Data Link Layer – Part II

Prof. Dr. Xiaoming Fu
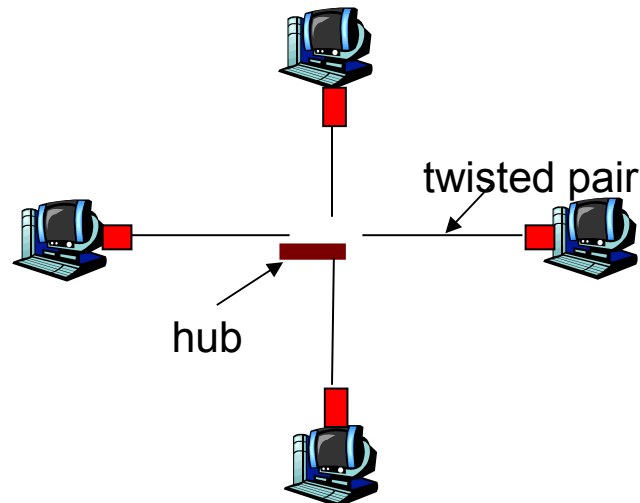
Link Layer

Hubs

… physical-layer ("dumb") repeaters:

- bits coming in one link go out *all* other links at same rate
- all nodes connected to hub can collide with one another
- no frame buffering
- no CSMA/CD at hub: host NICs detect collisions

twisted pair

hub

Don't really exist anymore

Switch

- link-layer device: smarter than hubs, take *active* role
  - store, forward Ethernet frames
  - examine incoming frame's MAC address, selectively forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment

- *transparent*
  - hosts are unaware of presence of switches

- *plug-and-play, self-learning*
  - switches do not need to be configured

# Switch: allows *multiple* simultaneous transmissions

○ hosts have dedicated, direct connection to switch

○ switches buffer packets

○ Ethernet protocol used on *each* incoming link, but no collisions; full duplex

  ○ each link is its own collision domain

○ *switching:* A-to-A' and B-to-B' simultaneously, without collisions

  ○ not possible with dumb hub
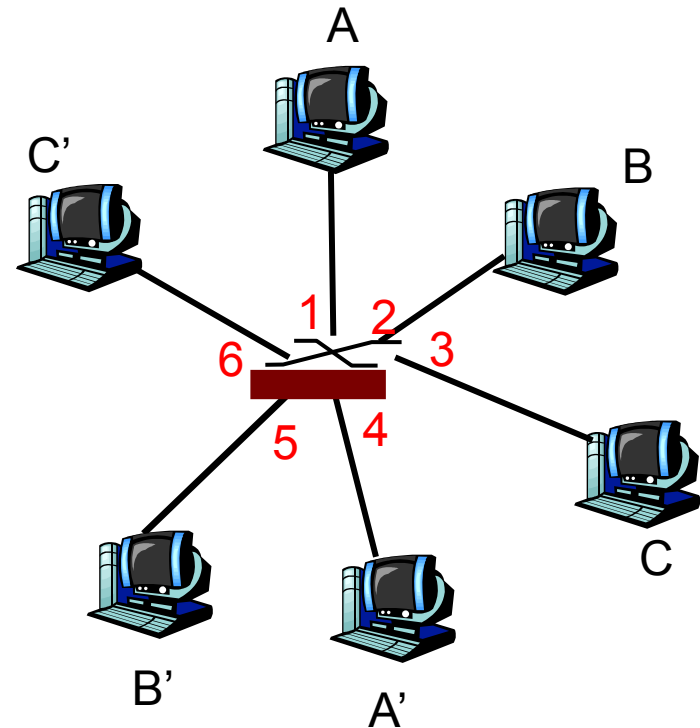
switch with six interfaces
(*1,2,3,4,5,6*)

Switch Table

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

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

   ○ (MAC address of host, interface to reach host, time stamp)

○ looks like a routing table!

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

   ○ something like a routing protocol?
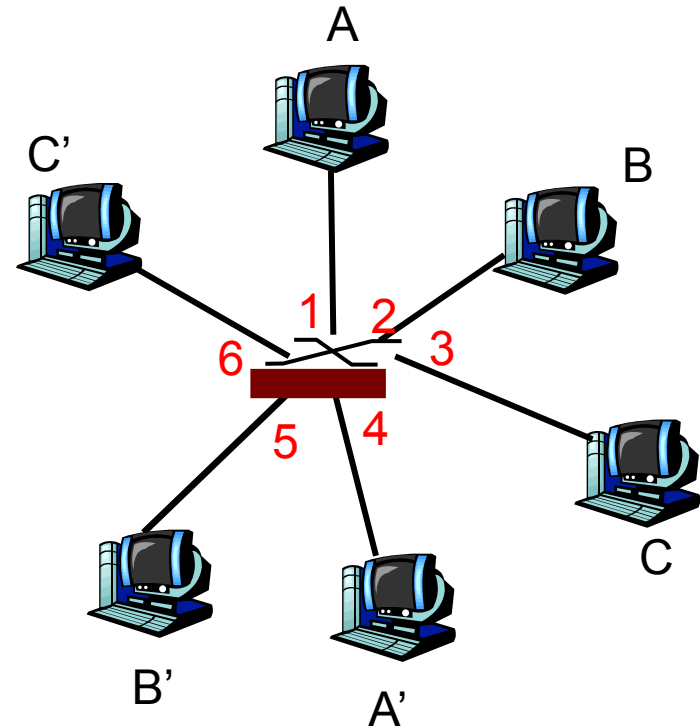
switch with six interfaces
(1,2,3,4,5,6)

Switch: self-learning

Source: A
Dest: A'

A | A | A' |

- 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

C'

B

1 2

6 3

5 4

C

B'

A'
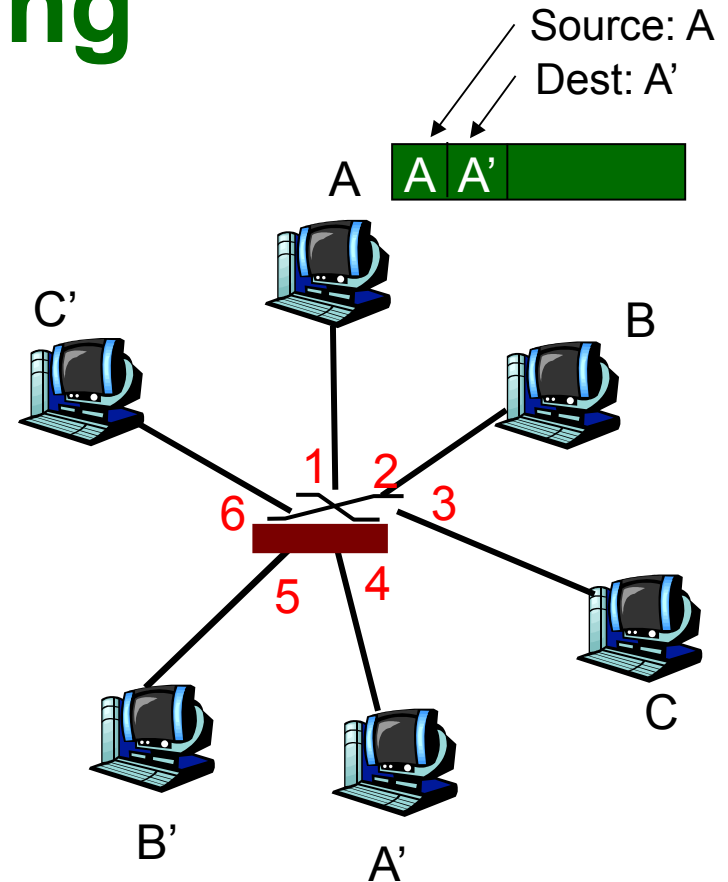
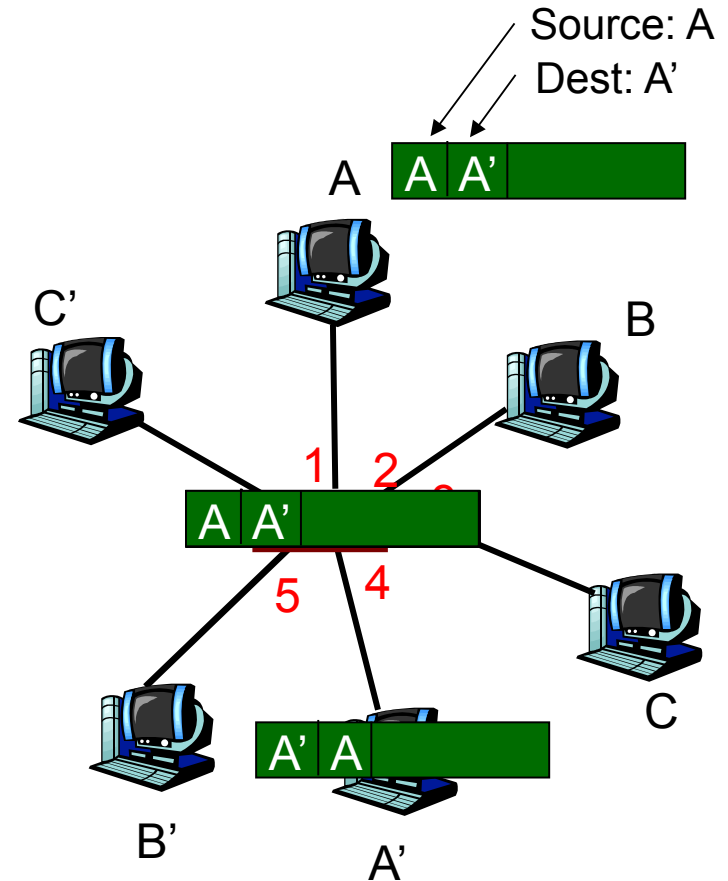| MAC addr	interface	TTL
A	1	60

Switch table (initially empty)

Switch: frame filtering/forwarding

When frame received:

1. record link associated with sending host
2. index switch table using MAC dest address
3. **if** entry found for destination
   then {
       if dest on segment from which frame arrived
           then drop the frame

               else forward the frame on interface indicated

       }
       else flood

> *forward on all but the interface on which the frame arrived*

Self-learning, forwarding: example

○ frame destination unknown: *flood*

○ destination A location known: *selective send*

Source: A
Dest: A'

MAC addr	interface	TTL
A	1	60
A'	4	60

Switch table (initially empty)
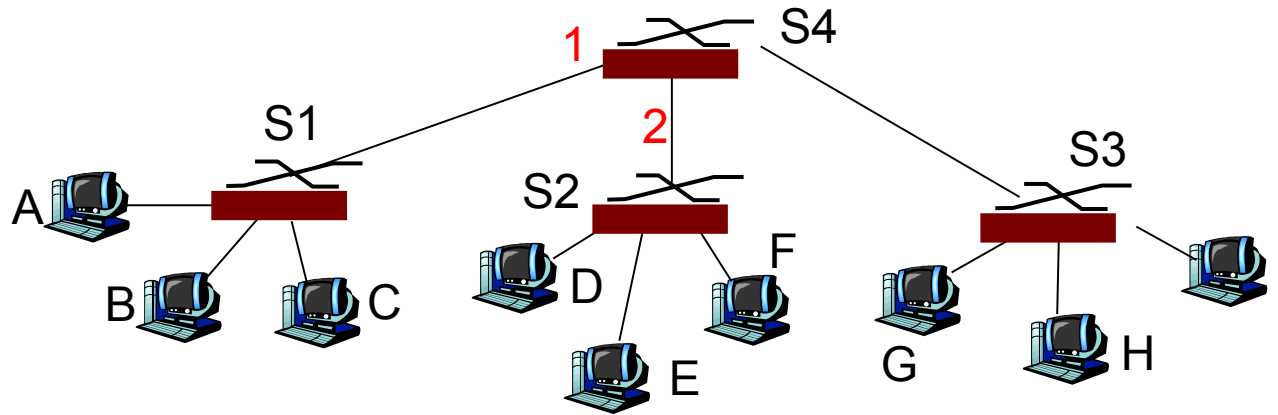
Interconnecting switches

○ switches can be connected together
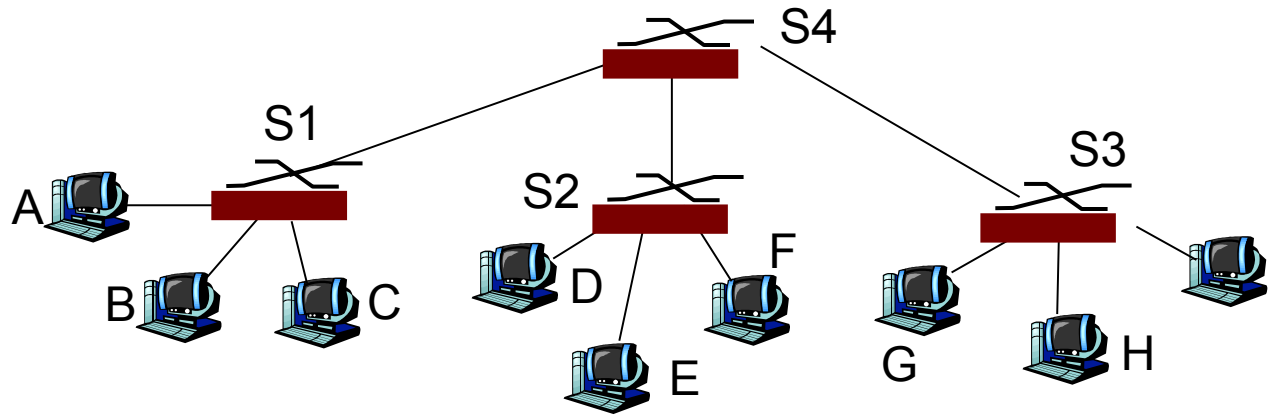
○ *Q:* sending from A to G - how does S1 know to forward frame destined to F via S4 and S3?

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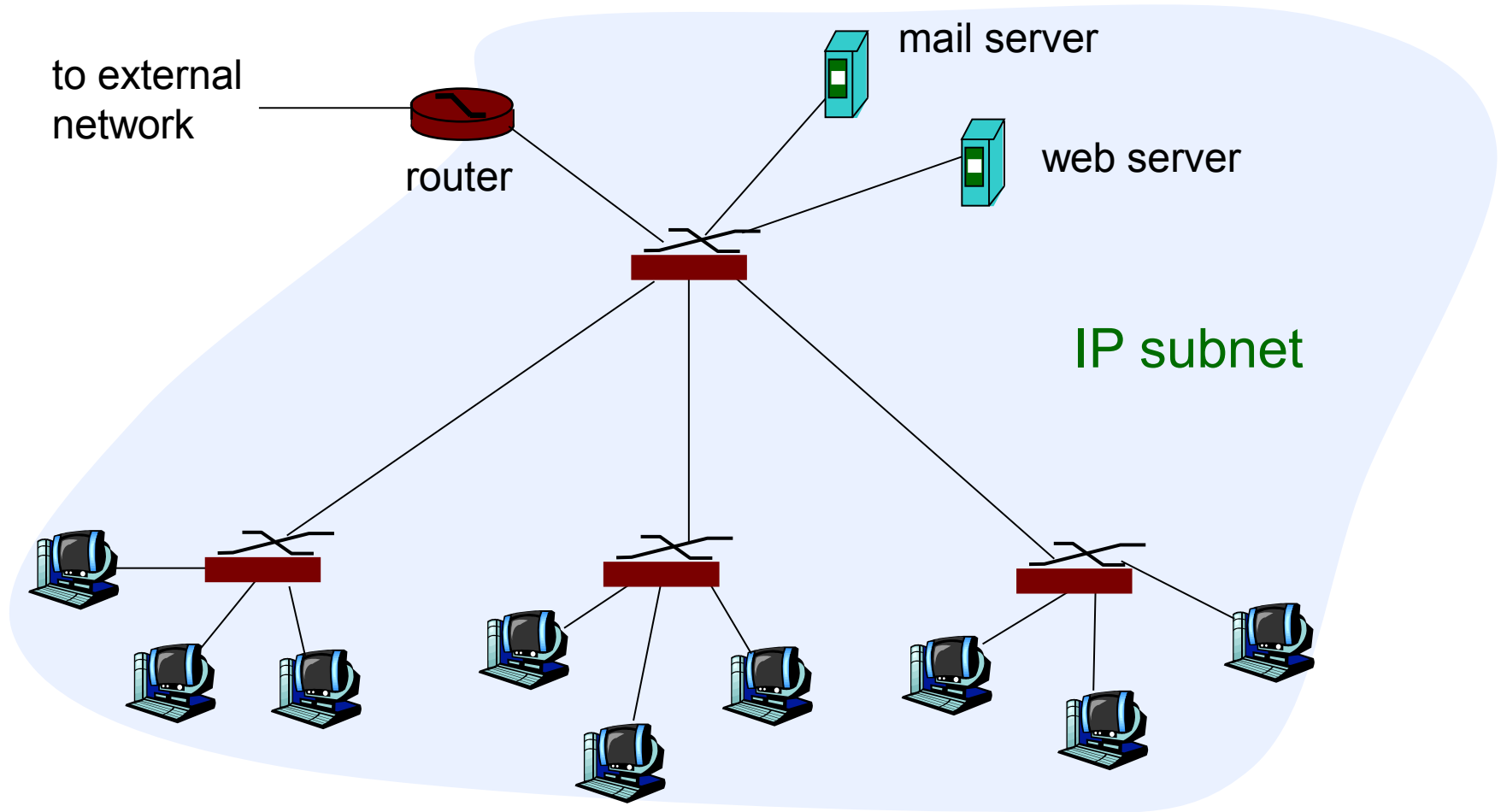
Self-learning multi-switch example

Suppose C sends frame to I, I responds to C

○ *Q:* show switch tables and packet forwarding in S1, S2, S3, S4

Institutional network (e.g. GöNet)

to external
network

router

mail server

web server

IP subnet

Switches vs. Routers

○ both store-and-forward devices
  ○ routers: network layer devices (examine network layer headers)
  ○ switches are link layer devices
○ routers maintain routing tables, implement routing algorithms
○ switches maintain switch tables, implement filtering, learning algorithms

Host	Bridge	Router	Host
5			5
4			4
3		3	3
2	2	2	2
1	1	1	1
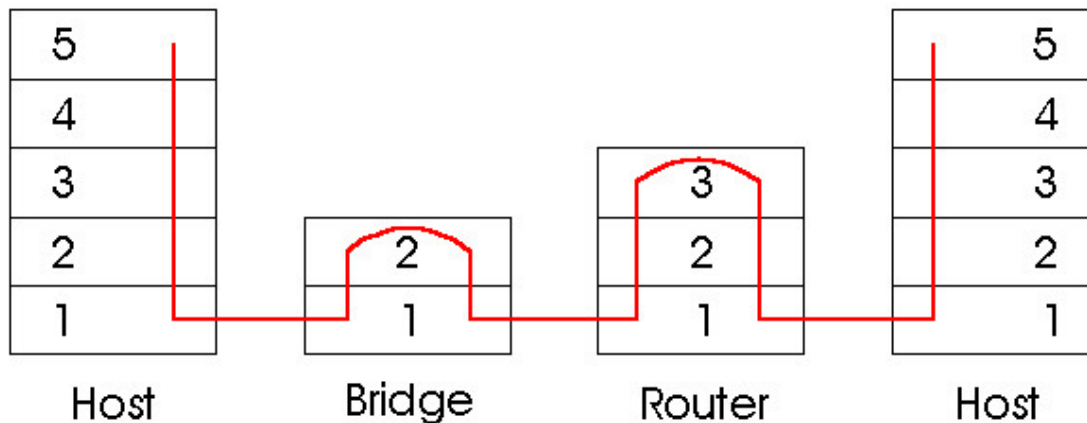
Link Layer

- 5.1 Introduction and services
- 5.2 Error detection and correction
- 5.3 Multiple access protocols
- 5.4 Link-Layer Addressing
- 5.5 Ethernet

- 5.6 Link-layer switches
- 5.7 PPP
- 5.8 Wireless links / Wi-Fi
- 5.9 Link Virtualization: ATM, MPLS

Point to Point Data Link Control

- one sender, one receiver, one link: easier than broadcast link:
  - no Media Access Control
  - no need for explicit MAC addressing
  - e.g., dialup link, ISDN line
- popular point-to-point DLC protocols:
  - PPP (point-to-point protocol)
  - HDLC: High level data link control (Data link used to be considered "high layer" in protocol stack!

PPP Design Requirements [RFC 1557]

- packet framing: encapsulation of network-layer datagram in data link frame
  - carry network layer data of any network layer protocol (not just IP) *at same time*
  - ability to demultiplex upwards
- bit transparency: must carry any bit pattern in the data field
- error detection (no correction)
- connection liveness: detect, signal link failure to network layer
- network layer address negotiation: endpoint can learn/configure each other's network address

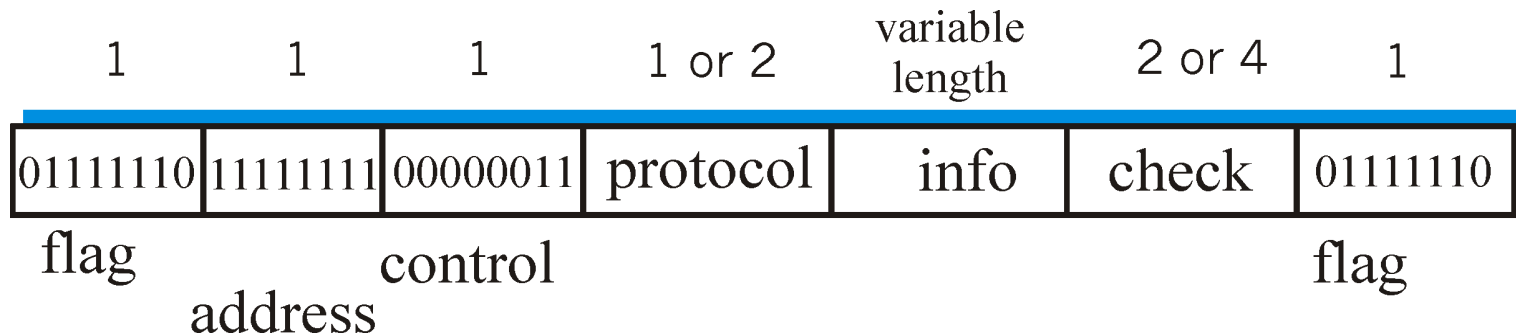# PPP non-requirements

○ no error correction/recovery

○ no flow control

○ out of order delivery OK

○ no need to support multipoint links (e.g., polling)

Error recovery, flow control, data re-ordering
all relegated to higher layers!

PPP Data Frame

○ Flag: delimiter (framing)

○ Address: does nothing (only one option)

○ Control: does nothing; in the future possible multiple control fields

○ Protocol: upper layer protocol to which frame delivered (eg, PPP-LCP, IP, IPCP, etc)

1	1	1	1 or 2	variable length	2 or 4	1
01111110	11111111	00000011	protocol	info	check	01111110
flag	address	control				flag

PPP Data Frame

- info: upper layer data being carried
- check: cyclic redundancy check for error detection

1	1	1	1 or 2	variable length	2 or 4	1
01111110	11111111	00000011	protocol	info	check	01111110

flag   address   control   flag
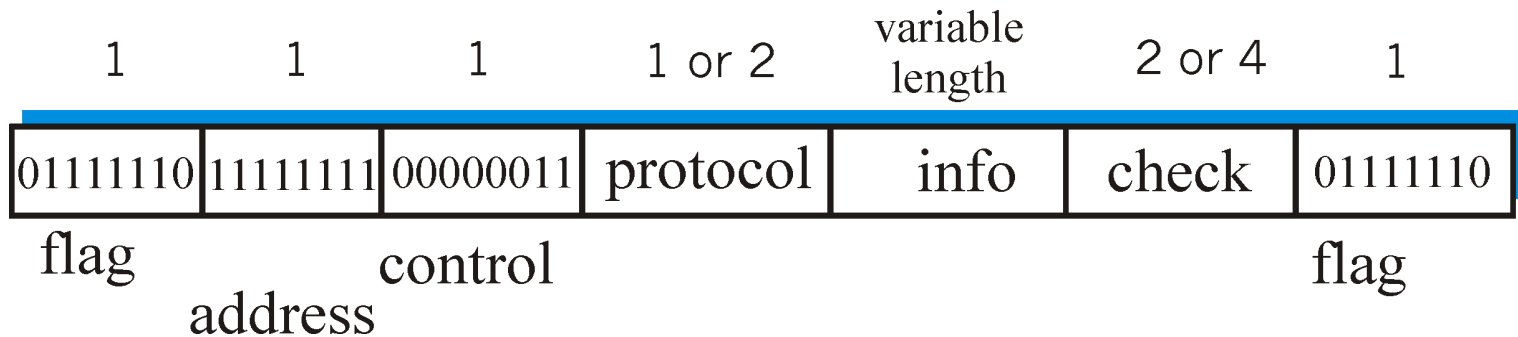
Byte Stuffing

○ "data transparency" requirement: data field must be allowed to include flag pattern <01111110>

    ○ Q: is received <01111110> data or flag?

○ Sender: adds ("stuffs") extra < 01111110> byte after each < 01111110> *data* byte

○ Receiver:

    ○ two 01111110 bytes in a row: discard first byte, continue data reception

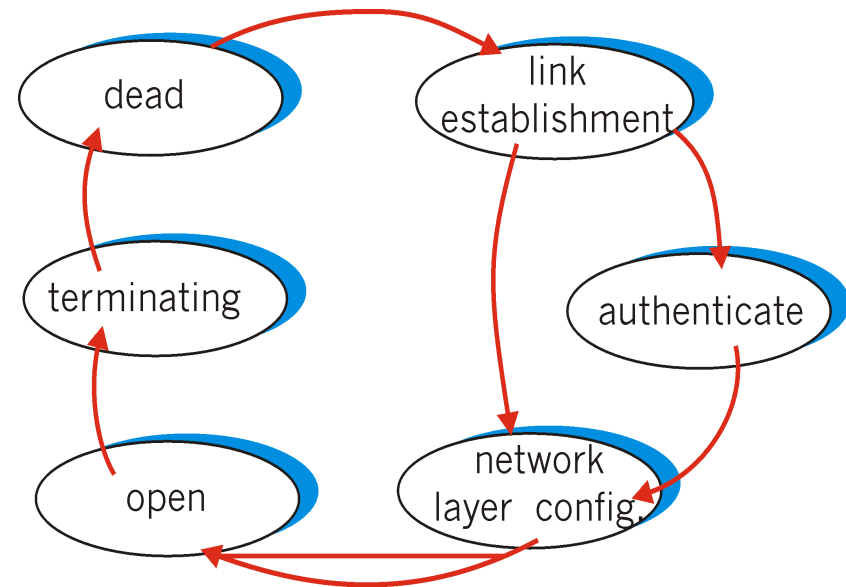   ○ single 01111110: flag byte

Byte Stuffing

flag byte
pattern
in data
to send

b5
b4
01111110
b2
b1

b1
b2
01111110
b4
b5

PPP

PPP

b5 b4 01111110 01111101 b2 b1

flag byte pattern plus
stuffed byte in transmitted
data
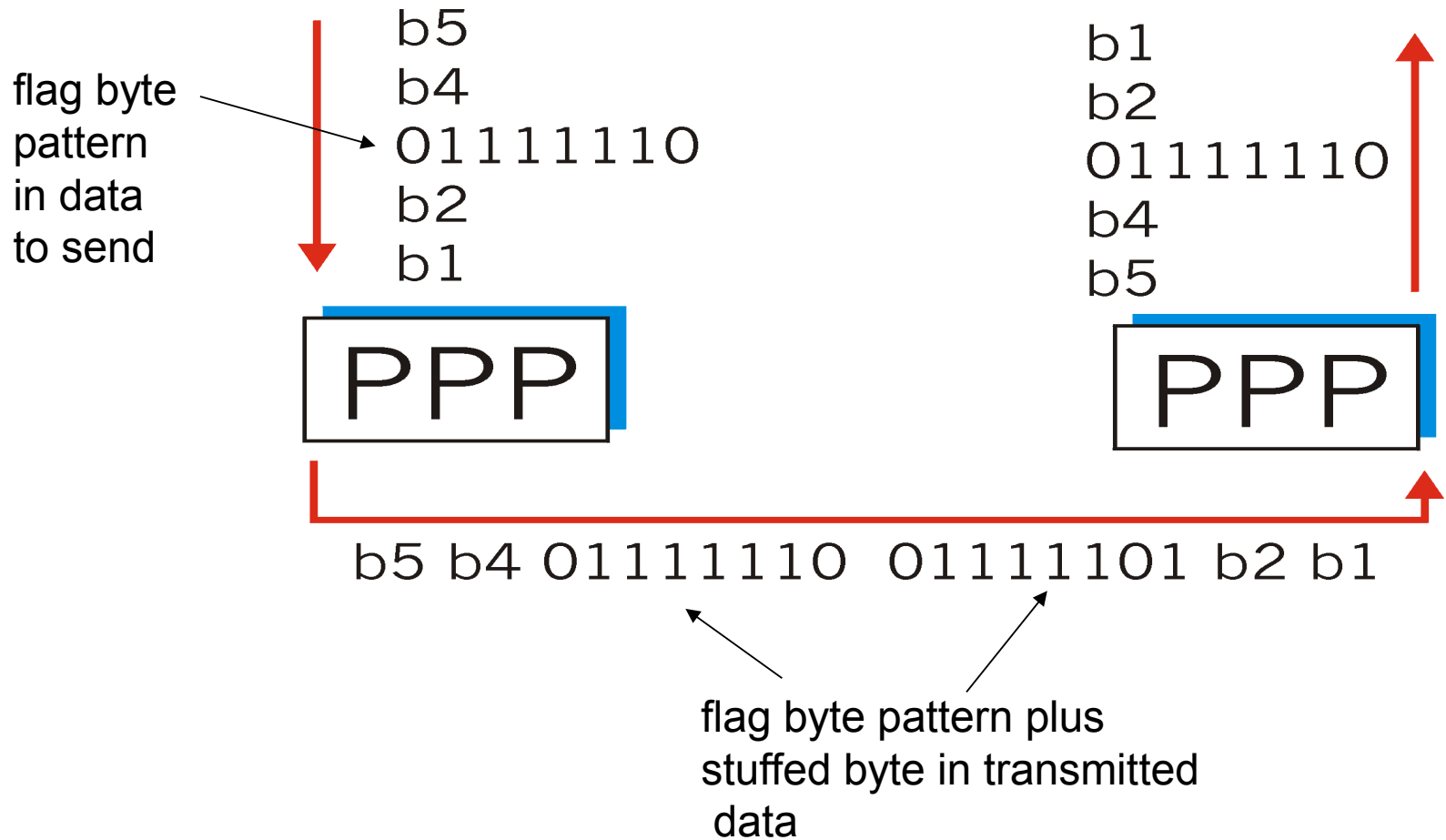
PPP Data Control Protocol

Before exchanging network-layer data, data link peers must

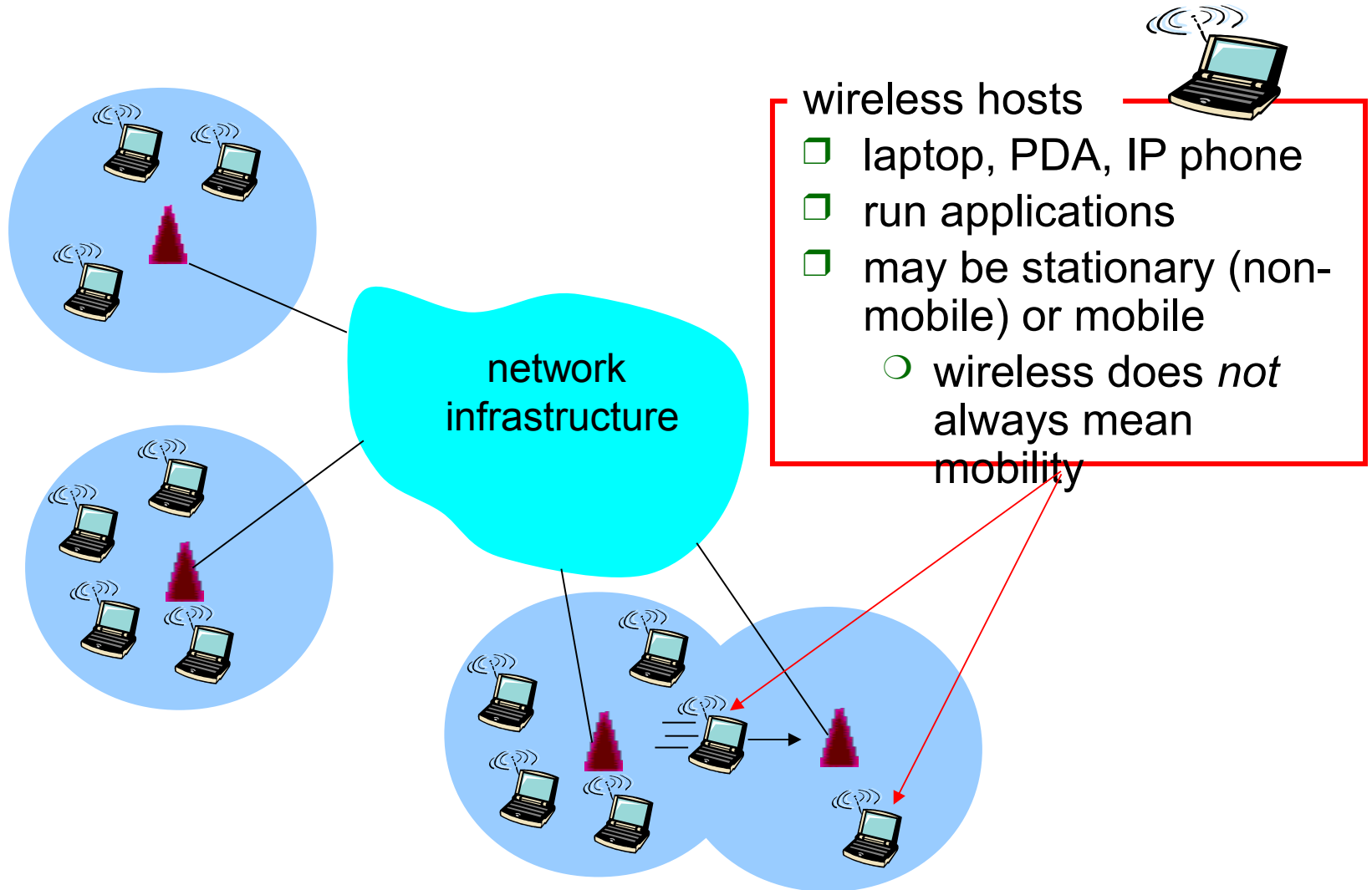○ configure PPP link (max. frame length, authentication)

○ learn/configure network layer information

○ for IP: carry IP Control Protocol (IPCP) msgs (protocol field: 8021) to configure/learn IP address

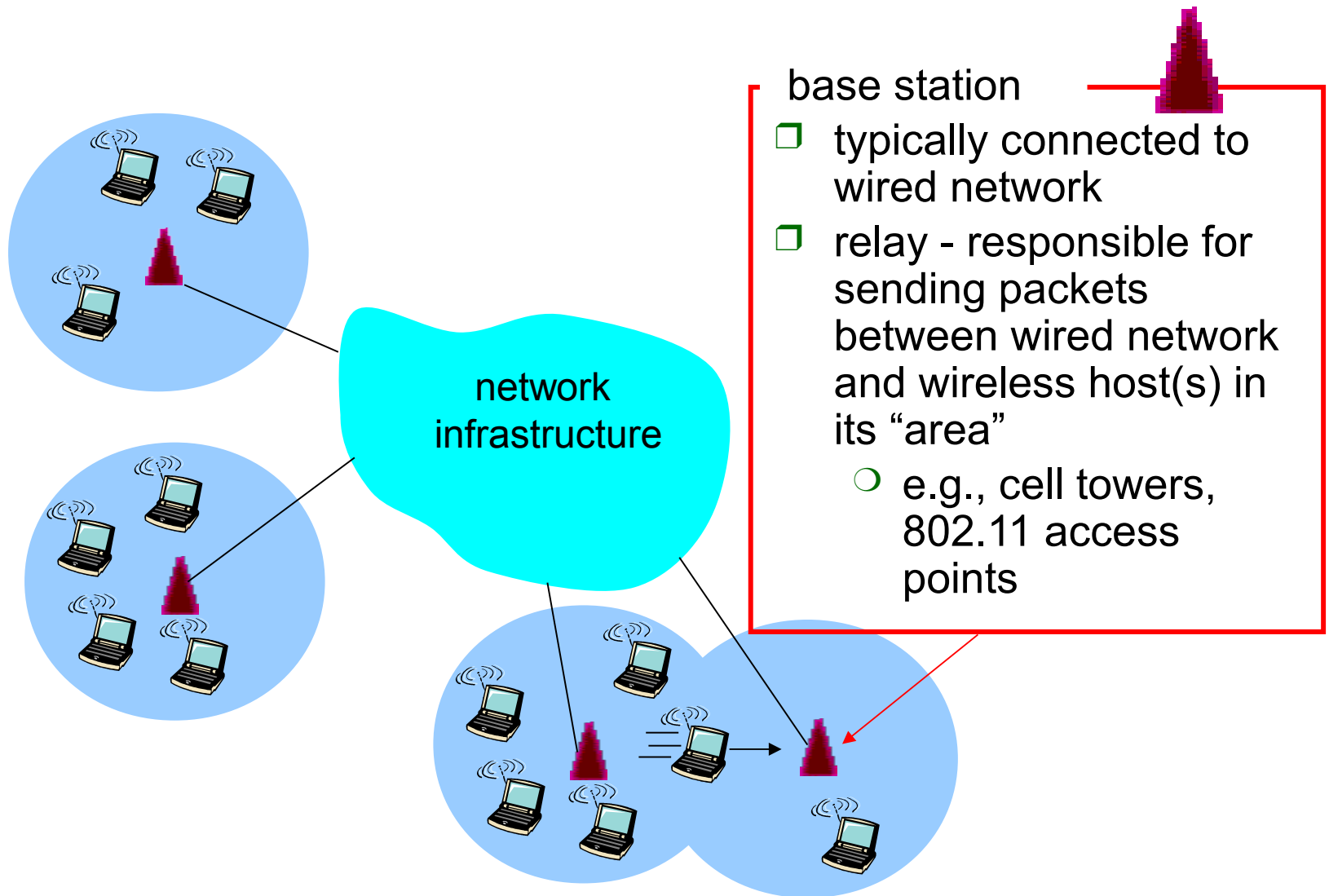# Link Layer

Elements of a wireless network

network
infrastructure

wireless hosts
- ❑ laptop, PDA, IP phone
- ❑ run applications
- ❑ may be stationary (non-mobile) or mobile
  - ○ wireless does *not* always mean mobility

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

network infrastructure

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 data rates, transmission distance

network infrastructure
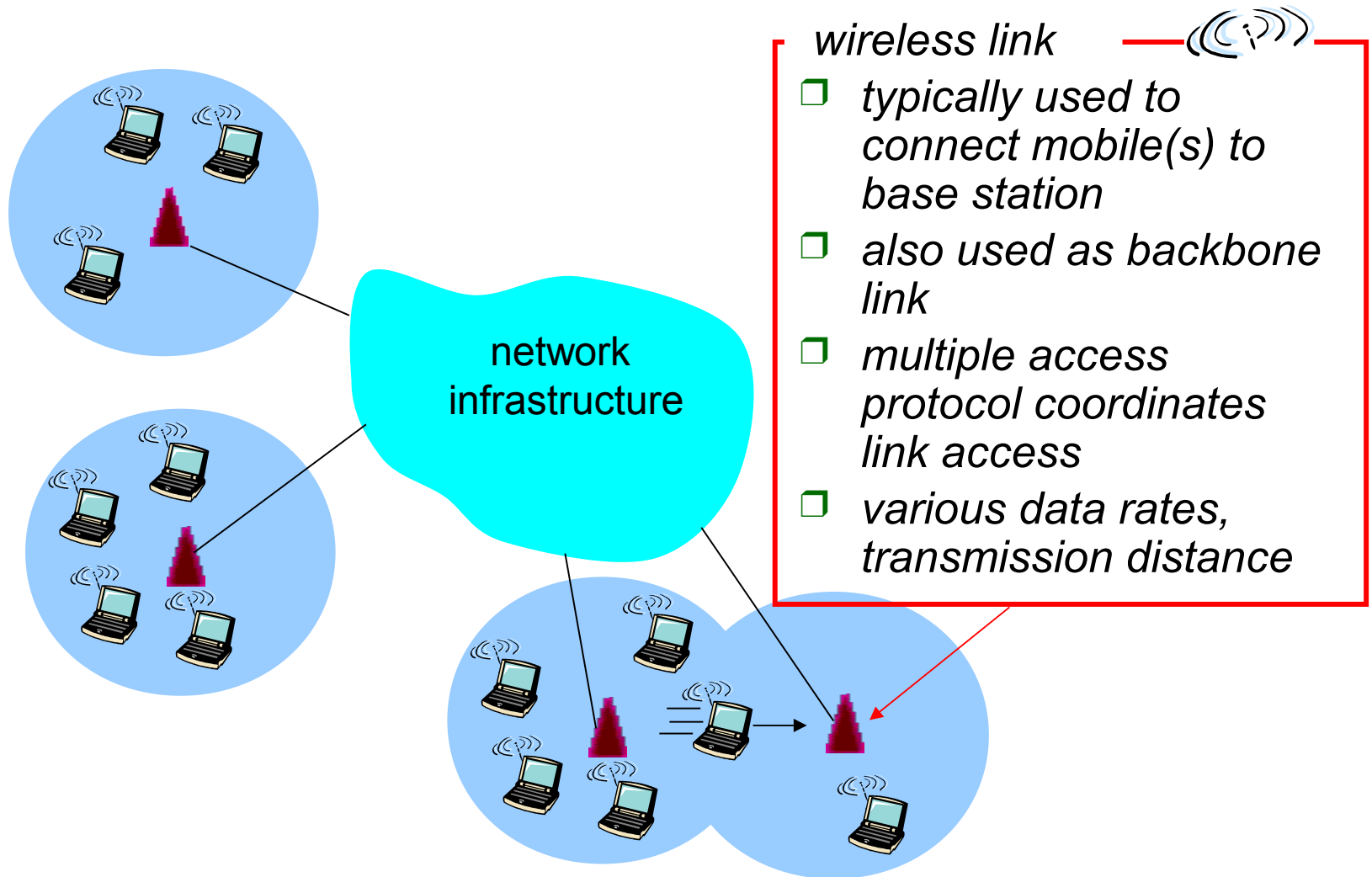
Characteristics of selected wireless link standards

Data rate (Mbps)

	Indoor 10-30m	Outdoor 50-200m	Mid-range outdoor 200m – 4 Km	Long-range outdoor 5Km – 20 Km	
200	802.11n				
54	802.11a,g	802.11a,g point-to-point			data
5-11	802.11b	802.16 (WiMAX)			
4		UMTS/WCDMA-HSPDA, CDMA2000-1xEVDO			3G cellular enhanced
1	802.15				
.384		UMTS/WCDMA, CDMA2000			3G
.056		IS-95, CDMA, GSM			2G

Elements of a wireless network

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

network infrastructure

Elements of a wireless network

ad hoc mode
- *no base stations*
- *nodes can only transmit to other nodes within link coverage*
- *nodes organize themselves into a network: route among themselves*

Wireless network taxonomy

|	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: mesh net
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless Link Characteristics (1)

Differences from wired link ….

- ○ decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- ○ interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- ○ multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

Wireless Link Characteristics (2)

○ SNR: signal-to-noise ratio
  ○ larger SNR – easier to extract signal from noise (a "good thing")

○ *SNR versus BER (bit error rate) tradeoffs*
  ○ *given physical layer:* increase power -> increase SNR->decrease BER
  ○ *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    • SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)
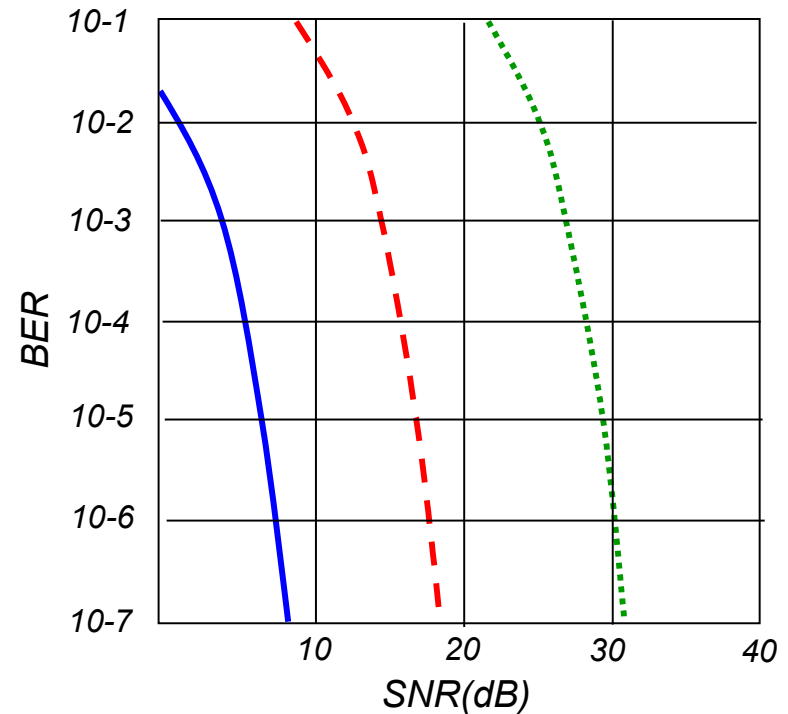
QAM256 (8 Mbps)

QAM16 (4 Mbps)

BPSK (1 Mbps)

Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):
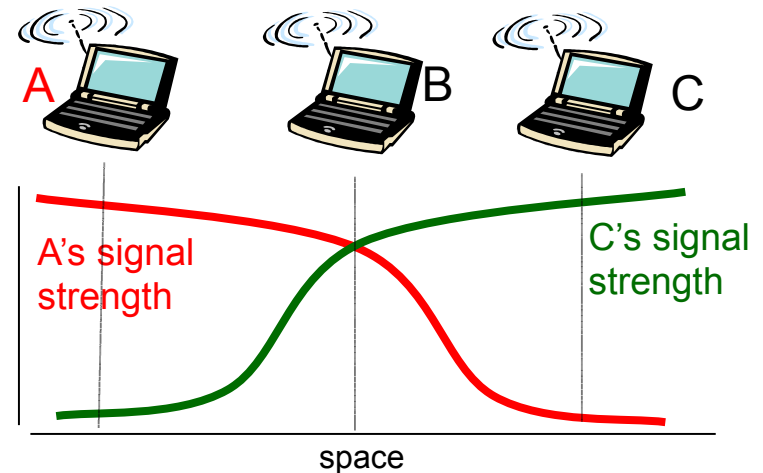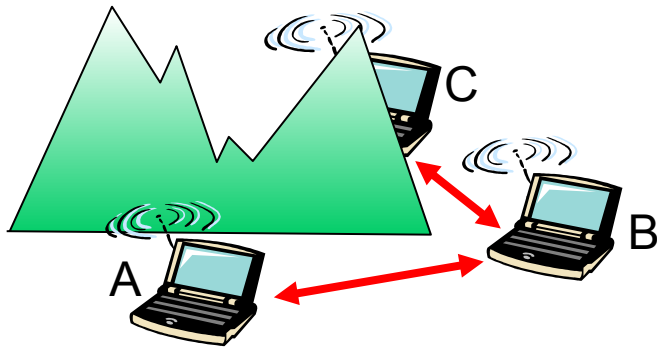
Hidden terminal problem

- ❐ *B, A hear each other*
- ❐ *B, C hear each other*
- ❐ *A, C can not hear each other*
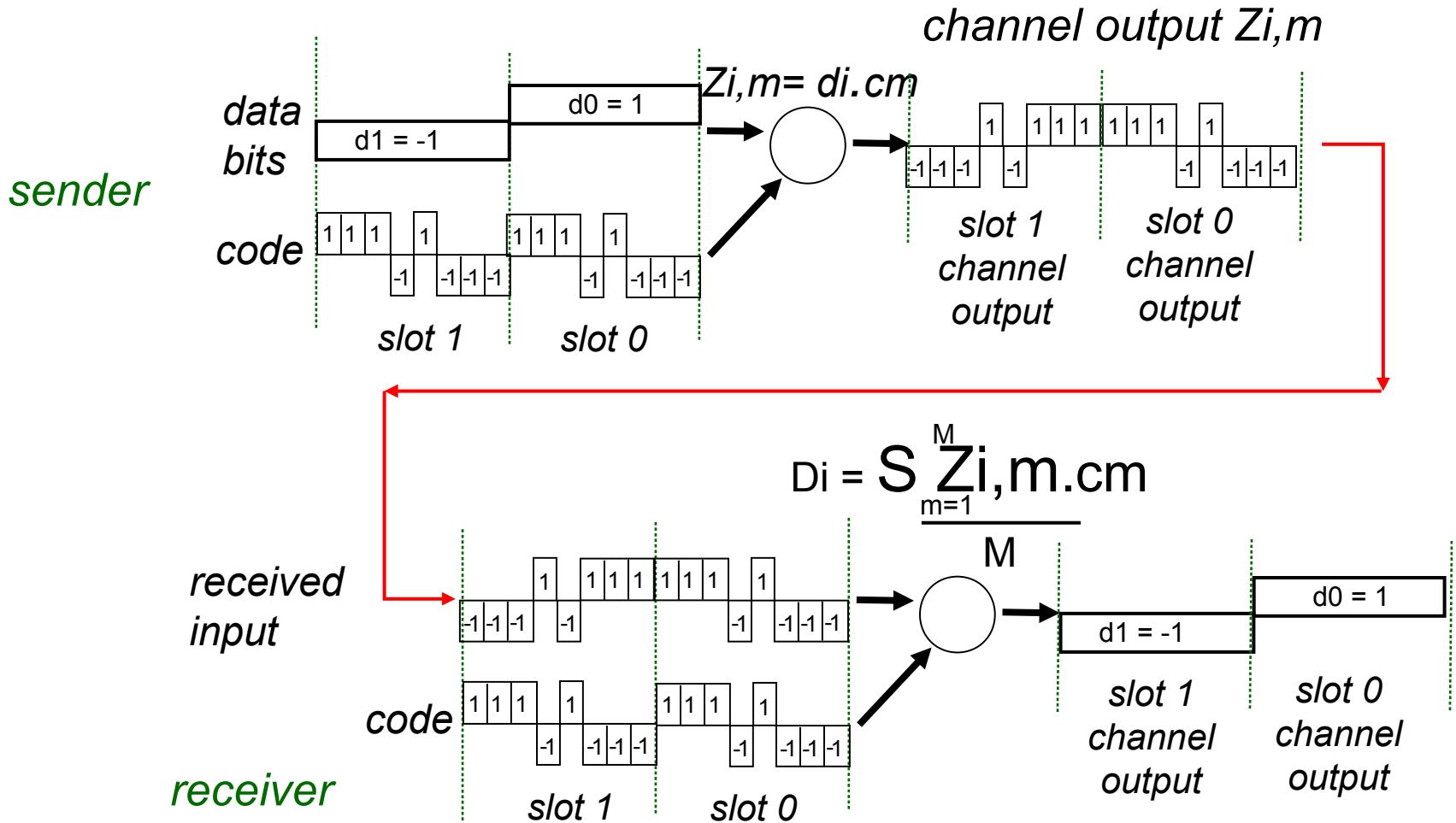
means A, C unaware of their interference at B

Signal attenuation:

- ❐ *B, A hear each other*
- ❐ *B, C hear each other*
- ❐ *A, C can not hear each other interfering at B*
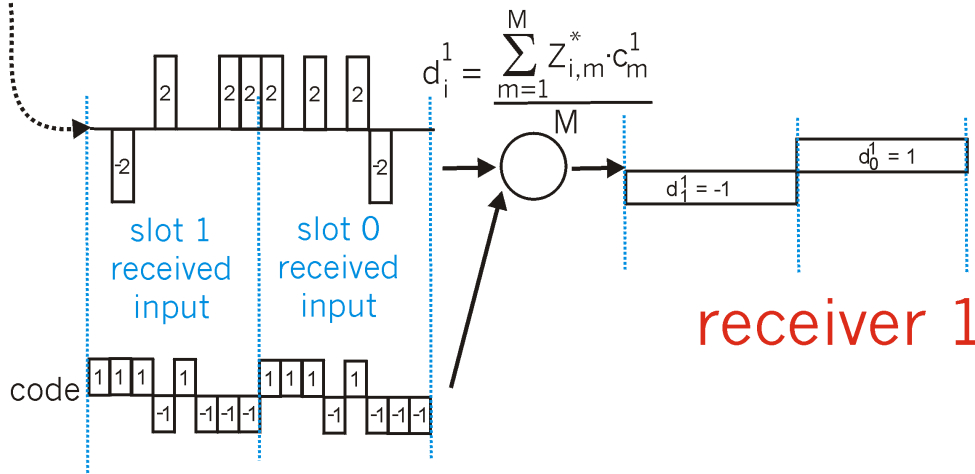
Code Division Multiple Access (CDMA)

○ used in several wireless broadcast channels (cellular, satellite, etc) standards

○ unique "code" assigned to each user; i.e., code set partitioning

○ all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data

○ *encoded signal* = (original data) X (chipping sequence)

○ *decoding:* inner-product of encoded signal and chipping sequence

○ allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

CDMA Encode/Decode

$Z_{i,m} = d_i.c_m$

channel output $Z_{i,m}$

$$D_i = \frac{\sum\limits_{m=1}^{M} Z_{i,m}.c_m}{M}$$

CDMA: two-sender interference

senders

$$Z^1_{i,m} = d^1_i \cdot c^1_m$$

$d^1_0 = 1$

$d^1_1 = -1$

code: 1 1 1 1 -1 -1 -1 -1

channel, $Z^*_{i,m}$

$d^2_1 = 1$ $d^2_0 = 1$

$$Z^2_{i,m} = d^2_i \cdot c^2_m$$

$$d^1_i = \dfrac{\sum\limits_{m=1}^{M} Z^*_{i,m} \cdot c^1_m}{M}$$

$d^1_0 = 1$

$d^1_1 = -1$

slot 1 received input   slot 0 received input

receiver 1
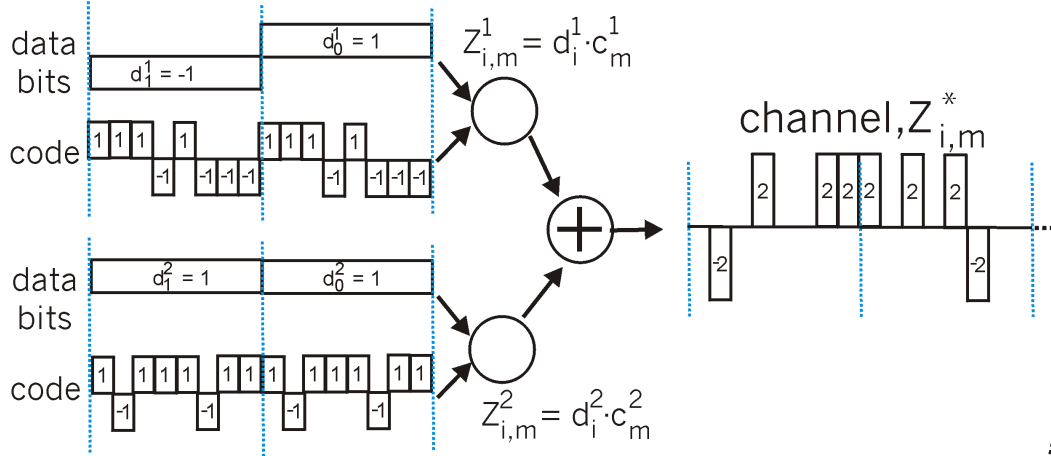
code

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code

- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

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

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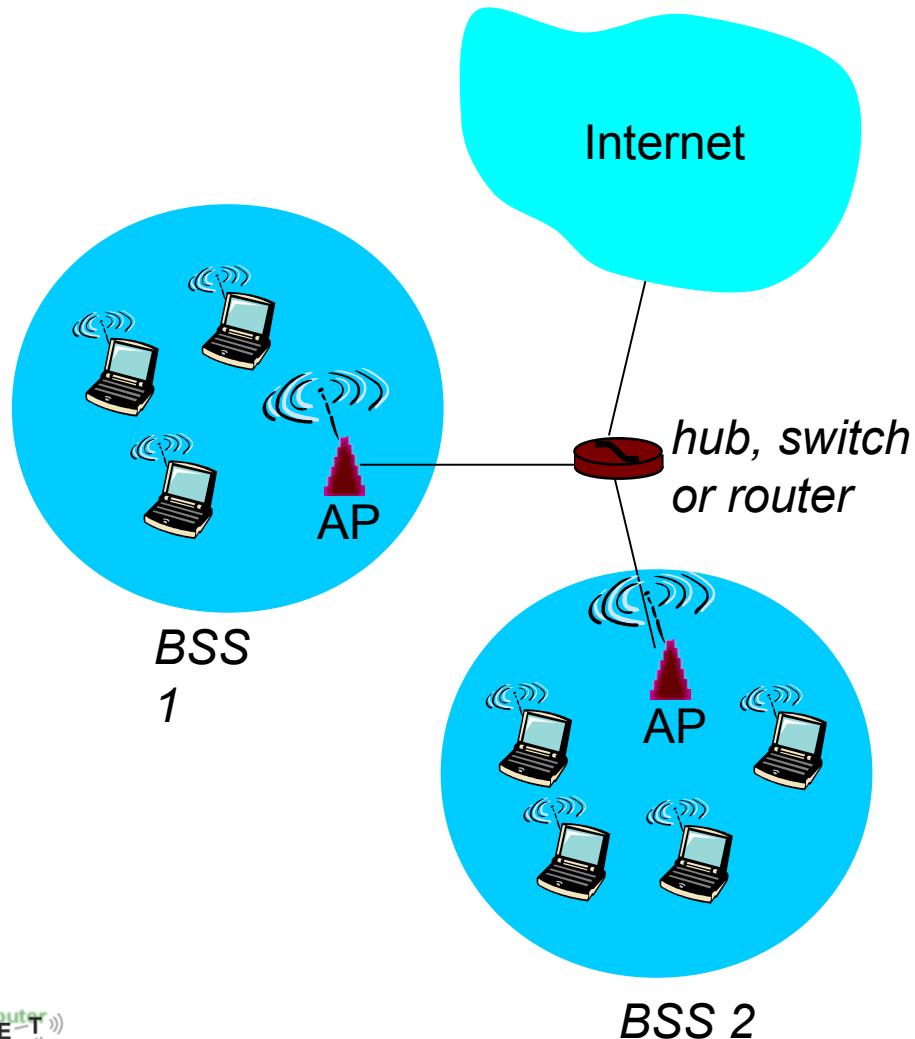
- *wireless host communicates with base station*
  - *base station = access point (AP)*
- *Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:*
  - *wireless hosts*
  - *access point (AP): base station*
  - *ad hoc mode: hosts only*

802.11: Channels, association

○ 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  ○ AP admin chooses frequency for AP
  ○ interference possible: channel can be same as that chosen by neighboring AP!
○ 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
  ○ may perform authentication [Chapter 8]
  ○ will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning
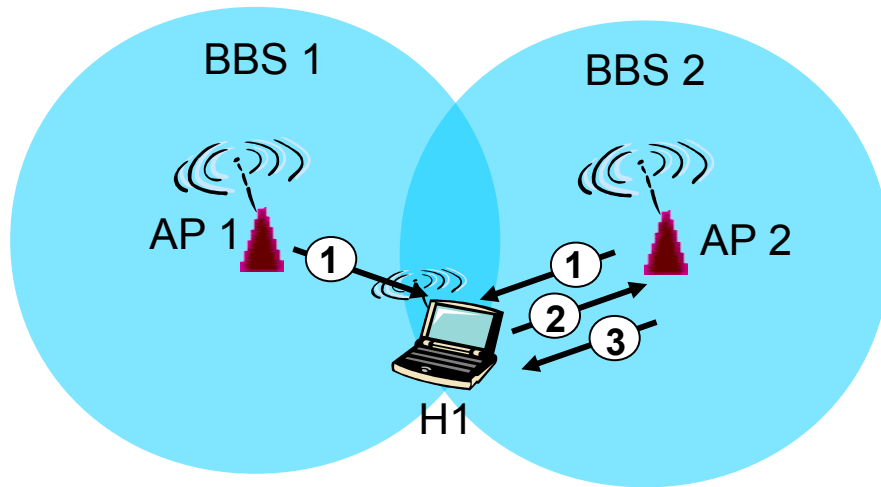
Passive Scanning:

(1) beacon frames sent from APs

(2) association Request frame sent:
H1 to selected AP

(3) association Response frame sent:
H1 to selected AP
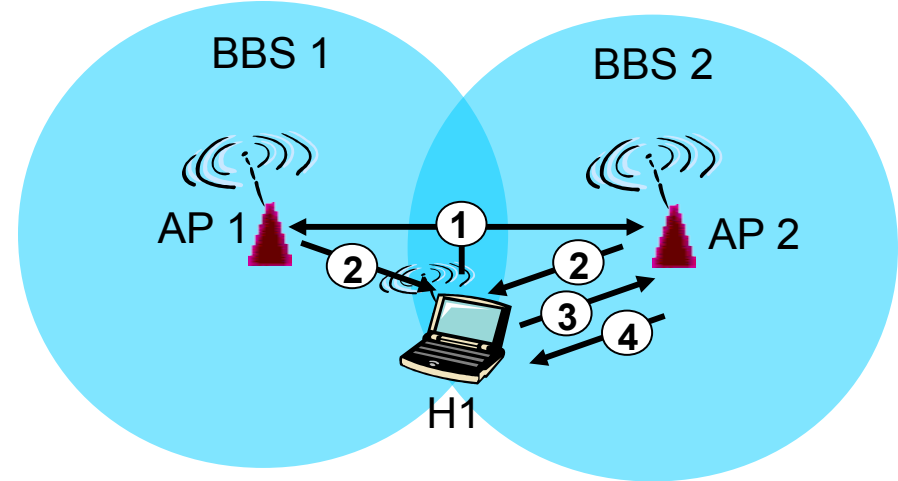
<u>Active Scanning</u>:

(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: H1 to selected AP

IEEE 802.11: multiple access

○ avoid collisions: 2+ nodes transmitting at same time

○ 802.11: CSMA - sense before transmitting
  ○ don't collide with ongoing transmission by other node

○ 802.11: *no* collision detection!
  ○ difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  ○ can't sense all collisions in any case: hidden terminal, fading
  ○ goal: *avoid collisions:* CSMA/C(ollision)A(voidance)

A's signal strength

C's signal strength

space
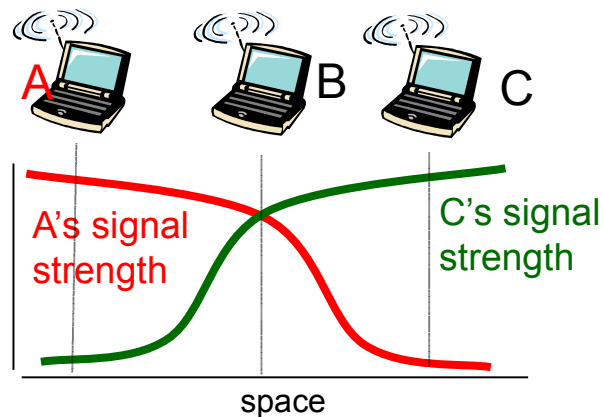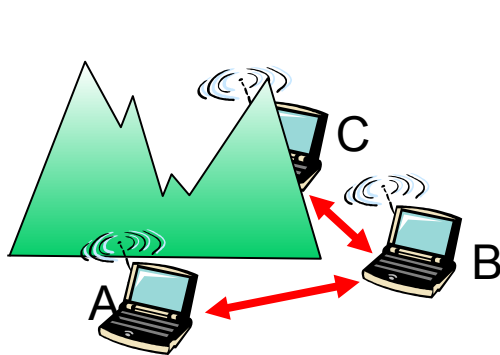
IEEE 802.11 MAC Protocol: CSMA/CA

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

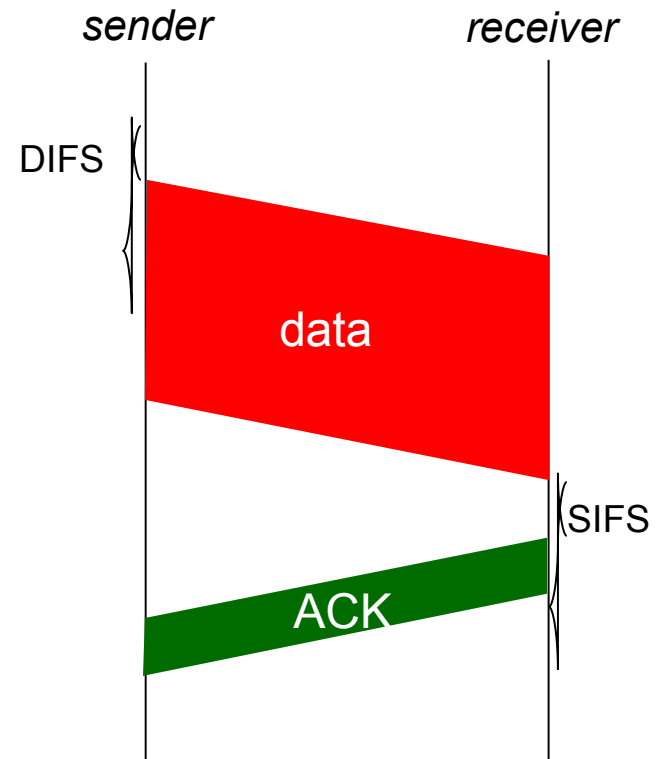timer counts down while channel idle

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)

sender   *receiver*

DIFS

data

SIFS

ACK

Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

○ sender first transmits *small* request-to-send (RTS) packets 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

> *avoid data frame collisions completely using small reservation packets!*

Collision Avoidance: RTS-CTS exchange

A

AP

B

RTS(A)

RTS(B)

reservation collision

RTS(A)

CTS(A)

CTS(A)

DATA (A)

defer

time

ACK(A)

ACK(A)

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 4: used only in ad hoc mode
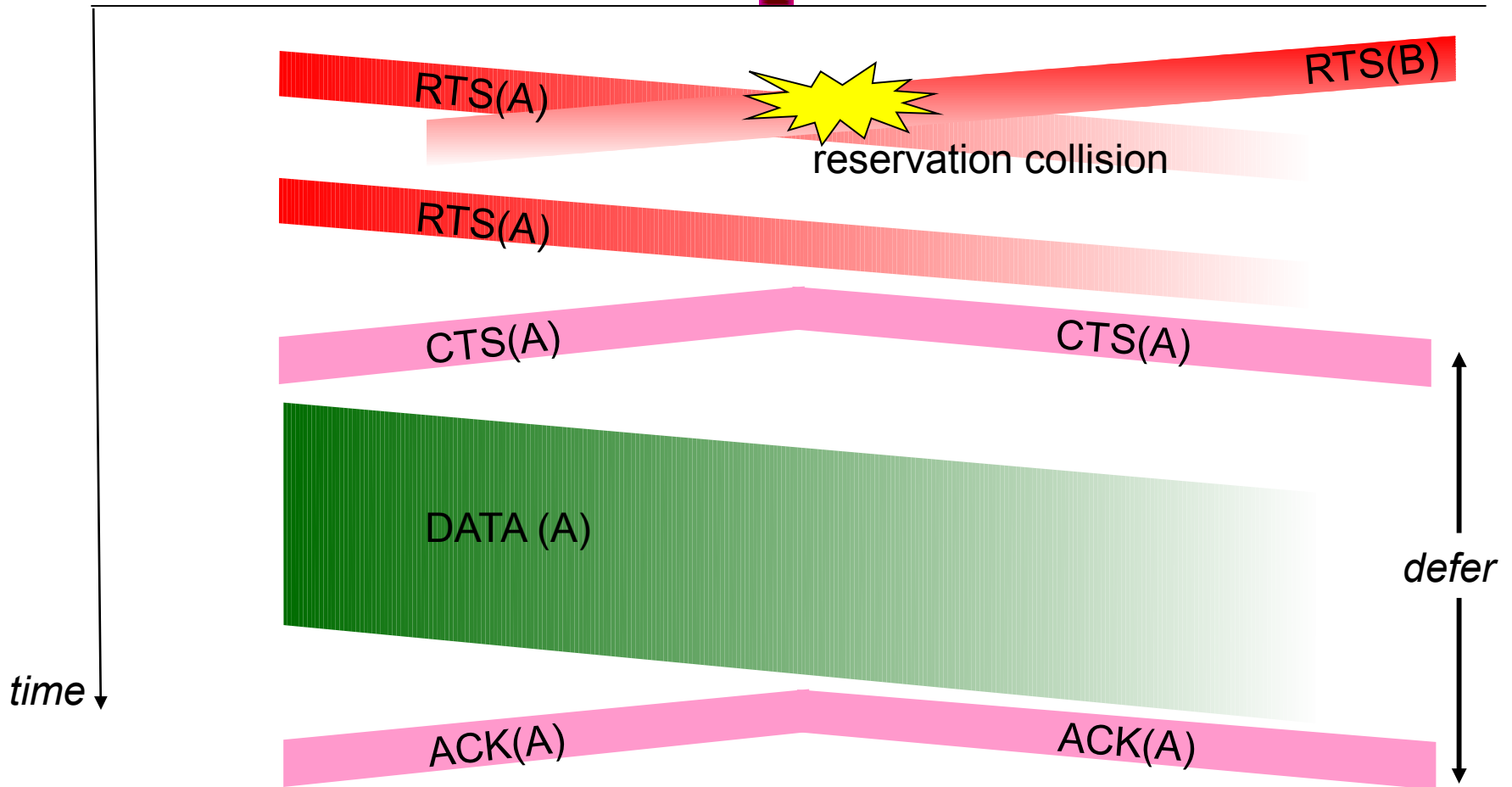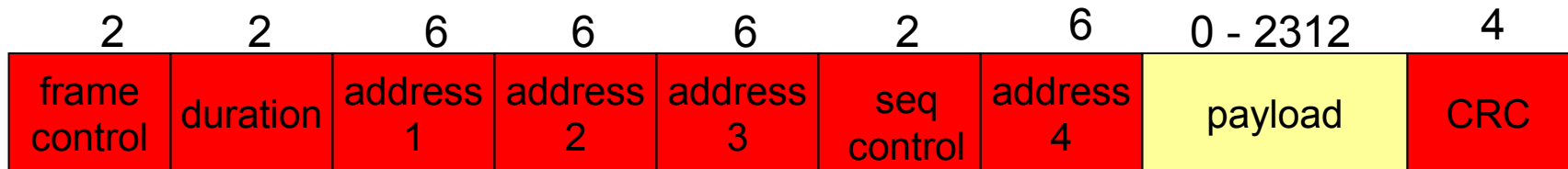
Address 1: MAC address of wireless host or AP to receive this frame

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

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

802.11 frame: addressing

Internet

H1

AP

R1 router

	R1 MAC addr	H1 MAC addr	
	dest. address	source address	

802.**3** frame

	AP MAC addr	H1 MAC addr	R1 MAC addr	
	address 1	address 2	address 3	

802.**11** frame

802.11 frame: more

duration of reserved transmission time (RTS/CTS)

frame seq # (for RDT)

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

Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

frame type (RTS, CTS, ACK, data)
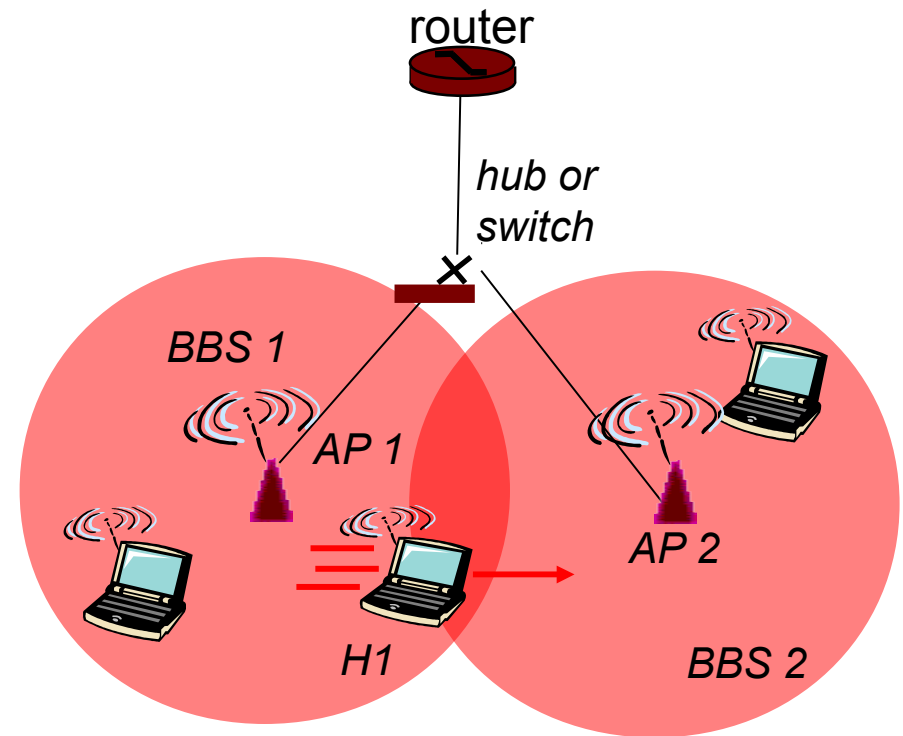
802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same

- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1

router

hub or switch

BBS 1

AP 1

AP 2

H1

BBS 2

802.11: advanced capabilities

Rate Adaptation

○ base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies


```
········· QAM256 (8 Mbps)
- - - - - QAM16 (4 Mbps)
━━━━━ BPSK (1 Mbps)
●        operating point
```
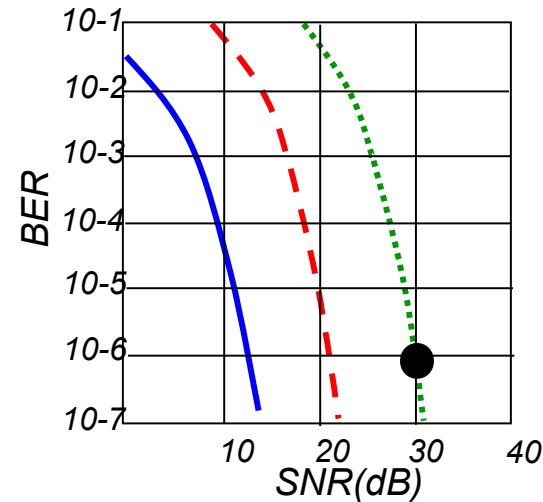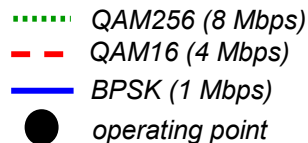
1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

802.11: advanced capabilities

○ Power Management

○ node-to-AP: "I am going to sleep until next beacon frame"

  ○ AP knows not to transmit frames to this node

  ○ node wakes up before next beacon frame

○ beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent

  ○ node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame
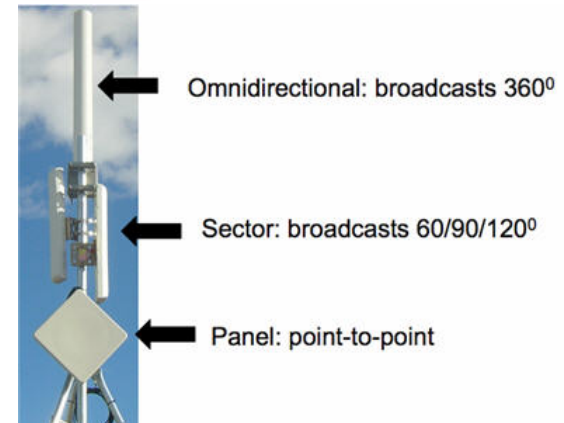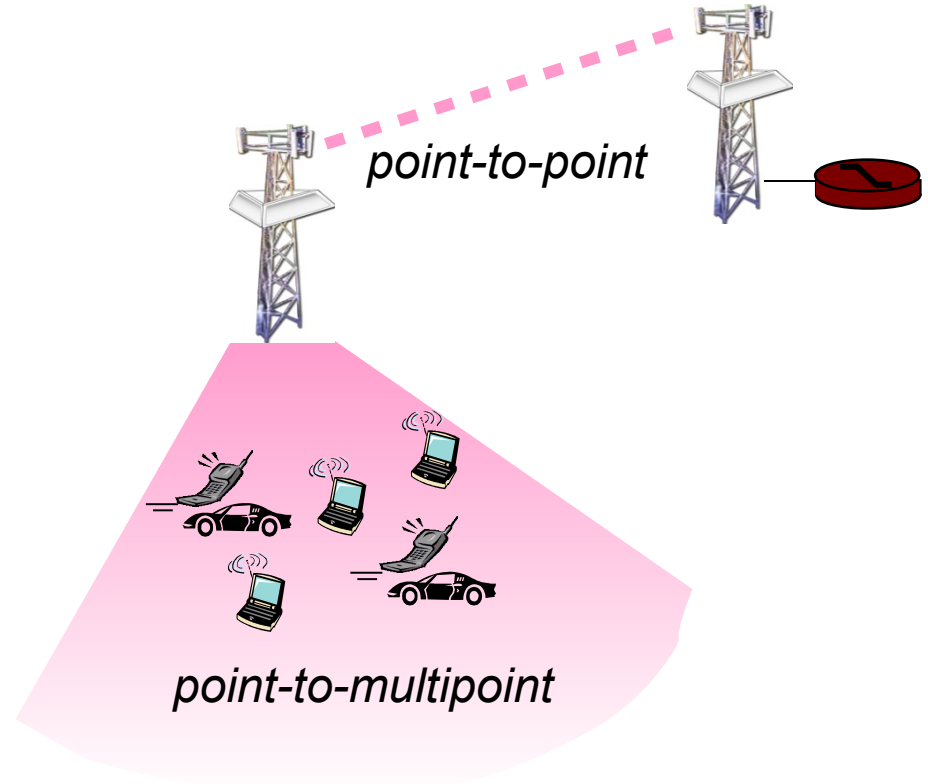
802.15: personal area network

○ less than 10 m diameter

○ replacement for cables (mouse, keyboard, headphones)

○ ad hoc: no infrastructure

○ master/slaves:
  ○ slaves request permission to send (to master)
  ○ master grants requests

○ 802.15: evolved from Bluetooth specification
  ○ 2.4-2.5 GHz radio band
  ○ up to 721 kbps
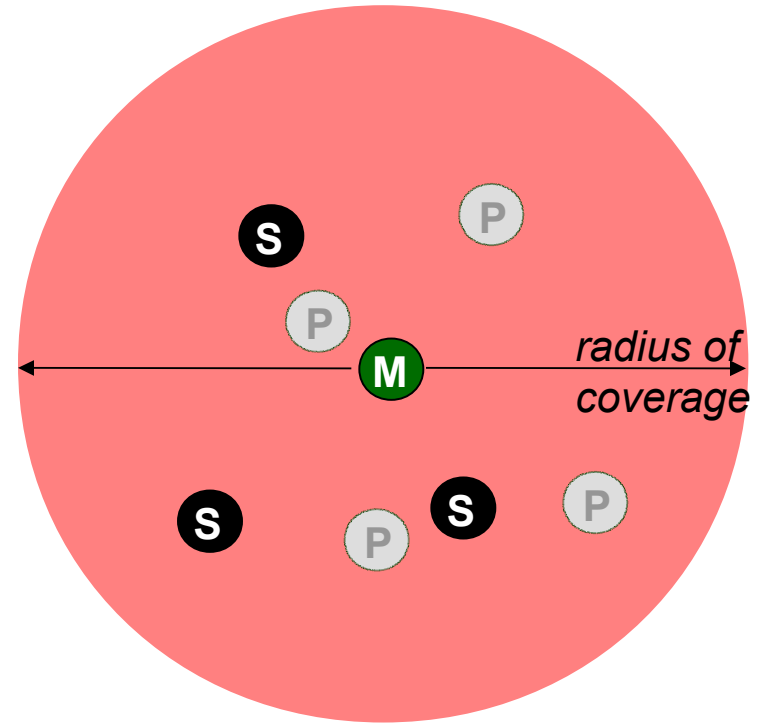
M Master device

S Slave device

P Parked device (inactive)

radius of coverage

802.16: WiMAX

- like 802.11 & cellular: 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")
  - ~14 Mbps

point-to-point

point-to-multipoint

Omnidirectional: broadcasts 360⁰

Sector: broadcasts 60/90/120⁰

Panel: point-to-point

Link Layer

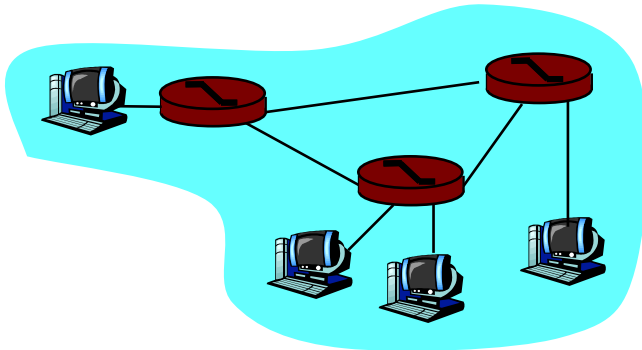# Virtualization of networks

Virtualization of resources: powerful abstraction in systems engineering:

- computing examples: virtual memory, virtual devices
    - Virtual machines: e.g., java
    - IBM VM os from 1960's/70's
- layering of abstractions: don't sweat the details of the lower layer, only deal with lower layers abstractly

The Internet: virtualizing networks
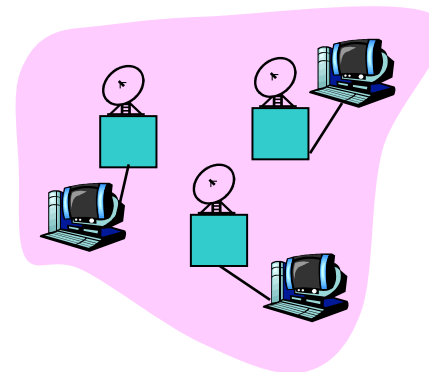
1974: multiple unconnected nets … differing in:

- ARPAnet
- data-over-cable networks
- packet satellite network (Aloha)
- packet radio network

- addressing conventions
- packet formats
- error recovery
- routing

ARPAnet

satellite net

"A Protocol for Packet Network Intercommunication",
V. Cerf, R. Kahn, IEEE Transactions on Communications,
May, 1974, pp. 637-648.

2: Data Link Layer

The Internet: virtualizing networks

Internetwork layer (IP):
- addressing: internetwork appears as single, uniform entity, despite underlying local network heterogeneity
- network of networks

Gateway:
- "embed internetwork packets in local packet format or extract them"
- route (at internetwork level) to next gateway

gateway

ARPAnet
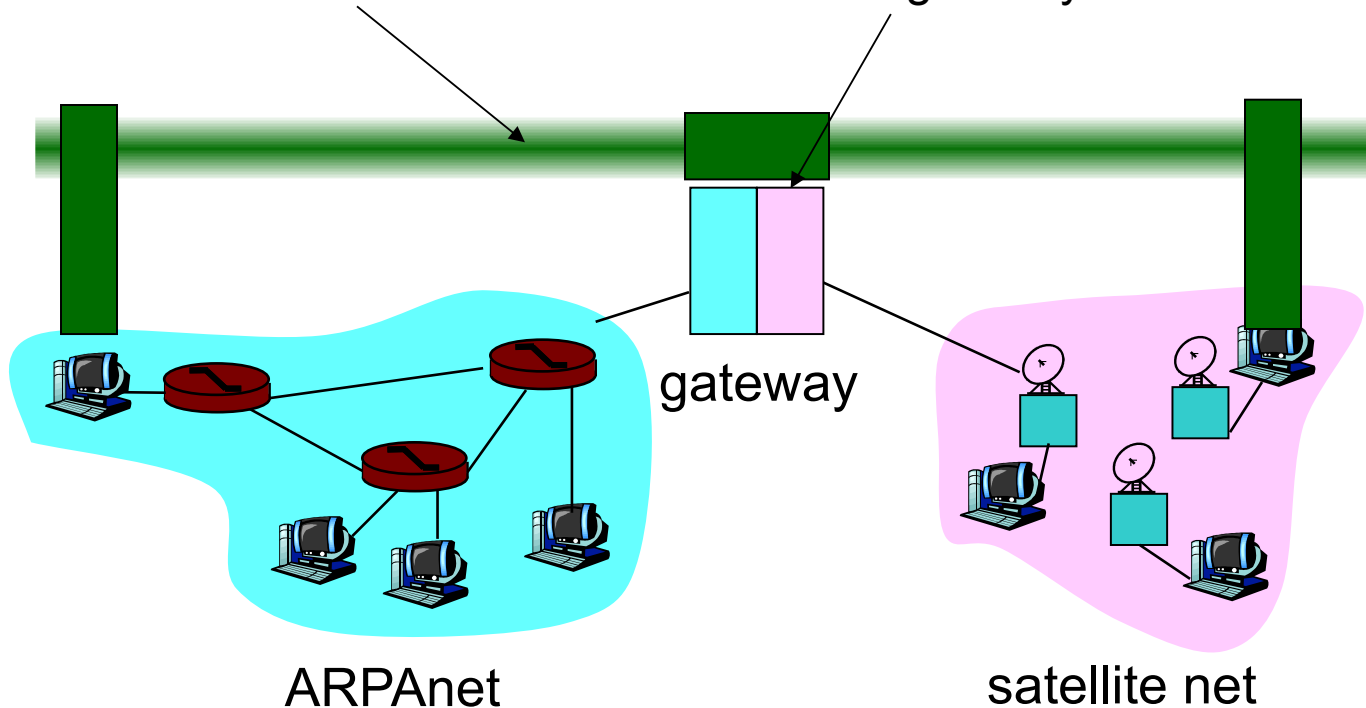
satellite net

Cerf & Kahn's Internetwork Architecture

What is virtualized?

○ two layers of addressing: internetwork and local network

○ new layer (IP) makes everything homogeneous at internetwork layer

○ underlying local network technology

  ○ cable

  ○ satellite

  ○ 56K telephone modem

  ○ today: MPLS (and ATM)

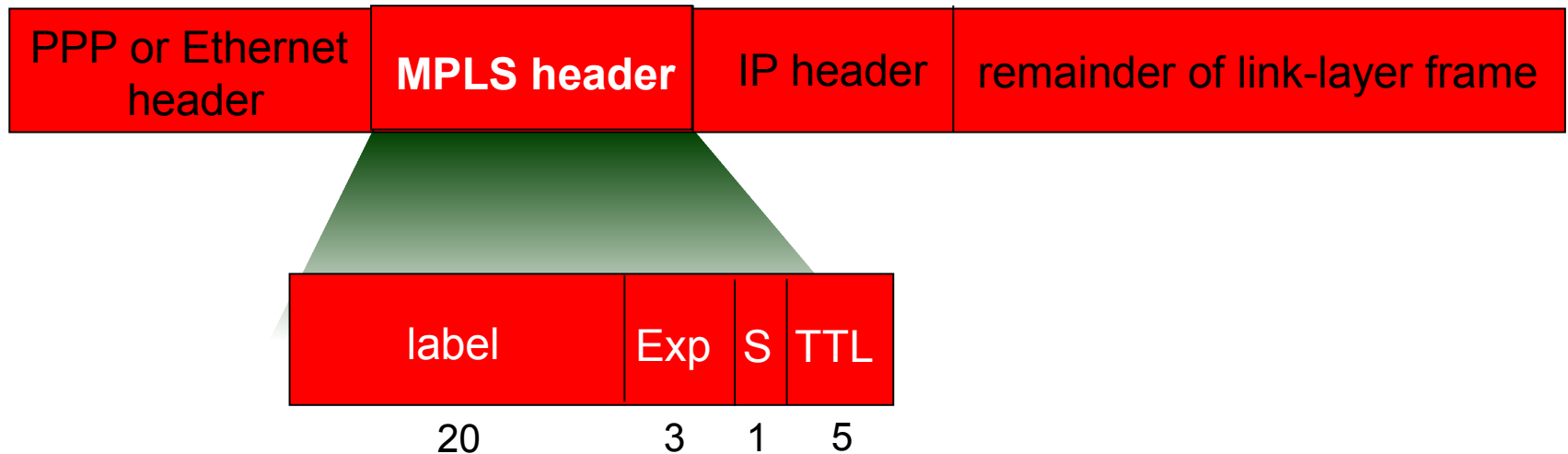 … "invisible" at internetwork layer. Looks like a link layer technology to IP!

MPLS and ATM

- MPLS and ATM separates networks in their own way
  - different service models, addressing, routing from Internet
- viewed by Internet as logical link connecting IP routers
  - just like dialup link is really part of separate network (telephone network)
- ATM – Asynchronous Transfer Mode
- MPLS – Multi-Protocol Label Switching

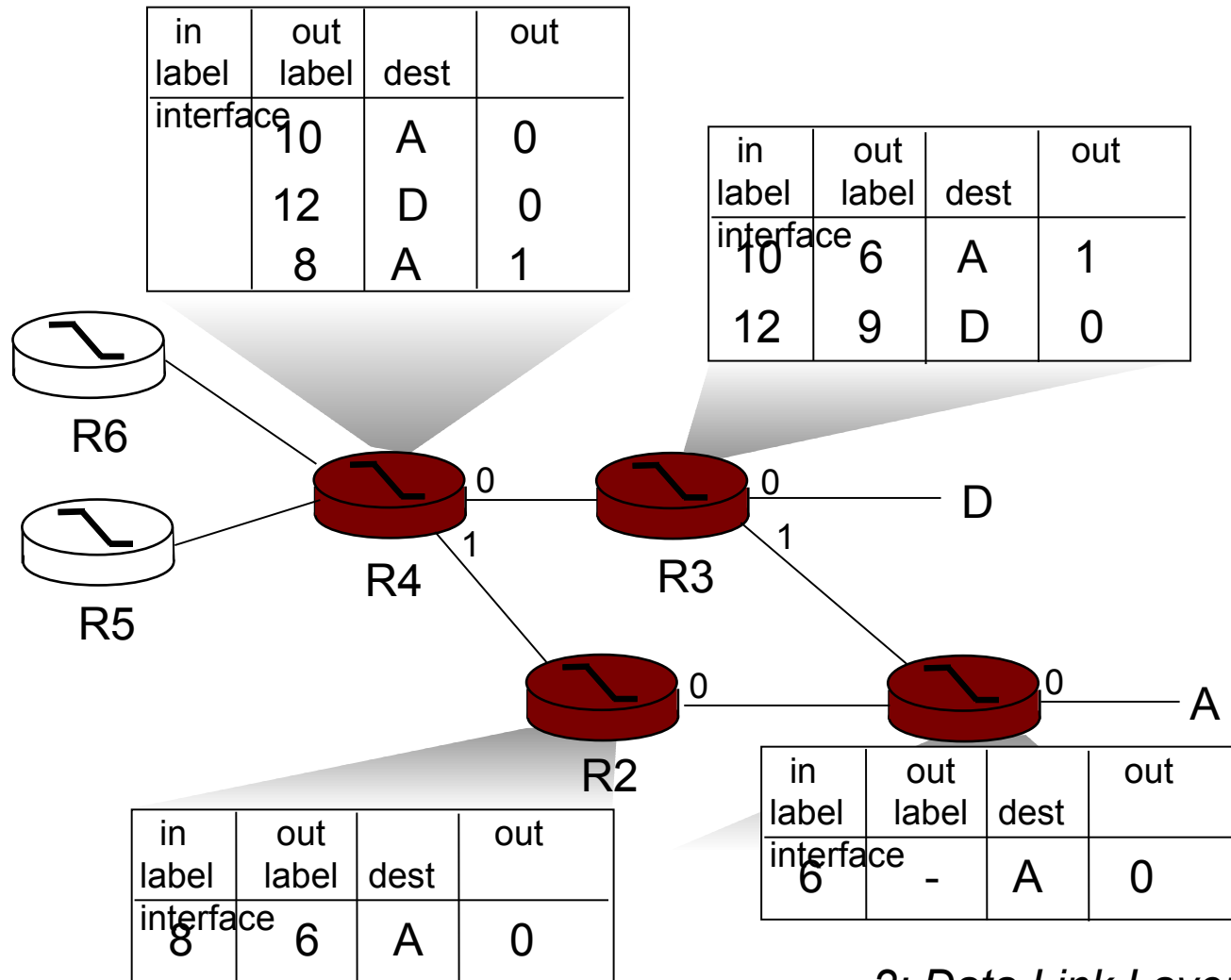# Multi-Protocol label switching (MPLS)

○ initial goal: speed up IP forwarding by using fixed length label (instead of IP address) to do forwarding

  ○ borrowing ideas from Virtual Circuit (VC) approach
  ○ but IP datagram still keeps IP address!

PPP or Ethernet header	MPLS header	IP header	remainder of link-layer frame

label	Exp	S	TTL
20	3	1	5

MPLS capable routers

○ a.k.a. label-switched router
○ forwards packets to outgoing interface based only on label value (don't inspect IP address)
  ○ MPLS forwarding table distinct from IP forwarding tables
○ signaling protocol needed to set up forwarding
  ○ RSVP-TE
  ○ forwarding possible along paths that IP alone would not allow (e.g., source-specific routing) !!
  ○ use MPLS for traffic engineering
○ must co-exist with IP-only routers

MPLS forwarding tables

in label interface	out label	dest	out
10	A	0	
12	D	0	
8	A	1	

in label interface	out label	dest	out
10	6	A	1
12	9	D	0

R6

R5

R4

0

R3

0 — D

1

1

R2

0 — A

0

in label interface	out label	dest	out
6	-	A	0

in label interface	out label	dest	out
8	6	A	0

Chapter 2: Summary

○ principles behind data link layer services:

   ○ error detection, correction

   ○ sharing a broadcast channel: multiple access

   ○ link layer addressing

○ instantiation and implementation of various link layer technologies

   ○ switched LANS

   ○ PPP

   ○ Wireless links

   ○ virtualized networks as a link layer: MPLS