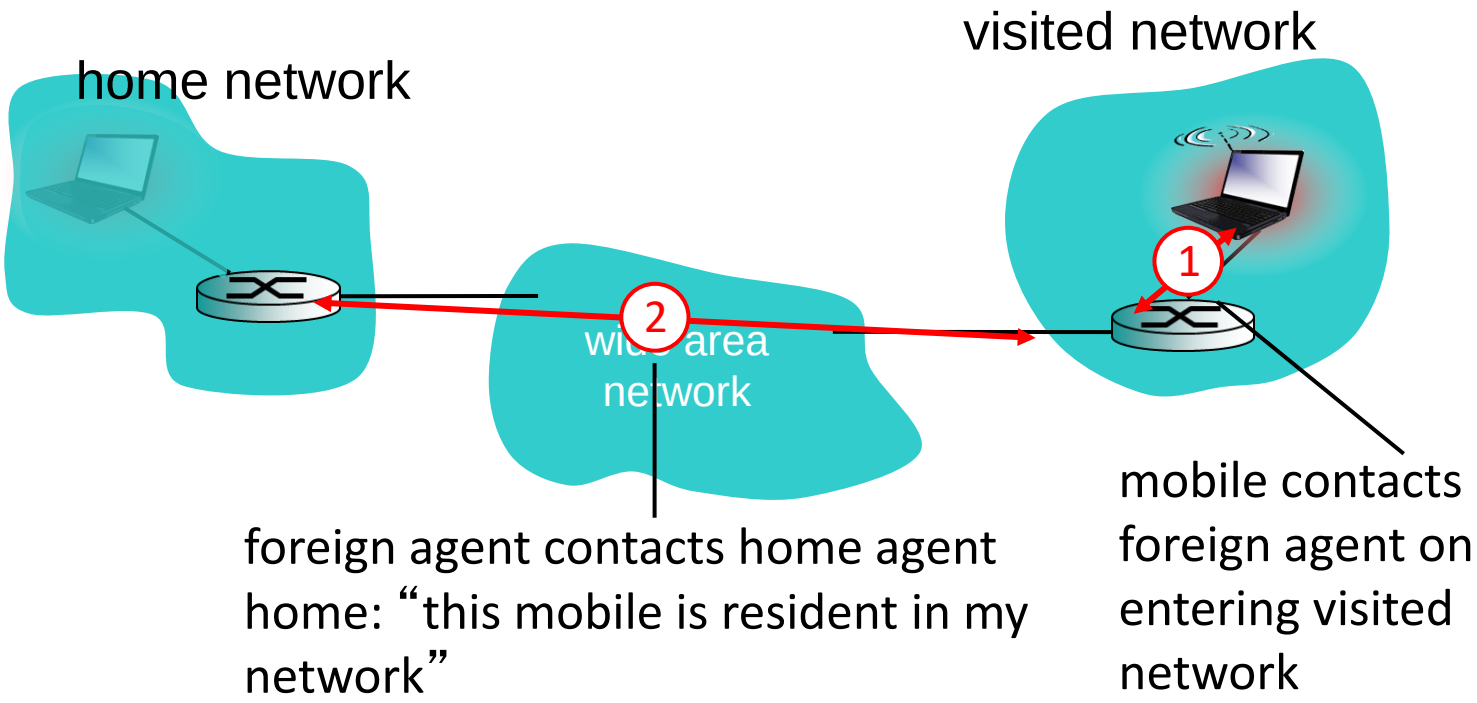
- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: approaches

- *let routing handle it:* routers advertise permanent addr… bile-nodes-in-residence via u… table exchange.
  - routing tables … e each mobile located
  - no changes to e… s

- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

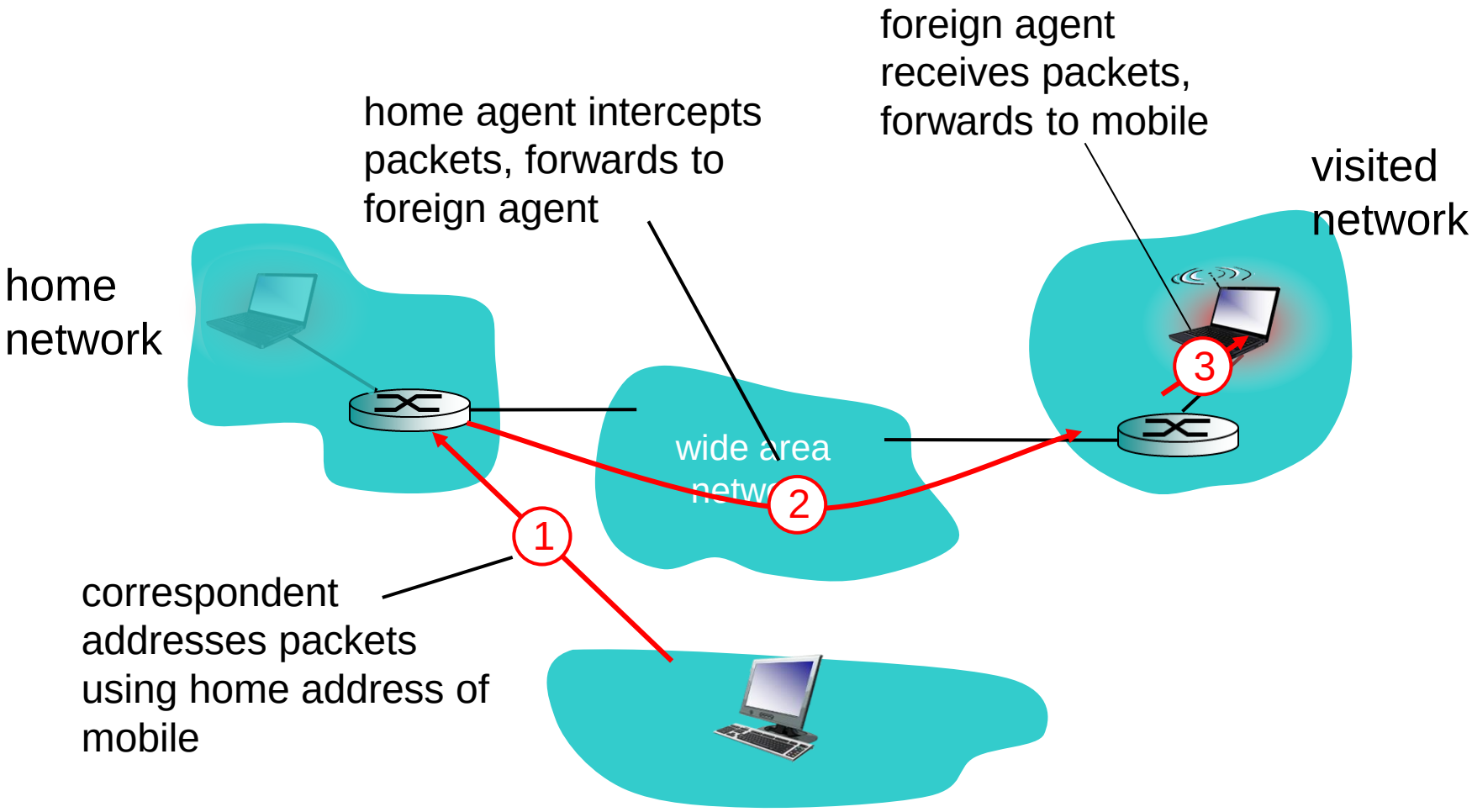
Mobility: registration



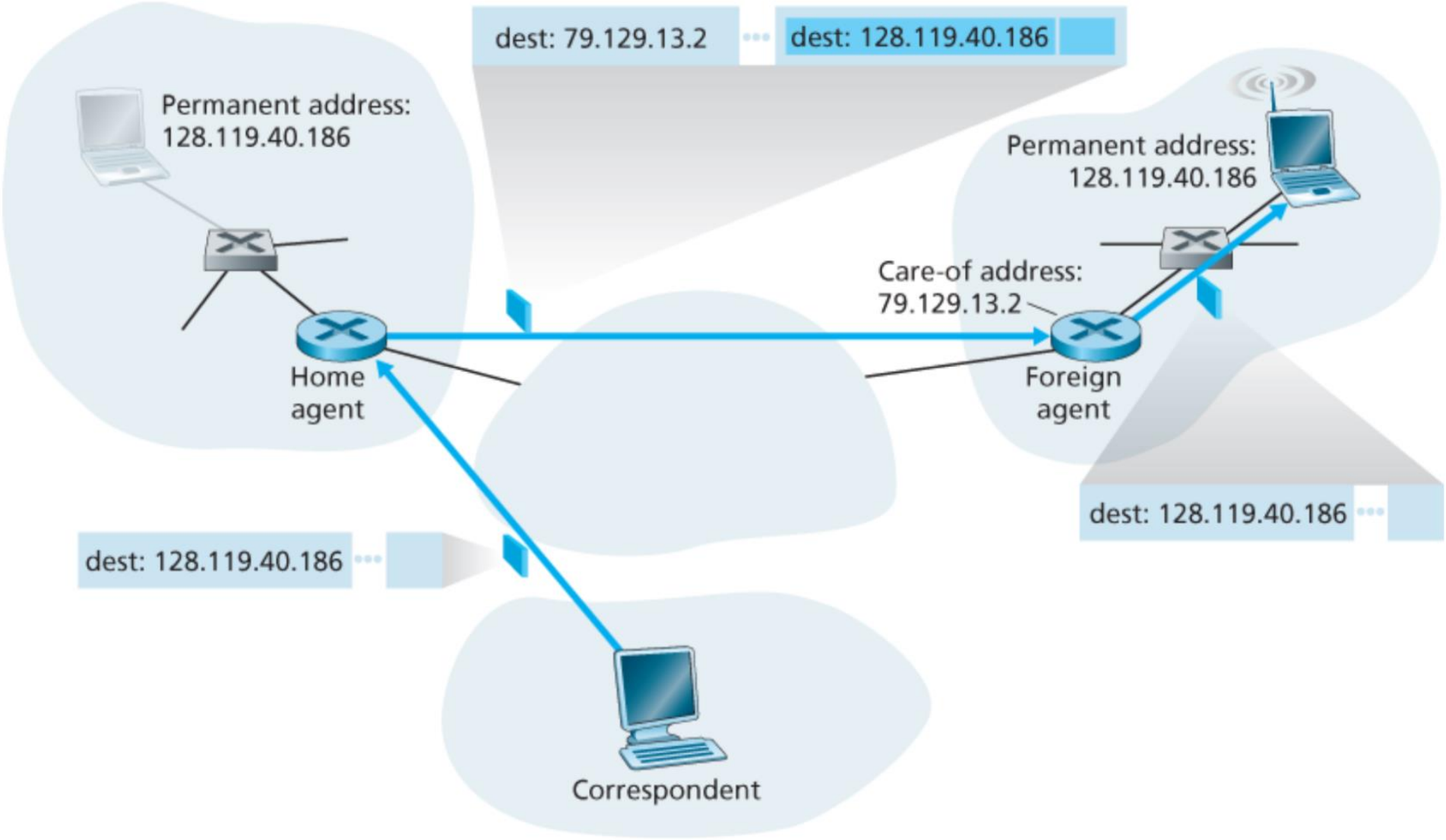
end result:

- foreign agent knows about mobile
- home agent knows location of mobile

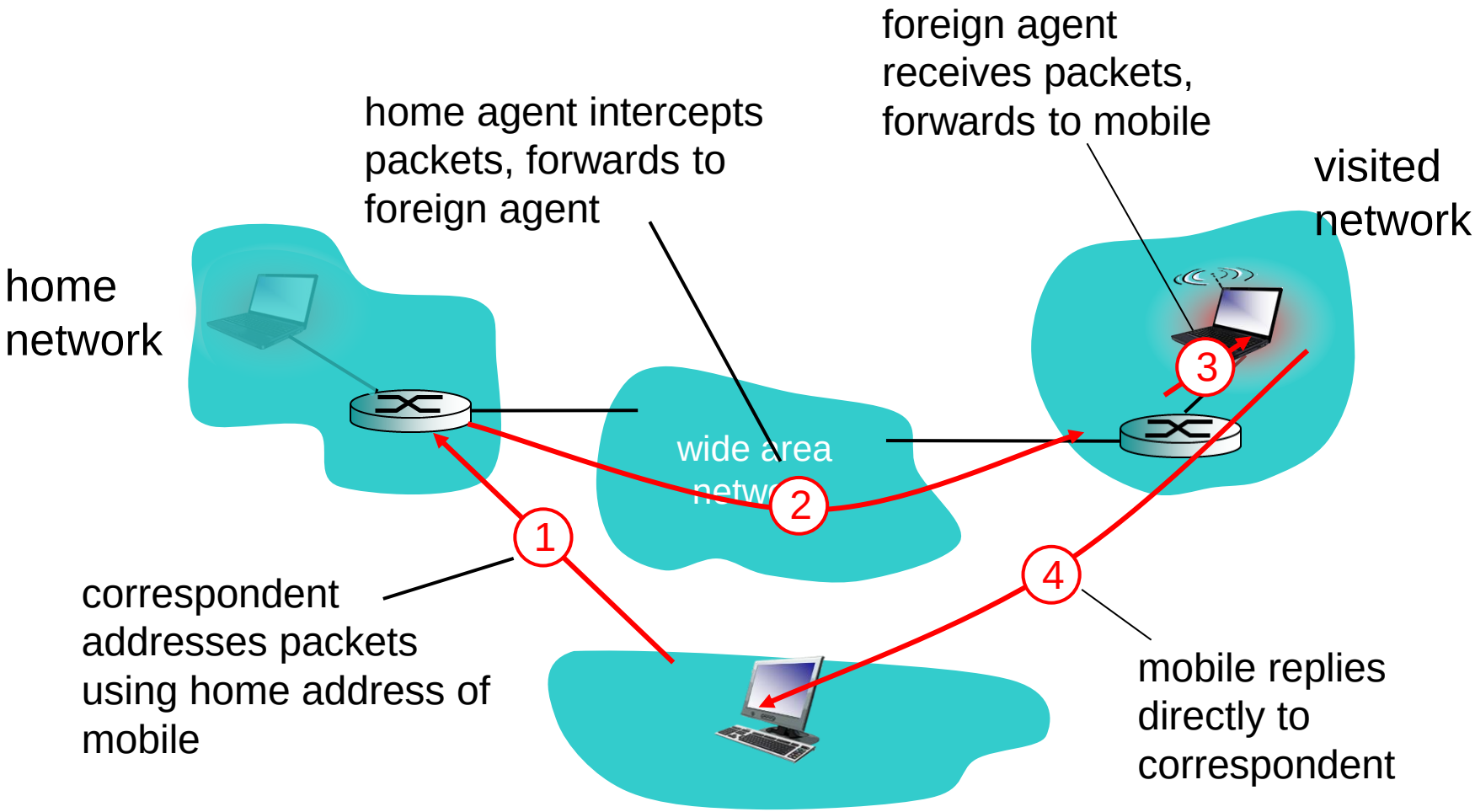
Mobility via indirect routing



Packet encapsulation

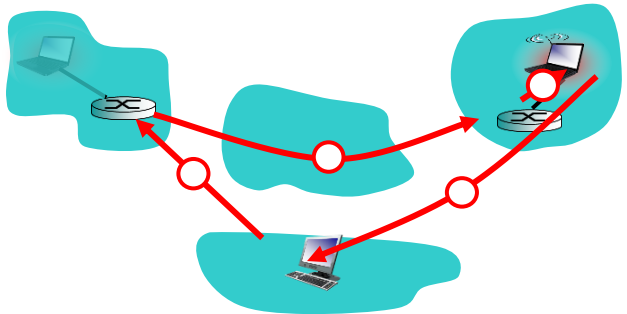


Mobility via indirect routing

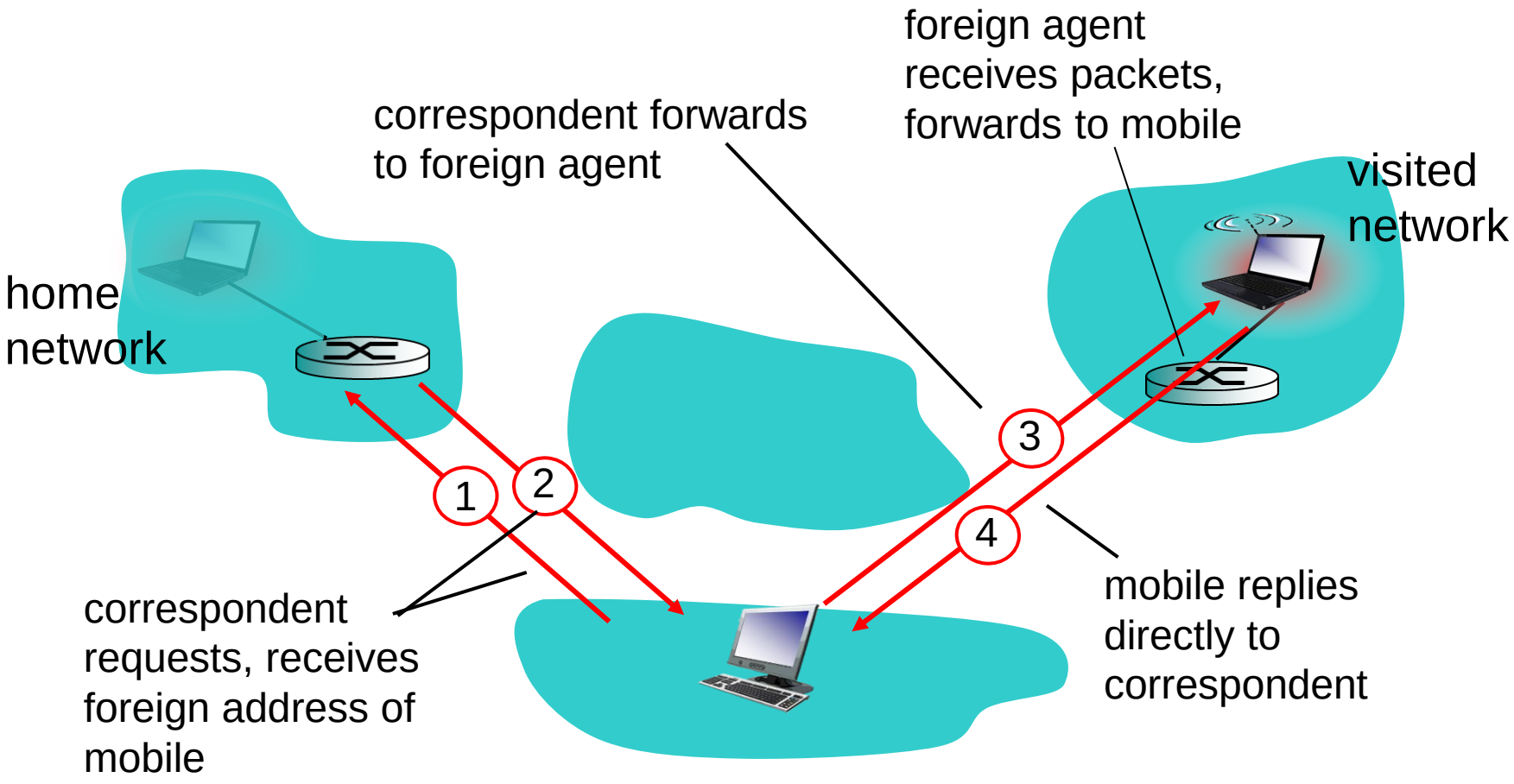


Indirect Routing: comments

- mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network



Mobility via direct routing



Mobility through multiple foreign networks