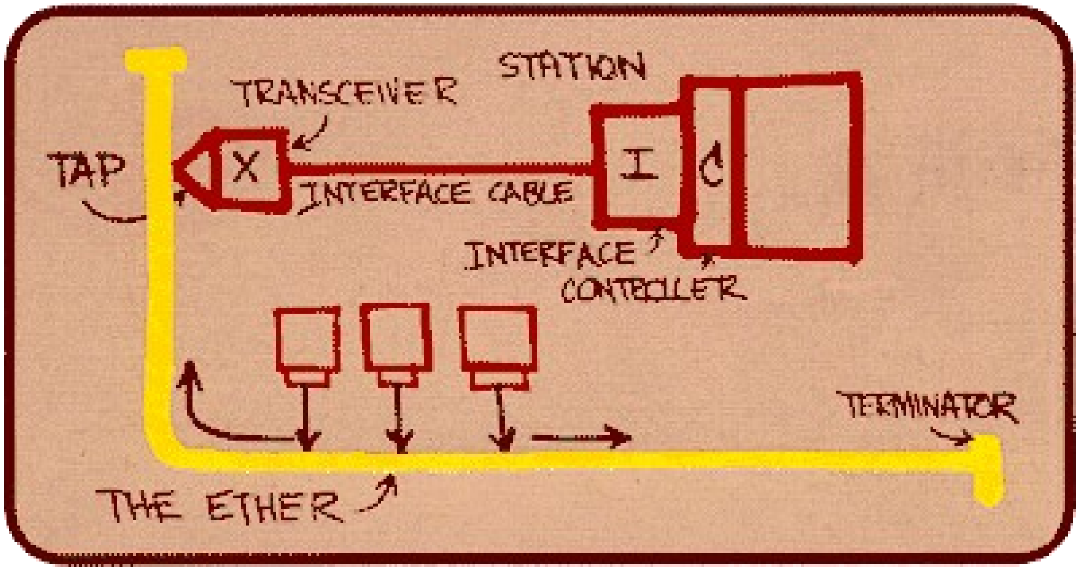
Ethernet

Dominant LAN technology:

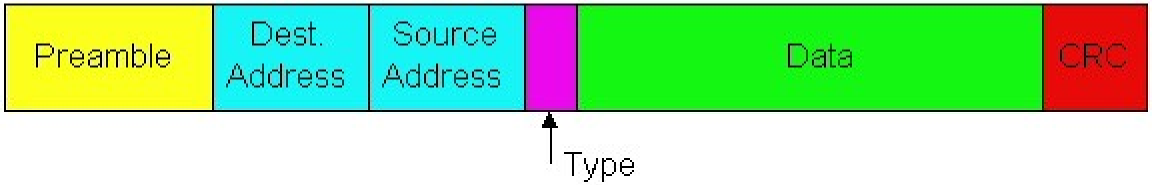
- cheap $$ for 100Mbs or even 1Gbps!
- first widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10, 100, 1000 Mbps



Metcalfe's Ethernet sketch

Ethernet Frame Structure

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

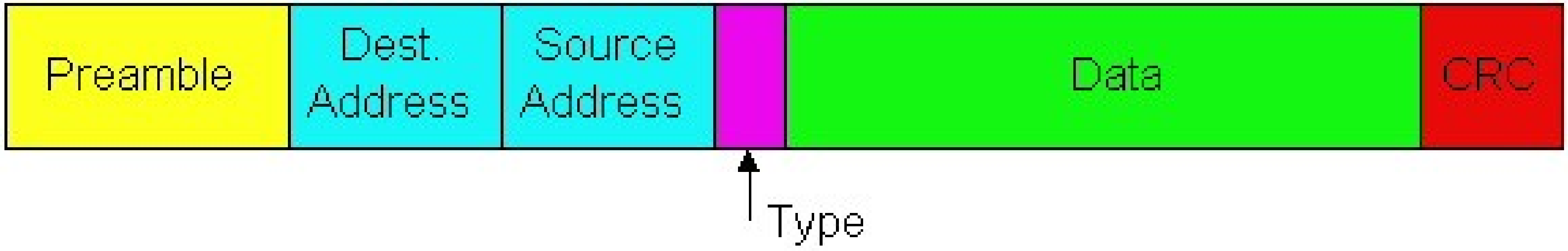


Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

Ethernet Frame Structure (more)

- Addresses: 6 bytes, frame is received by all adapters on a LAN and dropped if address does not match
- Type: indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: checked at receiver, if error is detected, the frame is simply dropped



Ethernet: Unreliable, connectionless

- connectionless: No handshaking between sending and receiving NICs
- unreliable: receiving NIC doesn't send acks or nacks to sending NIC
  - stream of datagrams passed to network layer can have gaps (missing datagrams)
  - gaps will be filled if app is using TCP
  - otherwise, app will see gaps
- Ethernet's MAC protocol: unslotted CSMA/CD

Ethernet: uses CSMA/CD

A: sense channel, **if** idle

then {

transmit and monitor the channel;

If detect another transmission

then {

abort and send jam signal;

update # collisions;

delay as required by exponential backoff algorithm;

goto A

}

else {done with the frame; set collisions to zero}

}

else {wait until ongoing transmission is over and goto A}

Ethernet's CSMA/CD (more)

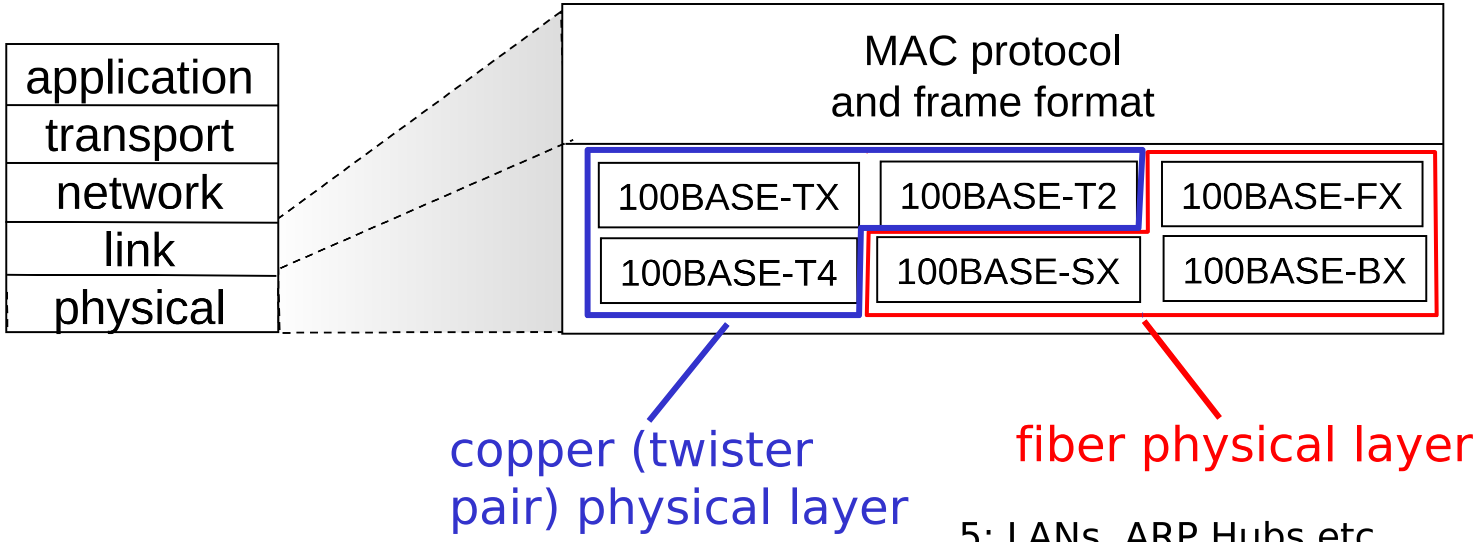
Jam Signal: make sure all other transmitters are aware of collision; 48 bits;

Exponential Backoff:

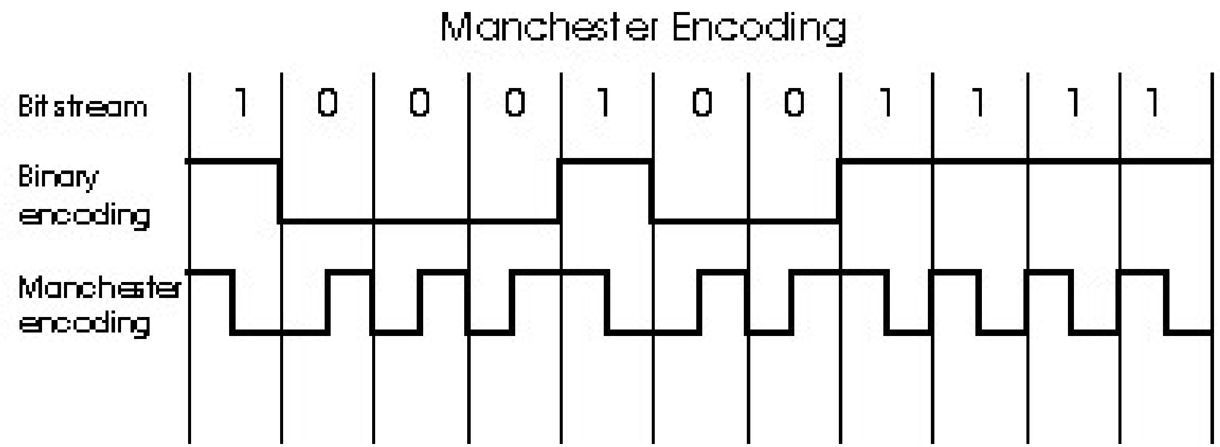
- *Goal*: adapt retransmission attempts to estimated current load
  - heavy load: random wait will be longer
- first collision: choose K from {0,1}; delay is K x 512 bit transmission times
- after second collision: choose K from {0,1,2,3}
  …
- after ten or more collisions, choose K from {0,1,2,3,4,…,1023}

802.3 Ethernet Standards: Link & Physical Layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10G bps
  - different physical layer media: fiber, cable



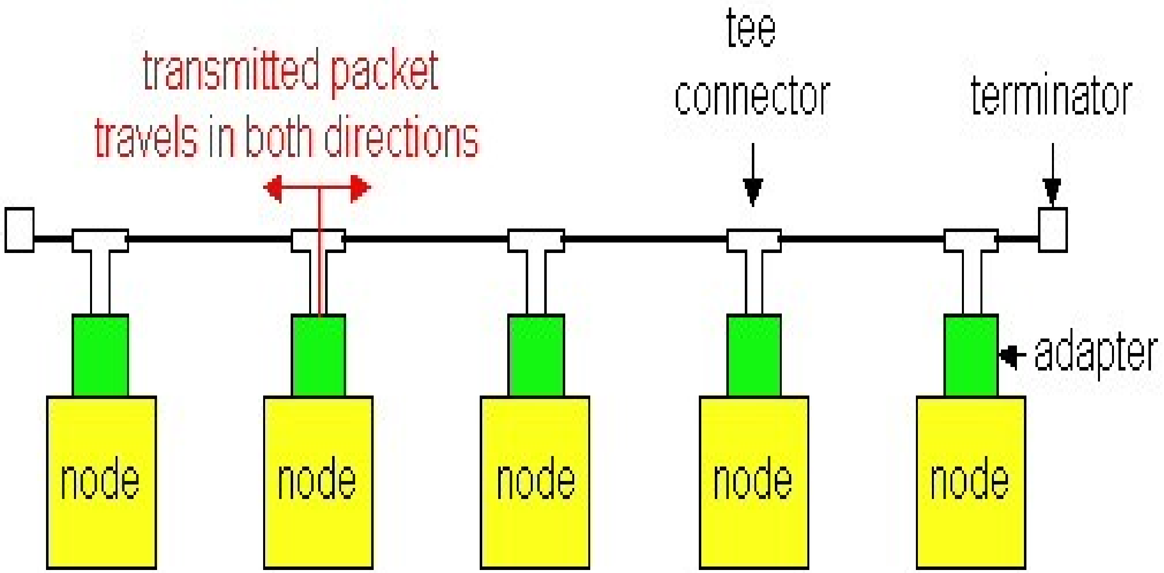
Manchester encoding



- used in 10BaseT
- each bit has a transition
- allows clocks in sending and receiving nodes to synchronize to each other
  - no need for a centralized, global clock among nodes!
- Hey, this is physical-layer stuff!

Ethernet Technologies: 10Base2

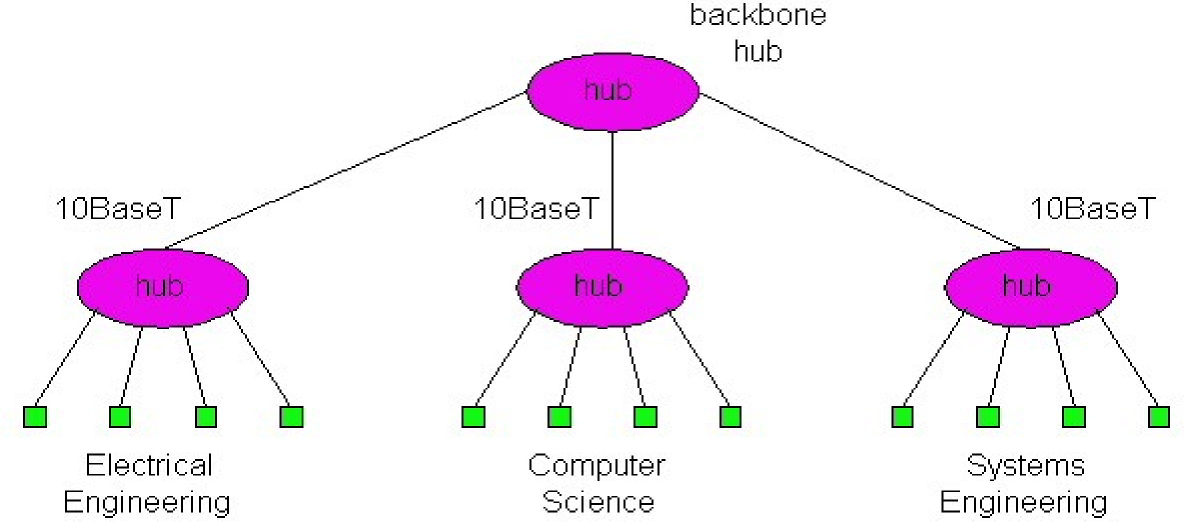
- 10: 10Mbps; 2: under 200 meters max cable length
- thin coaxial cable in a bus topology



- repeaters used to connect up to multiple segments
- repeater repeats bits it hears on one interface to its other interfaces: physical layer device only!

10BaseT and 100BaseT

- 10/100 Mbps rate; latter called "fast ethernet"
- T stands for Twisted Pair
- Hub to which nodes are connected by twisted pair, thus "star topology"
- CSMA/CD implemented at hub



10BaseT and 100BaseT (more)

- Max distance from node to Hub is 100 meters
- Hub can disconnect jabbering adapter
- Hub can gather monitoring information, statistics for display to LAN administrators

Gbit Ethernet

- use standard Ethernet frame format
- allows for point-to-point links and shared broadcast channels
- in shared mode, CSMA/CD is used; short distances between nodes to be efficient
- uses hubs, called here ''Buffered Distributors''
- Full-Duplex at 1 Gbps for point-to-point links

Token Passing: IEEE802.5 standard

- 4 Mbps
- max token holding time: 10 ms, limiting frame

- SD, ED mark start, end of packet
- AC: access control byte:
  - token bit: value 0 means token can be seized, value 1 means data follows FC
  - priority bits: priority of packet
  - reservation bits: station can write these bits to prevent stations with lower priority packet from seizing token after token becomes free

Token Passing: IEEE802.5 standard

- FC: frame control used for monitoring and maintenance
- source, destination address: 48 bit physical address, as in Ethernet
- data: packet from network layer
- checksum: CRC
- FS: frame status: set by dest., read by sender
  - set to indicate destination up, frame copied OK from ring
  - DLC-level ACKing

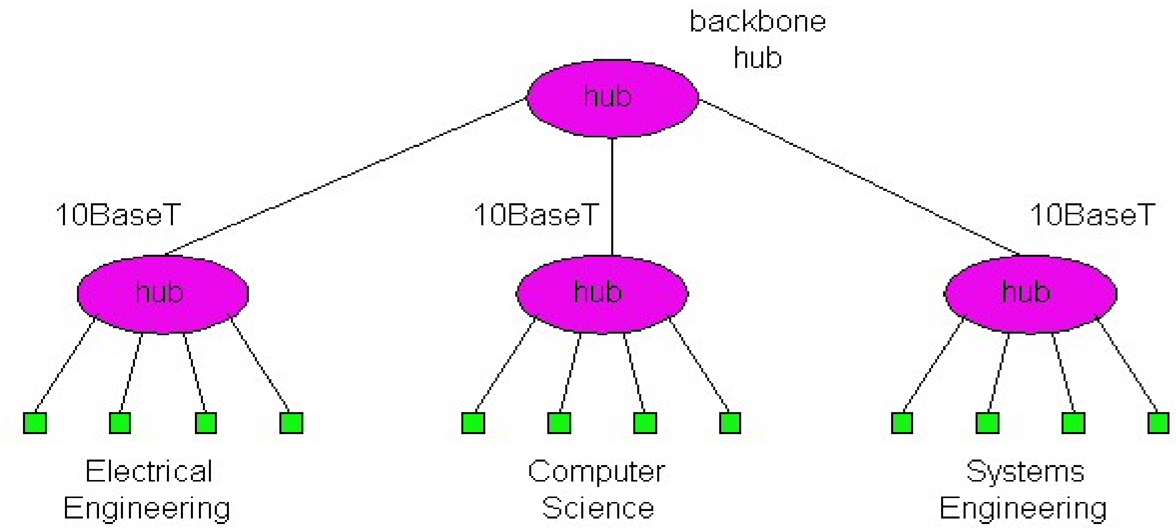
Interconnecting LANs

Q: Why not just one big LAN?

- Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
- limited length: 802.3 specifies maximum cable length
- Large ''collision domain'' (can collide with many stations)
- limited number of stations: 802.5 have token passing delays at each station

Hubs

- Physical Layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or multi-tier design), with backbone hub at its top



Hubs (more)

- Each connected LAN referred to as LAN **segment**
- Hubs do not isolate collision domains: node may collide with any node residing at any segment in LAN
- Hub Advantages:
  - simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one hub malfunctions
  - extends maximum distance between node pairs (100m per Hub)

Hub limitations

- single collision domain results in no increase in max throughput
  - multi-tier throughput same as single segment throughput
- individual LAN restrictions pose limits on number of nodes in same collision domain and on total allowed geographical coverage
- cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)

Bridges

- Link Layer devices: operate on Ethernet frames, examining frame header and selectively forwarding frame based on its destination
- Bridge isolates collision domains since it buffers frames
- When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit

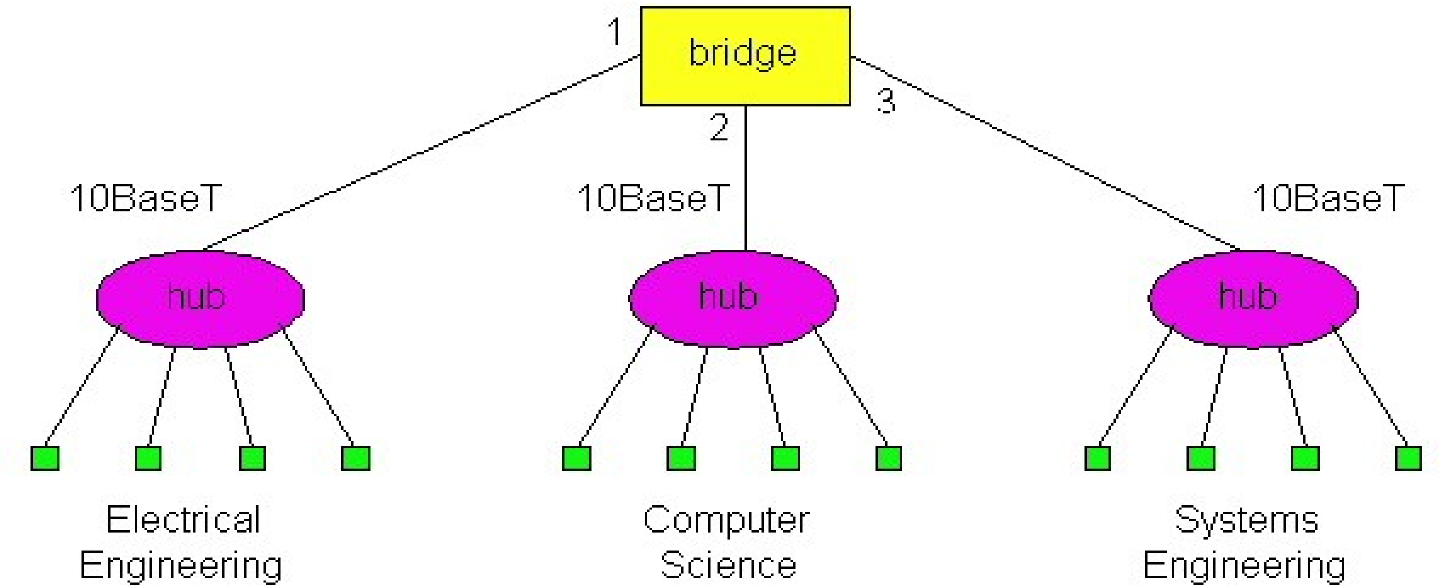
Bridges (more)

- Bridge advantages:
  - Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage
  - Can connect different type Ethernet since it is a store and forward device
  - Transparent: no need for any change to hosts LAN adapters

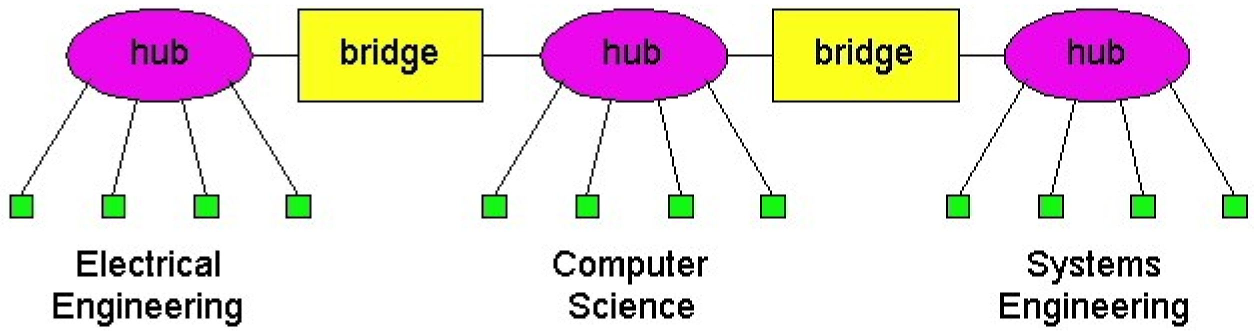
Bridges: frame filtering, forwarding

- bridges filter packets
  - same-LAN -segment frames not forwarded onto other LAN segments
- forwarding:
  - how to know which LAN segment on which to forward frame?
  - looks like a routing problem (more shortly!)

Backbone Bridge



Interconnection Without Backbone



- Not recommended for two reasons:
  - single point of failure at Computer Science hub
  - all traffic between EE and SE must path over CS segment

Bridge Filtering

- bridges *learn* which hosts can be reached through which interfaces: maintain filtering tables
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender location in filtering table
- filtering table entry:
  - (Node LAN Address, Bridge Interface, Time Stamp)
  - stale entries in Filtering Table dropped (TTL can be 60 minutes)

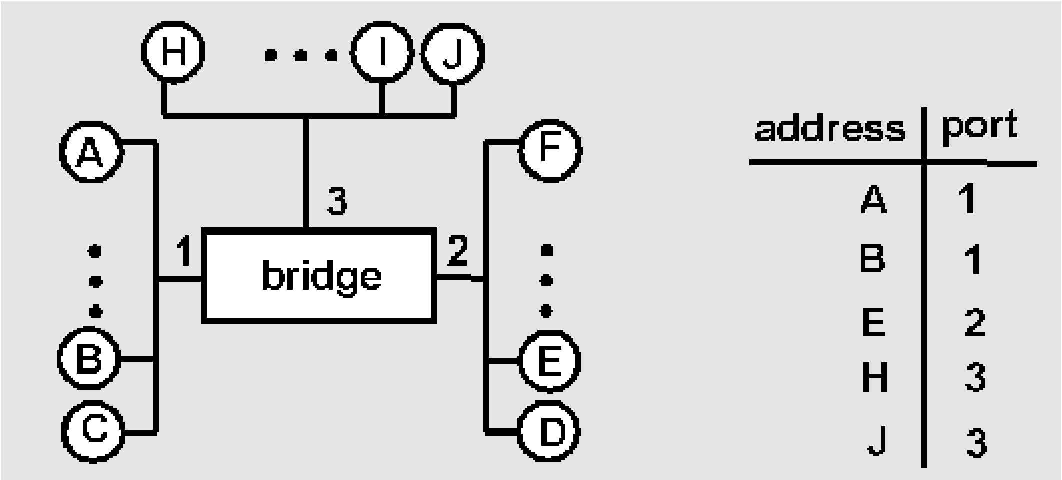
Bridge Filtering

- filering procedure:

```
if destination is on LAN on which frame was received
    then drop the frame
    else { lookup filtering table
           if entry found for destination
            then forward the frame on interface
              indicated;
            else flood;    /* forward on all but the
              interface on                          which the
              frame arrived*/
         }
```

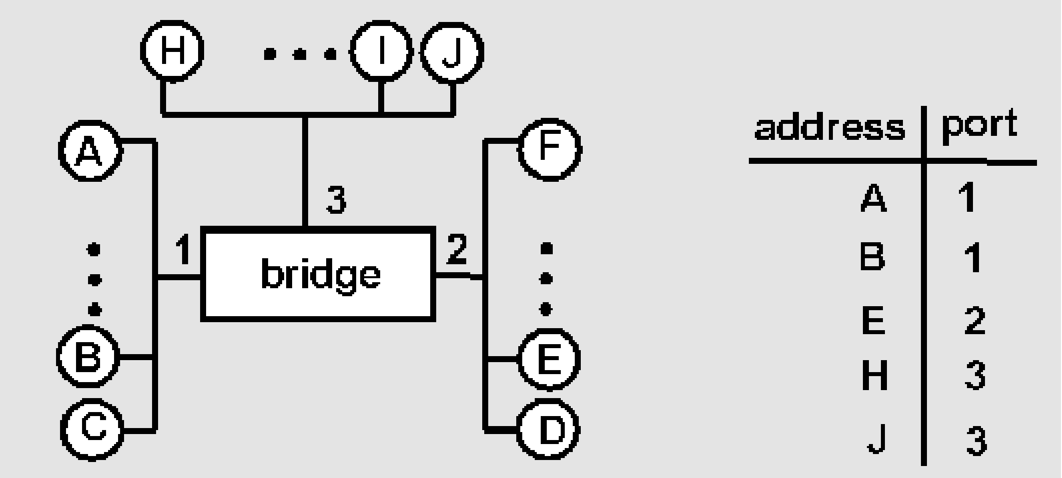
Bridge Learning: example

Suppose C sends frame to D and D replies back with frame to C



- C sends frame, bridge has no info about D, so floods to both LANs
  - bridge notes that C is on port 1
  - frame ignored on upper LAN
  - frame received by D

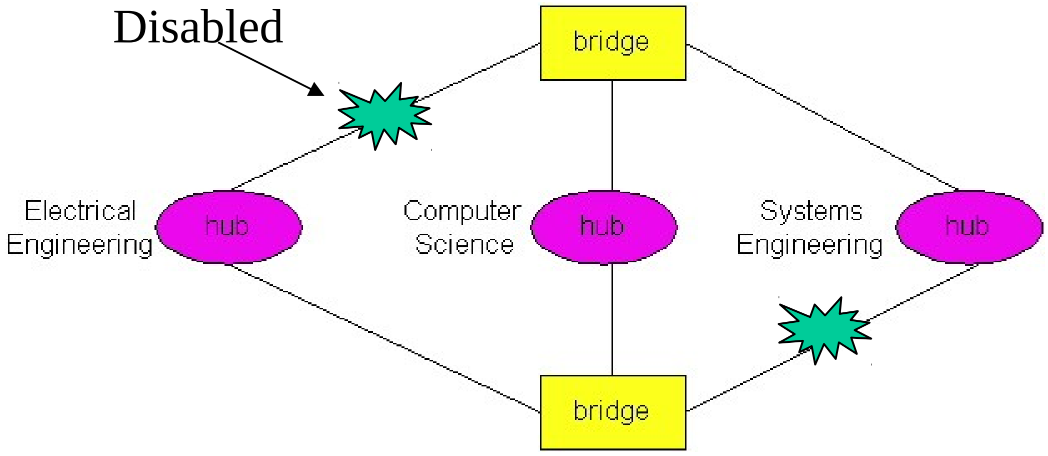
Bridge Learning: example



- D generates reply to C, sends
  - bridge sees frame from D
  - bridge notes that D is on interface 2
  - bridge knows C on interface 1, so *selectively* forwards frame out via interface 1

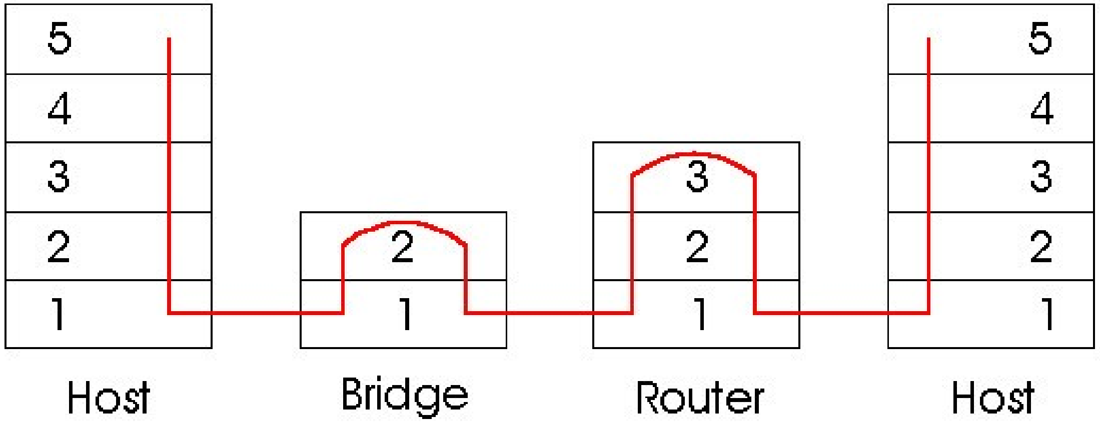
Bridges Spanning Tree

- for increased reliability, desirable to have redundant, alternate paths from source to dest
- with multiple simultaneous paths, cycles result - bridges may multiply and forward frame forever
- solution: organize bridges in a spanning tree by disabling subset of interfaces



WWF Bridges vs. Routers

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are Link Layer devices
- routers maintain routing tables, implement routing algorithms
- bridges maintain filtering tables, implement filtering, learning and spanning tree algorithms



Routers vs. Bridges

Bridges + and -

+ Bridge operation is simpler requiring less processing bandwidth
- Topologies are restricted with bridges: a spanning tree must be built to avoid cycles
- Bridges do not offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge)

Routers vs. Bridges

Routers + and -

+ arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)

+ provide firewall protection against broadcast storms

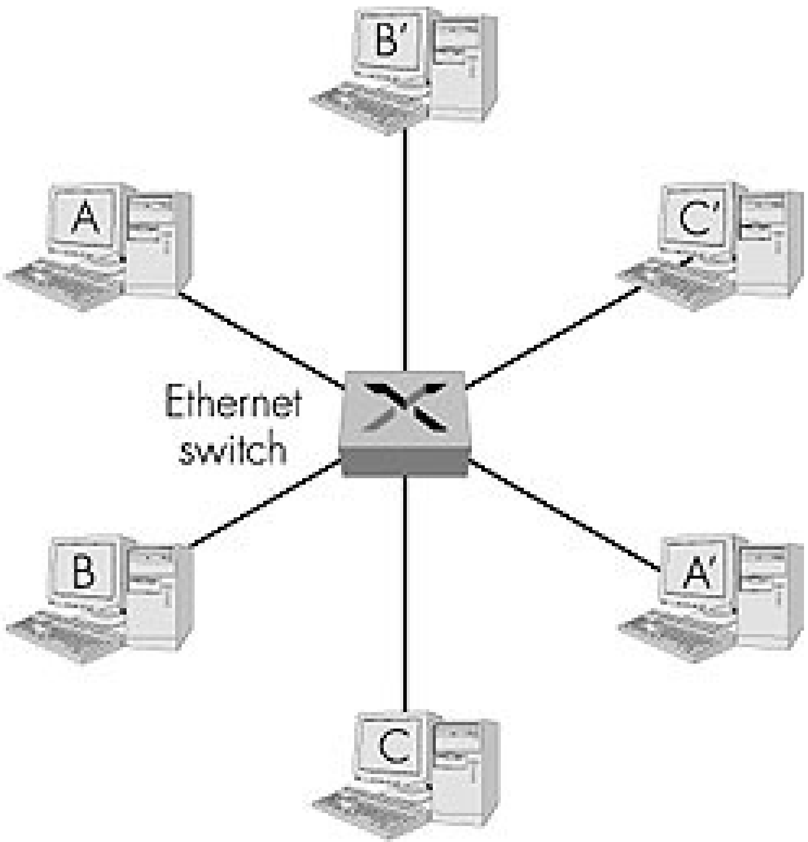
- require IP address configuration (not plug and play)

- require higher processing bandwidth

- bridges do well in small (few hundred hosts) while routers used in large networks (thousands of hosts)

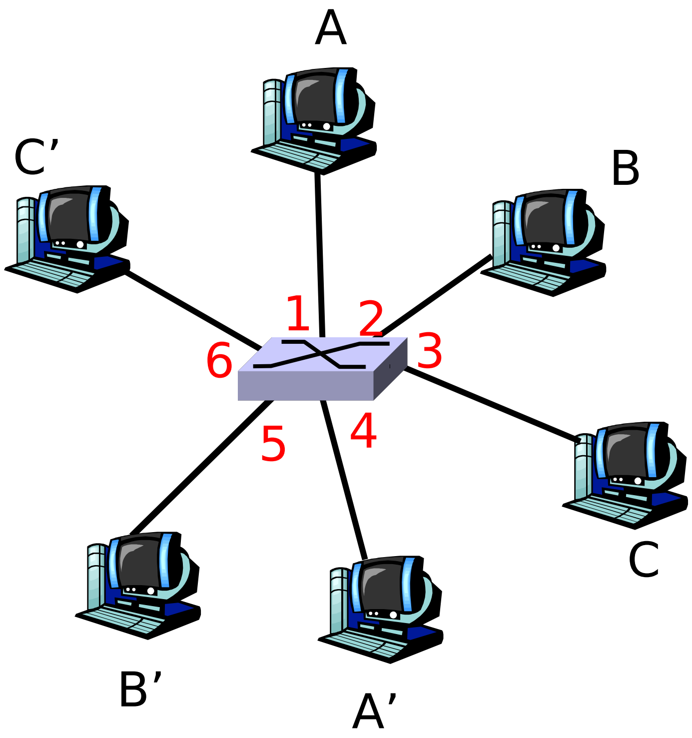
Ethernet Switches

- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-B and A'-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!



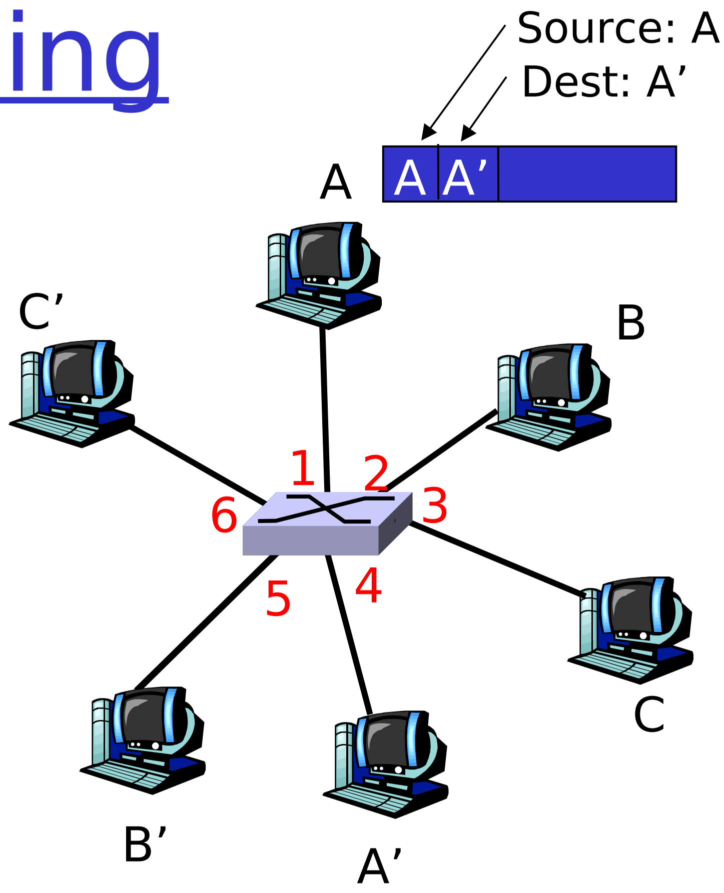
Switch Table

- *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



- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table

MAC addr	interface	TTL
A	*1*	*60*

Switch table (initially empty)

Switch: frame filtering/forwarding

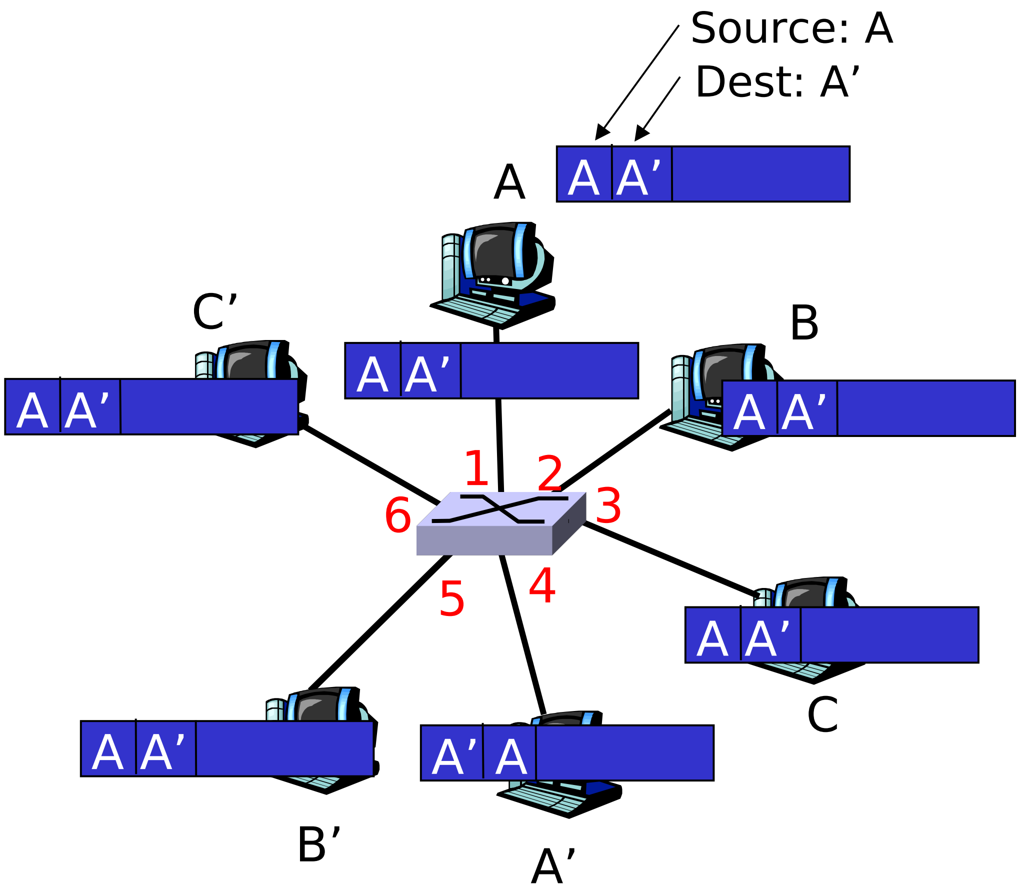
When frame received:

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*

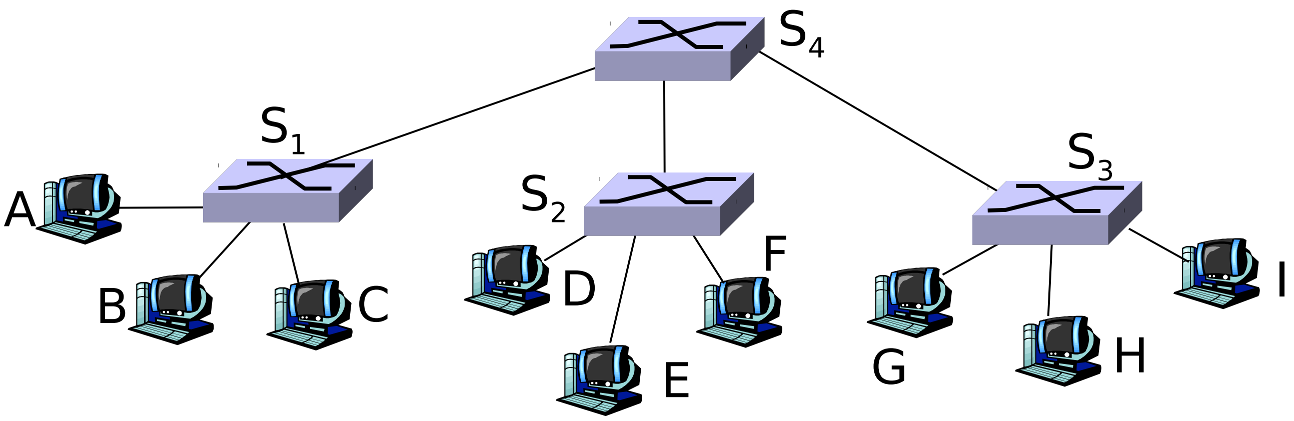


MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

Switch table (initially empty)

Interconnecting switches

- switches can be connected together

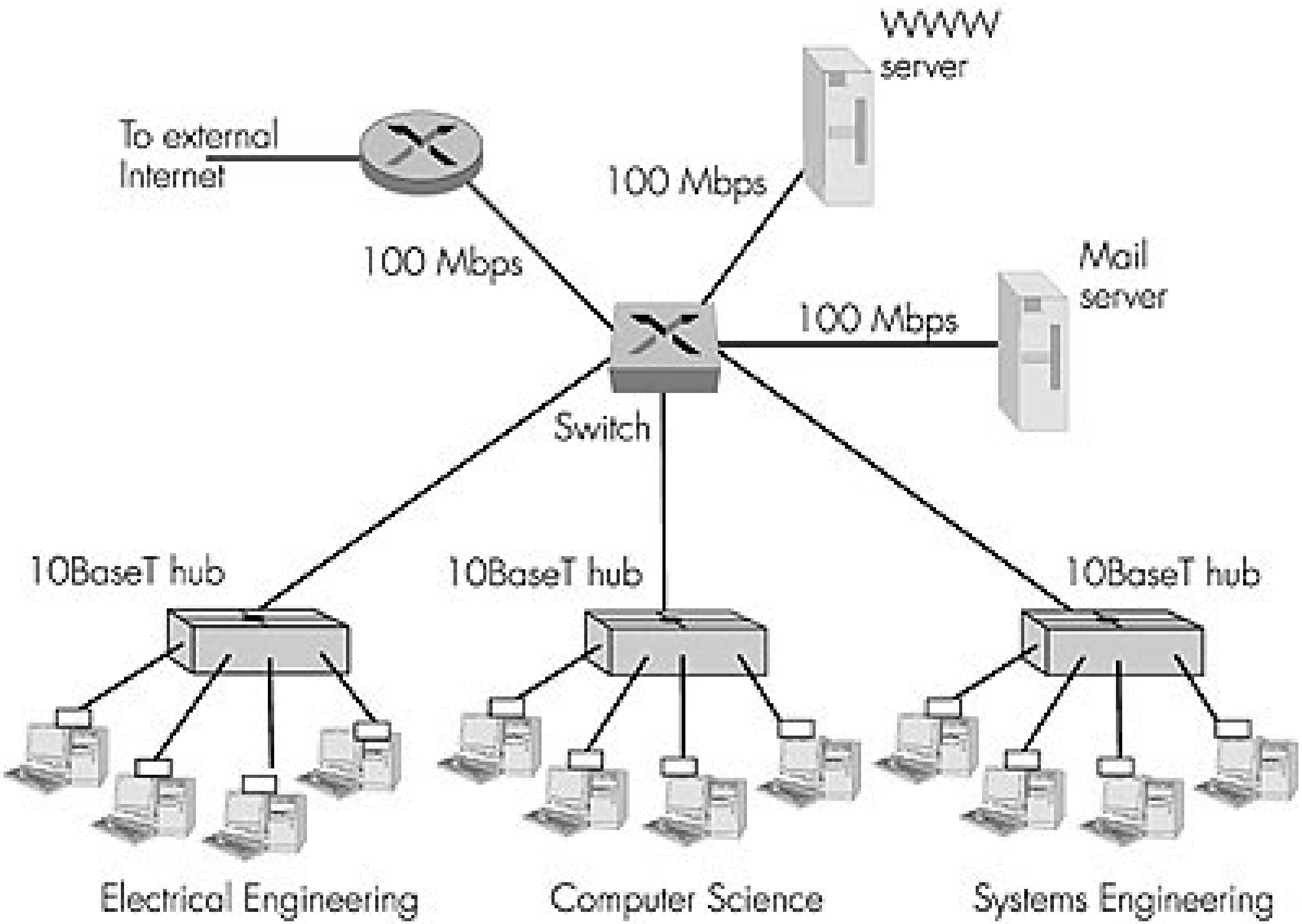


- *Q:* sending from A to G - how does S_1 know to forward frame destined to F via S_4 and S_3?
- *A:* self learning! (works exactly the same as in single-switch case!)

Ethernet Switches

- cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- combinations of shared/dedicated, 10/100/1000 Mbps interfaces

Ethernet Switches (more)



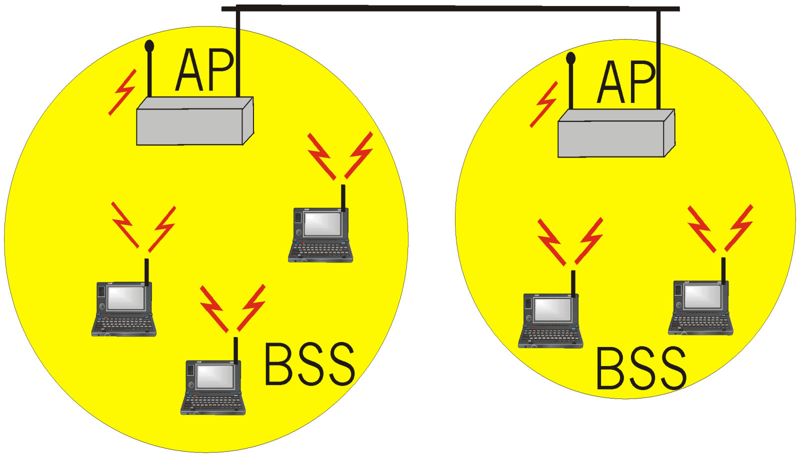
Wireless LANs

(chapter 6 on the new edition)

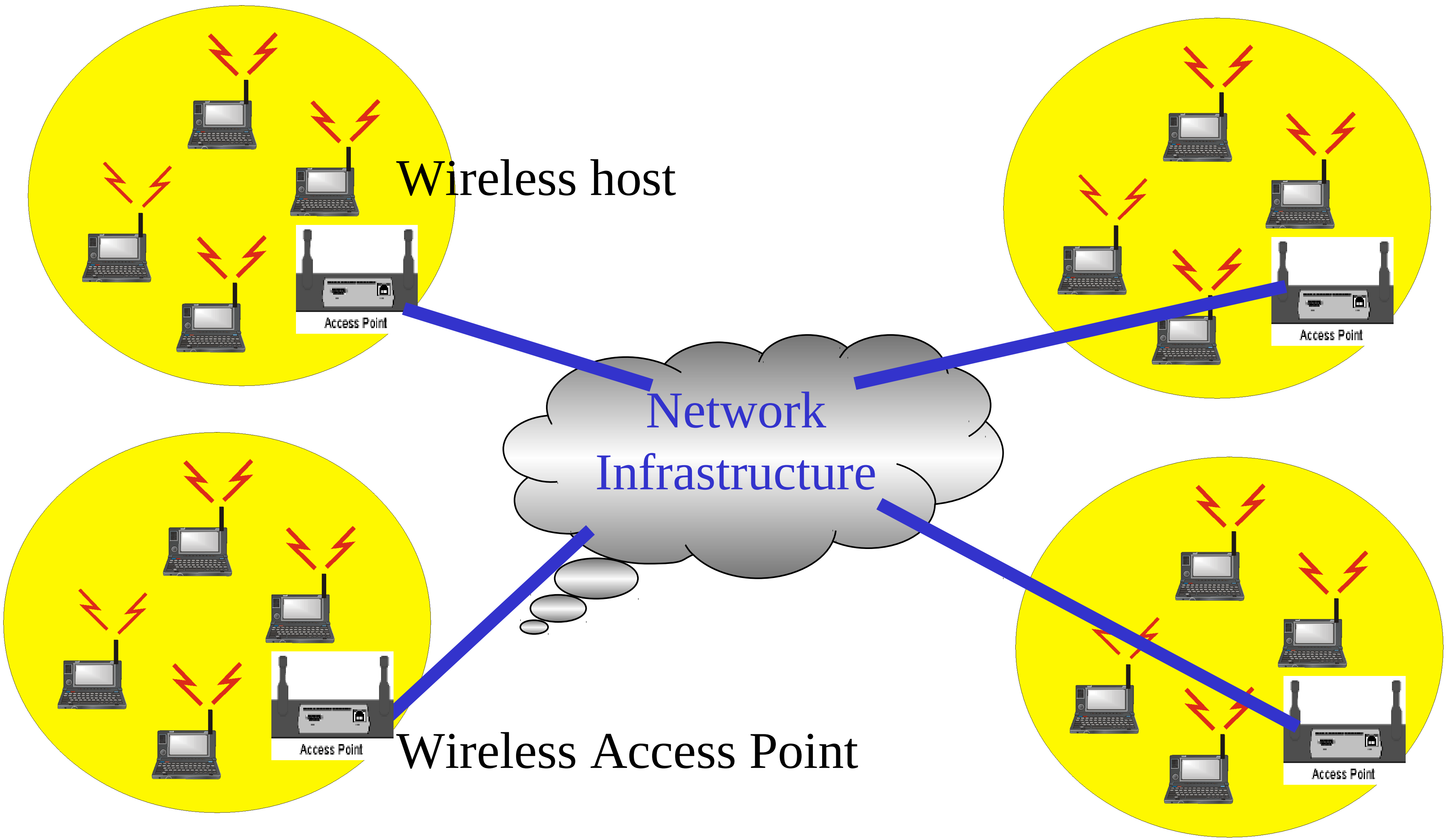
IEEE 802.11 Wireless LAN

- IEEE 802.11 standard:
  - MAC protocol
  - unlicensed frequency spectrum: 900Mhz, 2.4Ghz

- **Basic Service Set (BSS) (a.k.a. cell) contains:**
  - **wireless hosts**
  - **access point (AP): base station**
- **BSS's combined to form distribution system (DS)**

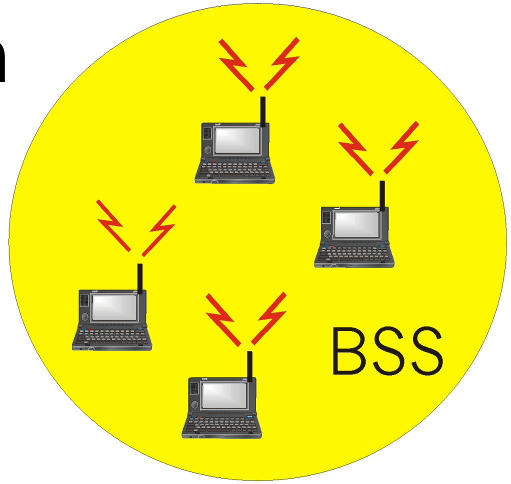


Wireless LANs



Ad Hoc Networks

- Ad hoc network: IEEE 802.11 stations can dynamically form network *without* AP. (Ad Hoc means “for this(purpose)”)
- Applications:
  - laptop meeting in conference room, car
  - interconnection of person
  - battlefield
- IETF (Internet Engineering Task Force)
- MANET (Mobile Ad hoc Networks) working group



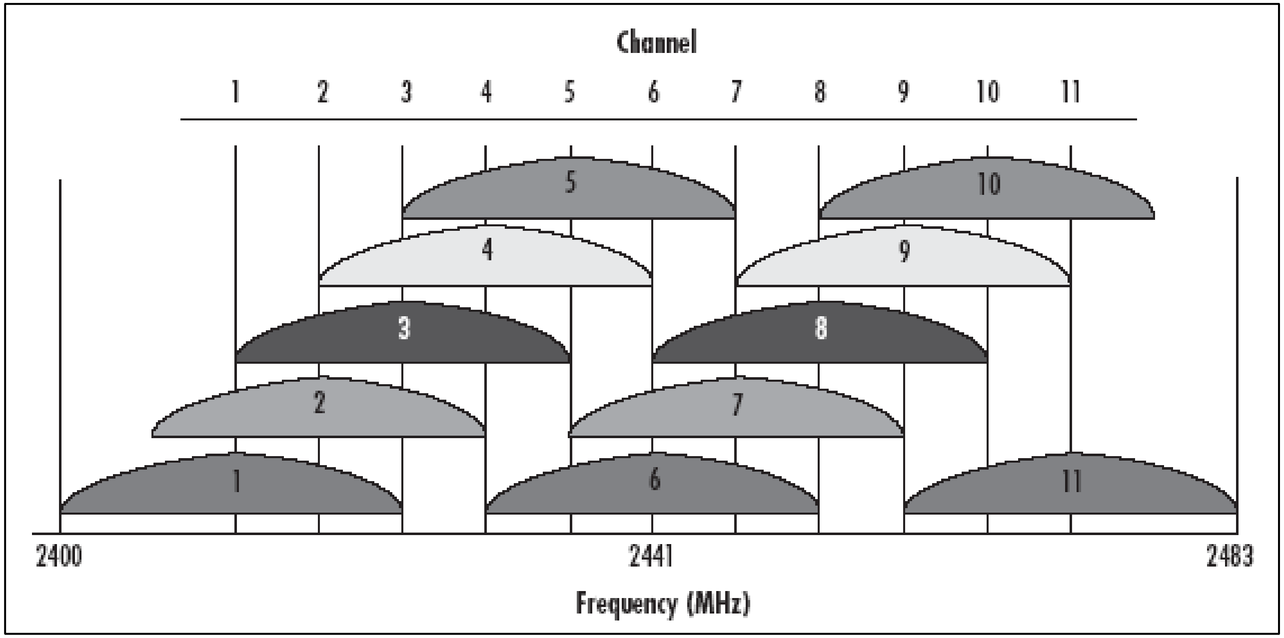
IEEE 802.11 Wireless LAN

- 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

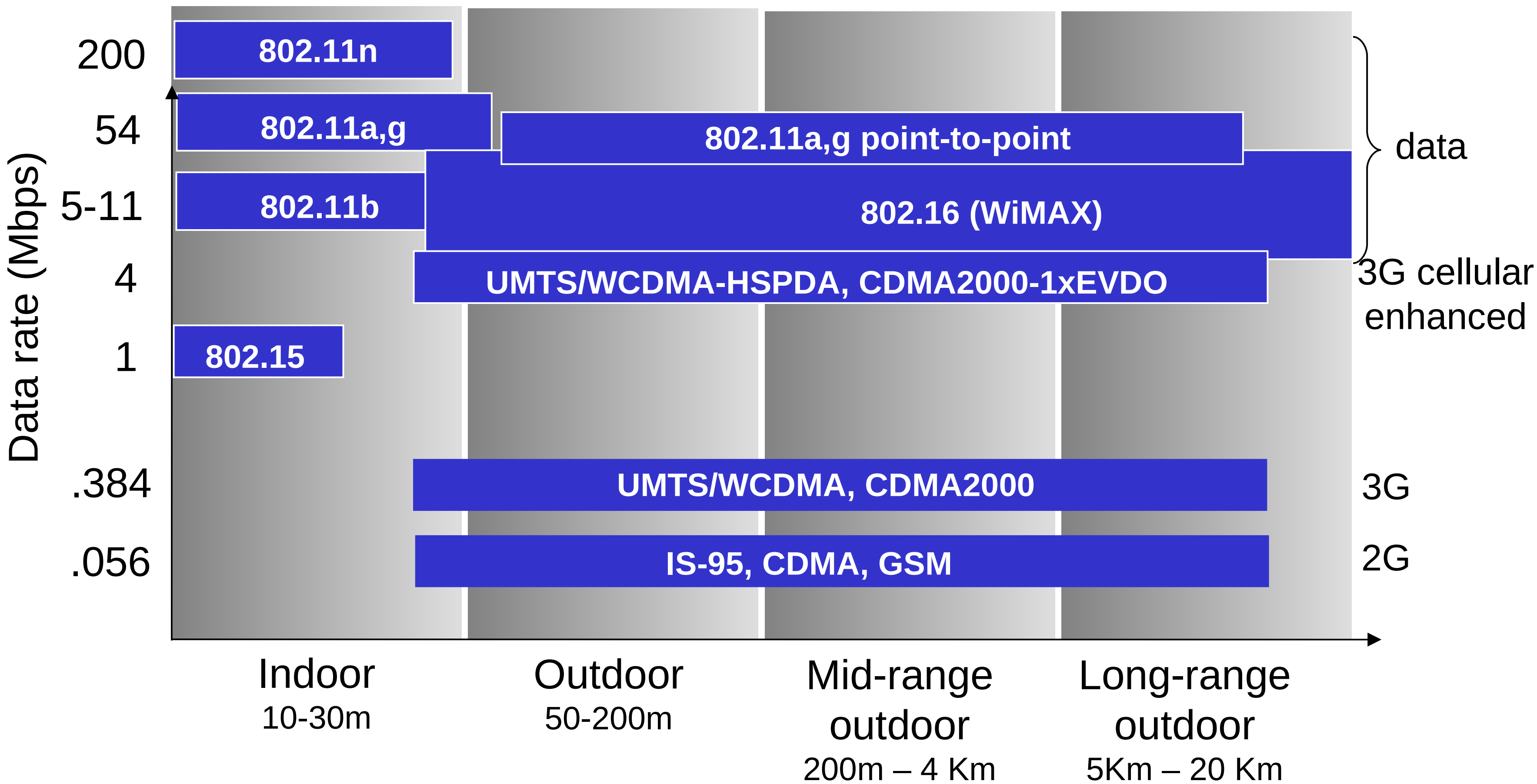
- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

Frequencies for IEEE wireless LANs

- Channels for IEEE 802.11b

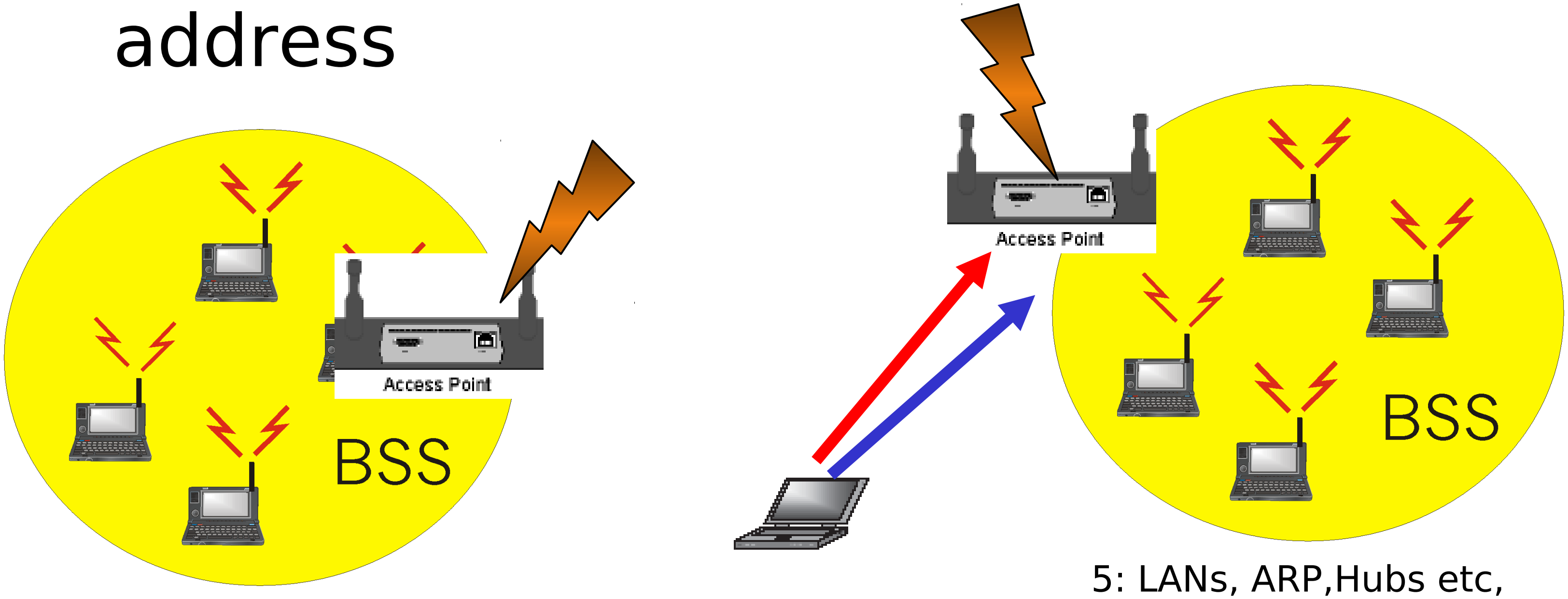


Characteristics of selected wireless link standards



Connecting to AP

- How does an incoming station connects to AP?
- One AP is selected, host dialogues with AP using 802.11 association protocol.
- DHCP discovery message-> gets an IP address



Considerations

- Radio signal passing through walls
- Signal in free space – disperses
- Microwave
- Nearby motors etc
- 2.4 GHz wireless phones
- Same frequency: 802.11b wireless LANs

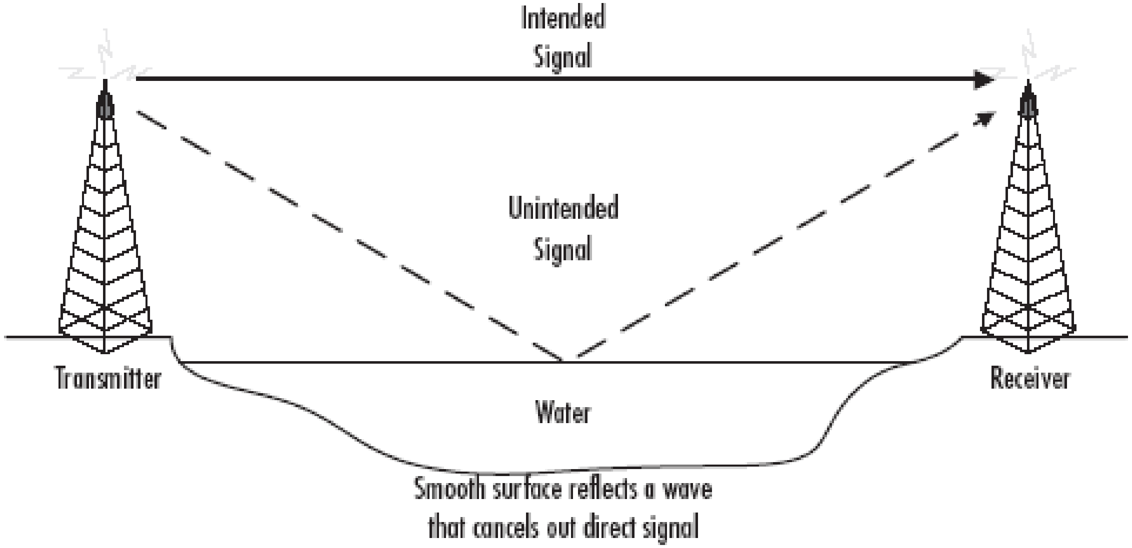
Wireless Link Characteristics (1)

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”

Considerations



- Reflected signals can be problem...

Considerations

- Security: authentication (either via MAC address or user/passwd is used, but not very strong.
- Initially no encryption was provided for wireless LANs, not even for the AP beacon
  - We now know that this is poor implementation…

IEEE 802.11 MAC Protocol: CSMA/CA

802.11 CSMA: sender

- if sense channel idle for **DISF** (Distrib. Inter Frame Space) seconds.

  then transmit entire frame (no collision detection)

-if sense channel busy

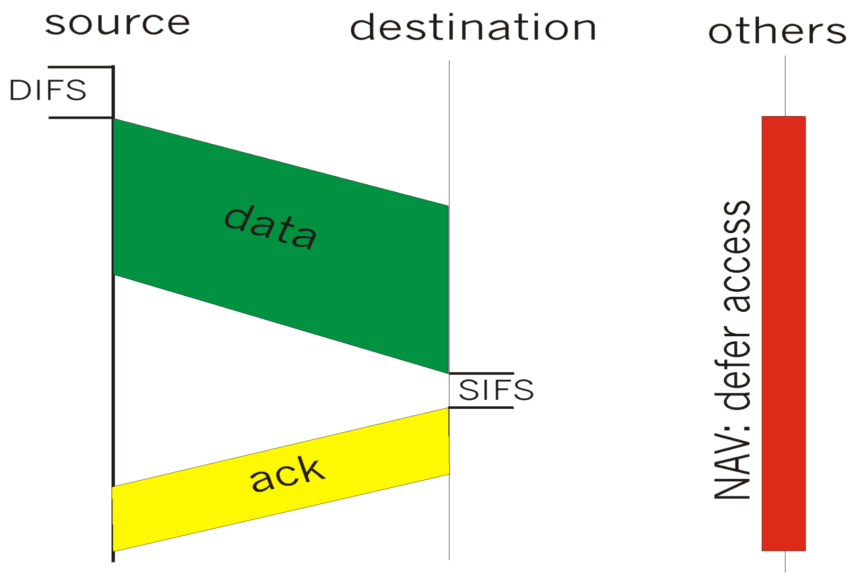
  then binary back-off

802.11 CSMA receiver:

if received OK

  return ACK after **SIFS**

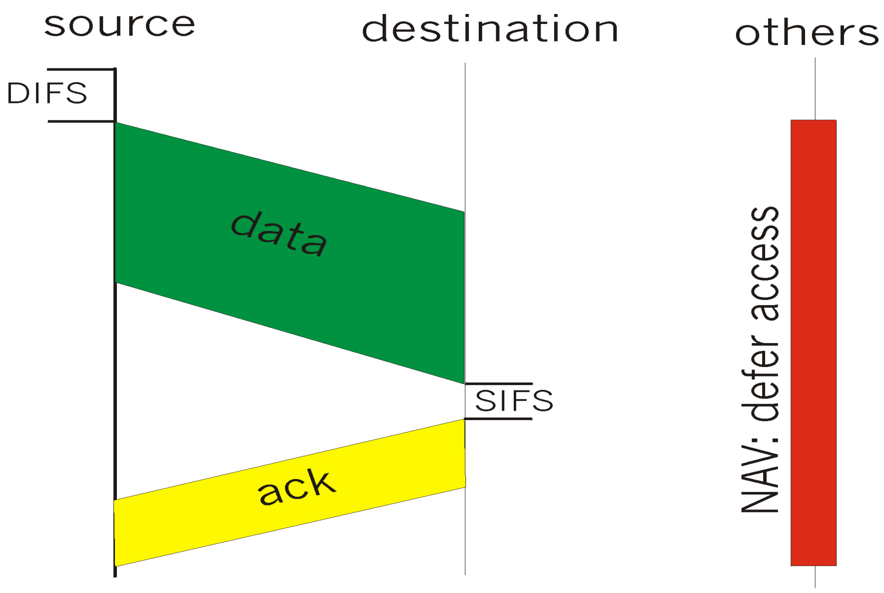
(Short Inter Frame Space)



IEEE 802.11 MAC Protocol

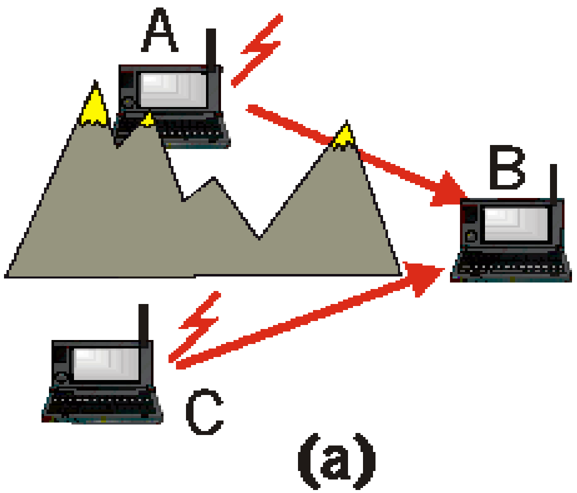
802.11 CSMA Protocol: others

- **NAV**: Network Allocation Vector
- 802.11 frame has transmission time field
- others defer access for NAV time units



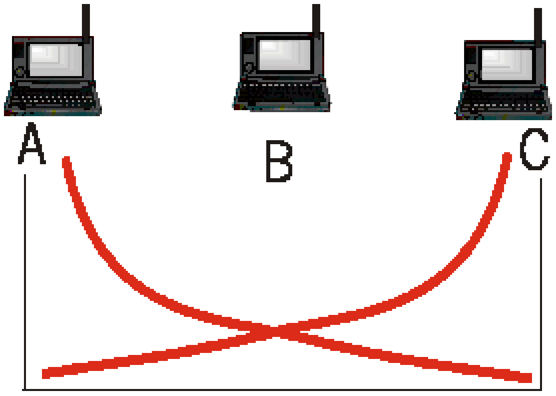
Hidden Terminal effect

- hidden terminals: A, C cannot hear each other
  - obstacles, signal attenuation
  - collisions at B



Hidden Terminal effect

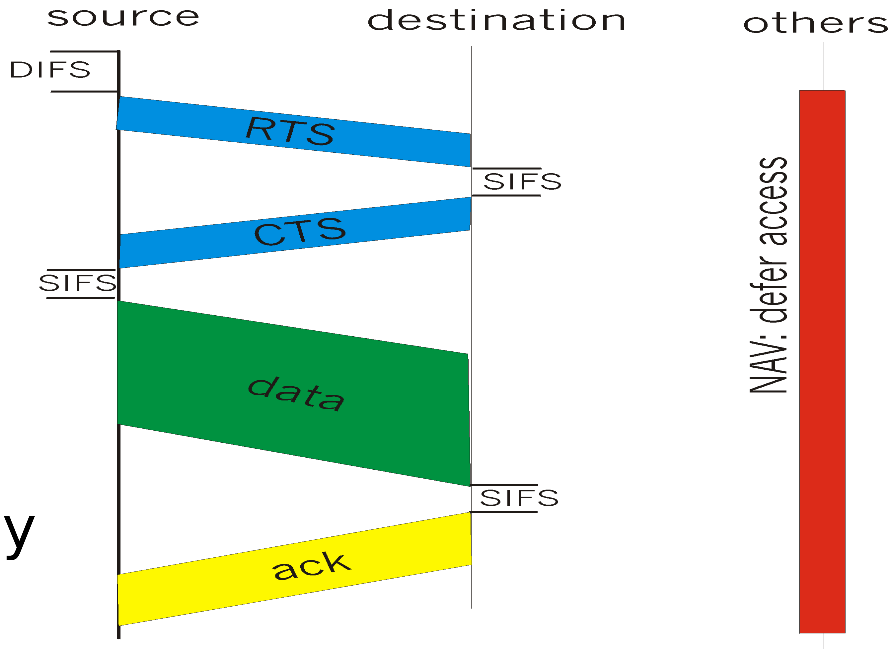
- goal: avoid collisions at B
- **CSMA/CA: CSMA with C**ollision **A**voidance



(b)

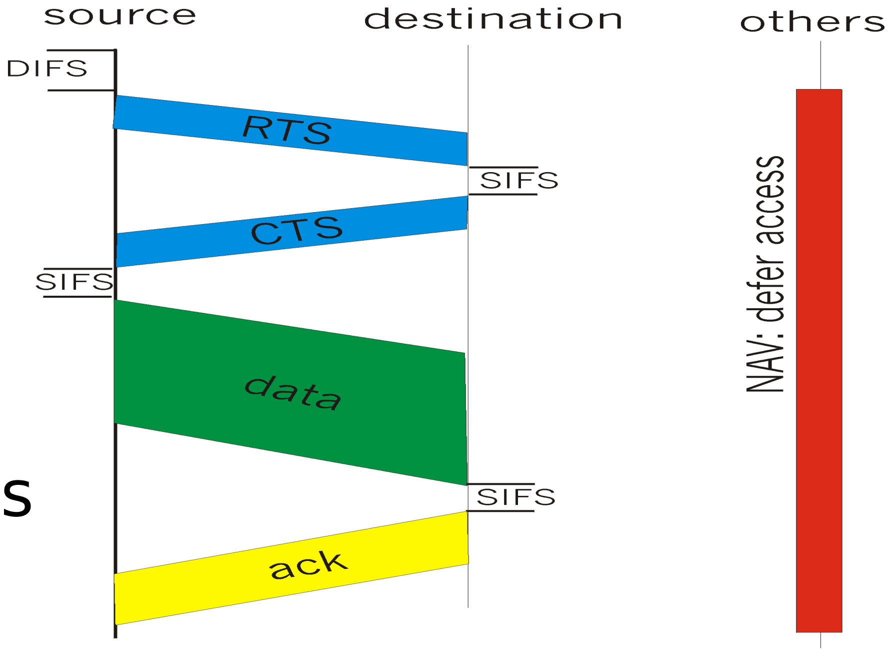
Collision Avoidance: RTS-CTS exchange

- CSMA/CA: explicit channel reservation
  - sender: send short RTS: ***request to send***
  - receiver: reply with short CTS: ***clear to send***
- CTS reserves channel for sender, notifying (possibly hidden) stations
- avoid hidden station collisions



Collision Avoidance: RTS-CTS exchange

- RTS and CTS short:
  - collisions less likely, of shorter duration
  - end result similar to collision detection
- IEEE 802.11 allows:
  - CSMA
  - CSMA/CA: reservations
  - polling from AP



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

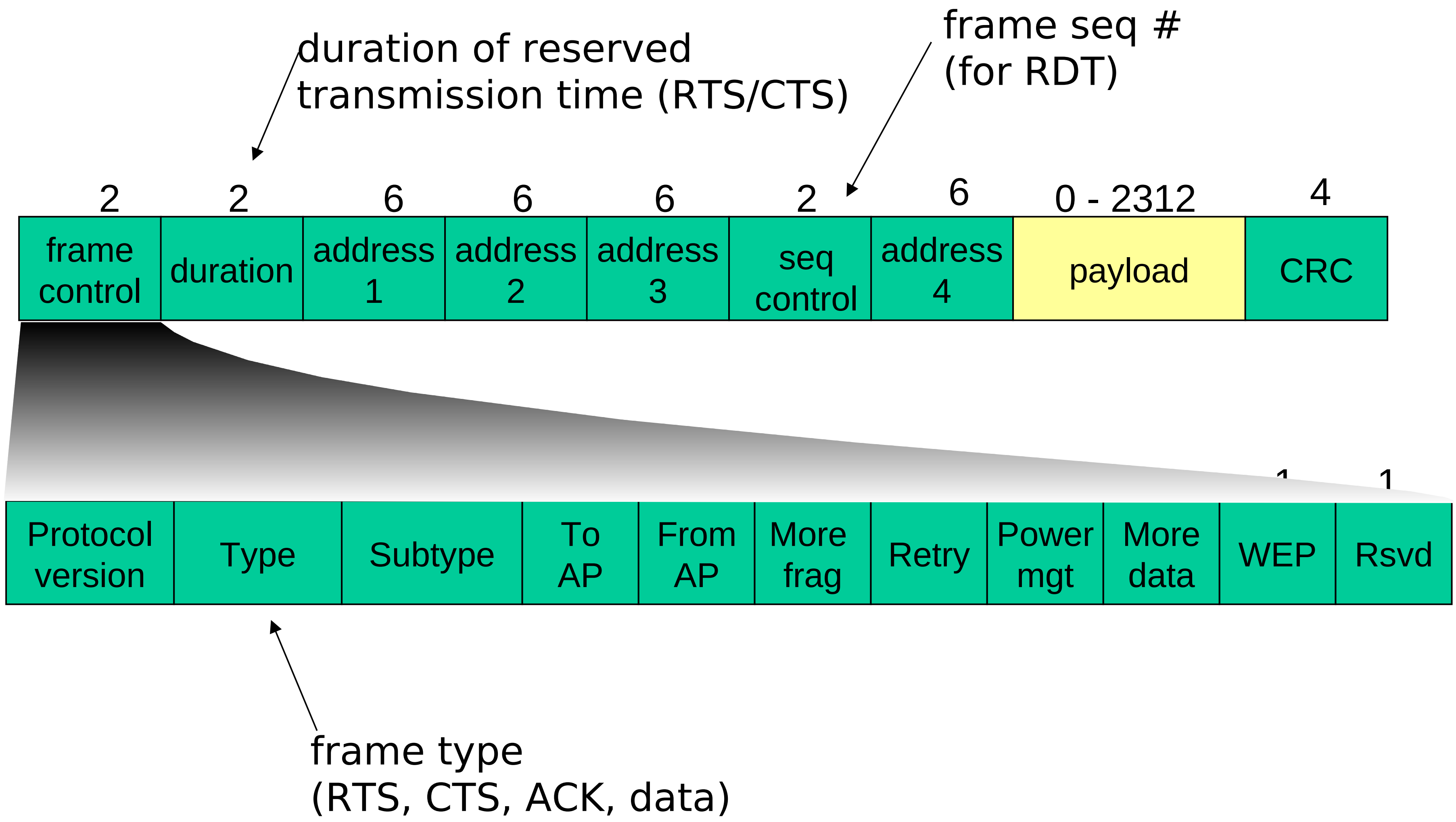
Address 4: used only in ad hoc mode

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

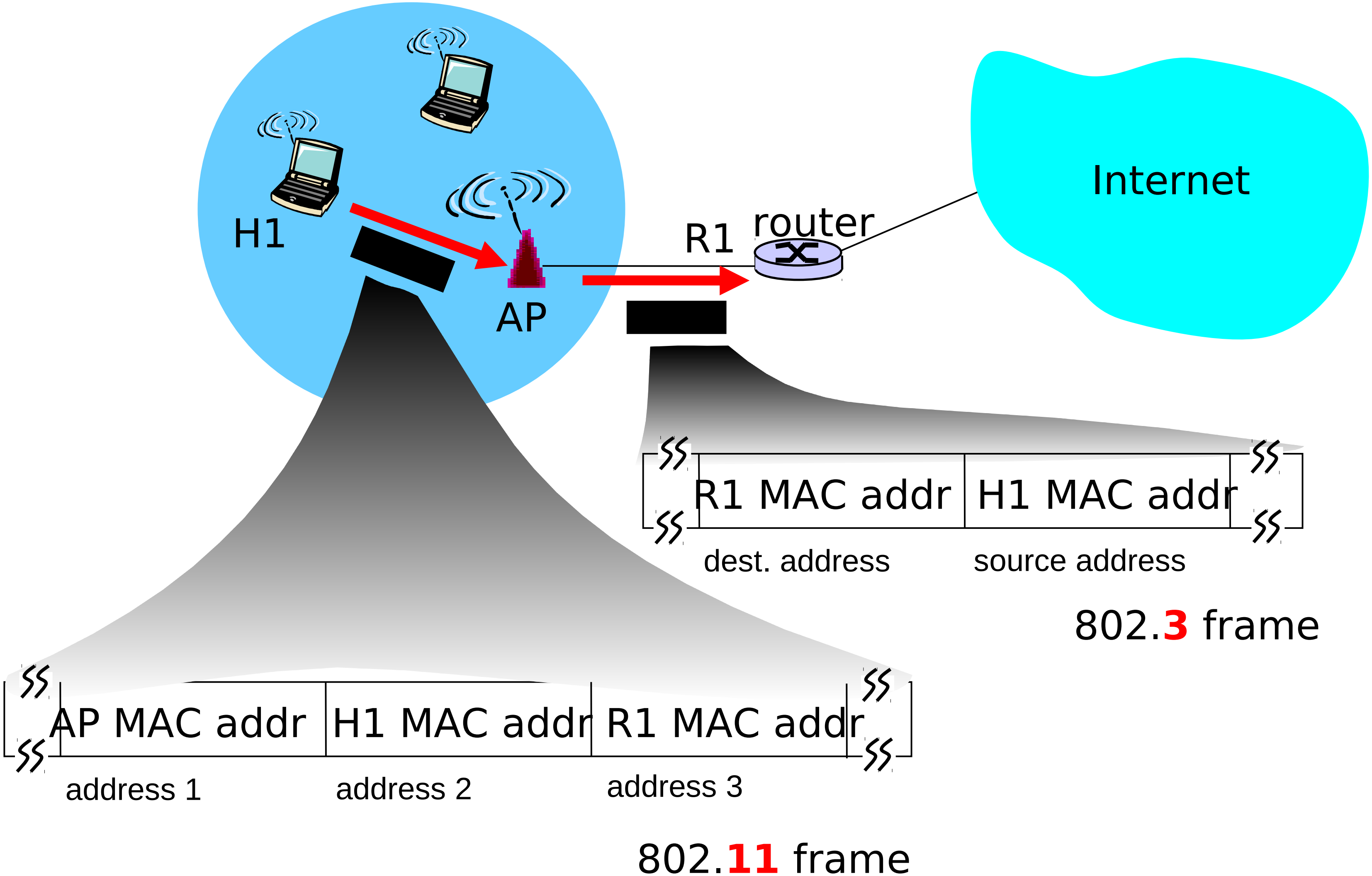
Address 3: MAC address of router interface to which AP is attached

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

802.11 frame: more



802.11 frame: addressing



Chapter 5: Summary

- principles behind data link layer services:
  - error detection, correction
  - sharing a broadcast channel: multiple access
  - link layer addressing, ARP
- various link layer technologies
  - Ethernet
  - hubs, bridges, switches
  - IEEE 802.11 LANs
  - PPP