Multiple Access Links and Protocols

Three types of links:

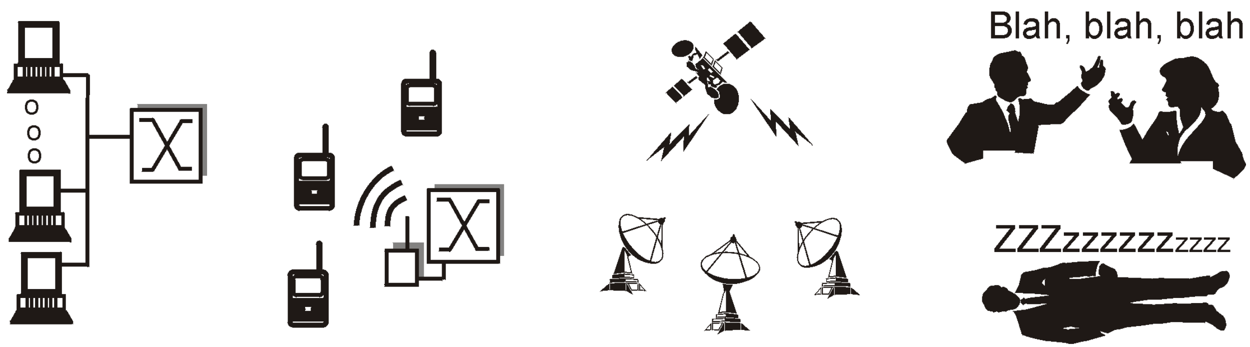
(a) Point-to-point (single wire)

(b) Broadcast (shared wire or medium; eg, E-net, wireless, etc.)

(c) Switched (eg, switched E-net, ATM etc)

We start with **Broadcast** links. Main challenge:

Multiple Access Protocol

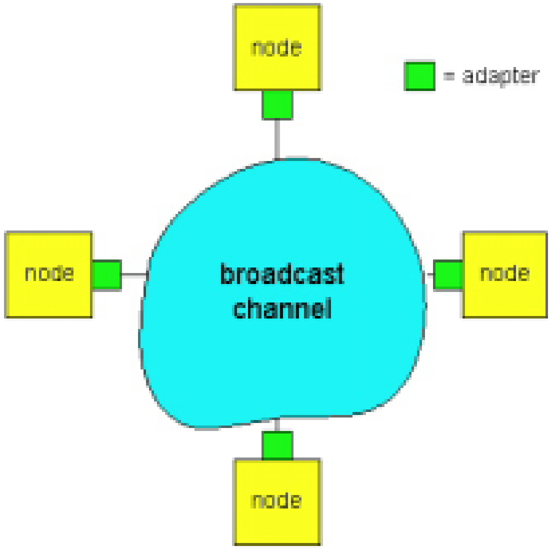


shared wire (e.g. Ethernet) — shared wireless (e.g. Wavelan) — satellite — cocktail party

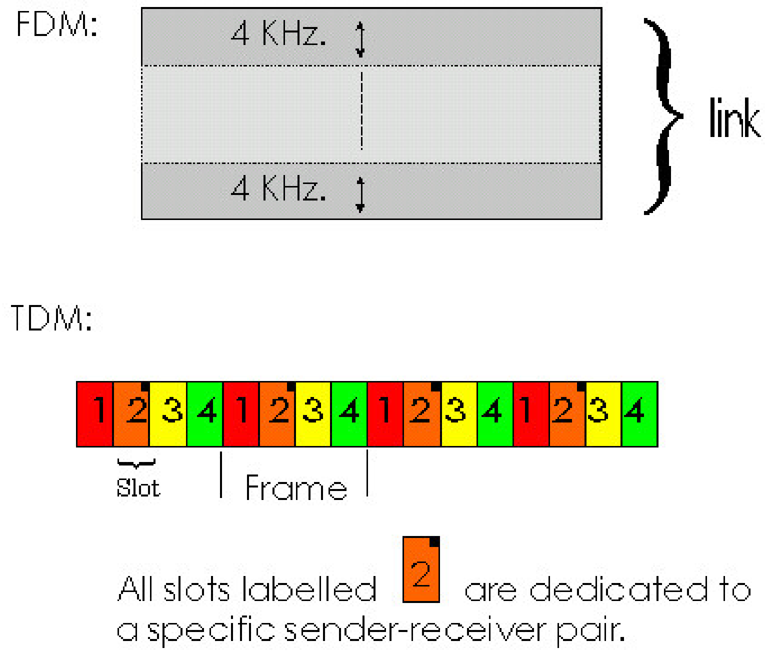
Multiple Access Control (MAC) Protocols

- MAC protocol: coordinates transmissions from different stations in order to minimize/avoid collisions
- (a) **Channel Partitioning** MAC protocols
- (b) **Random Access** MAC protocols
- (c) "**Taking turns**" MAC protocols

- Goal: **efficient, fair, simple, decentralized**



Channel Partitioning MAC protocols

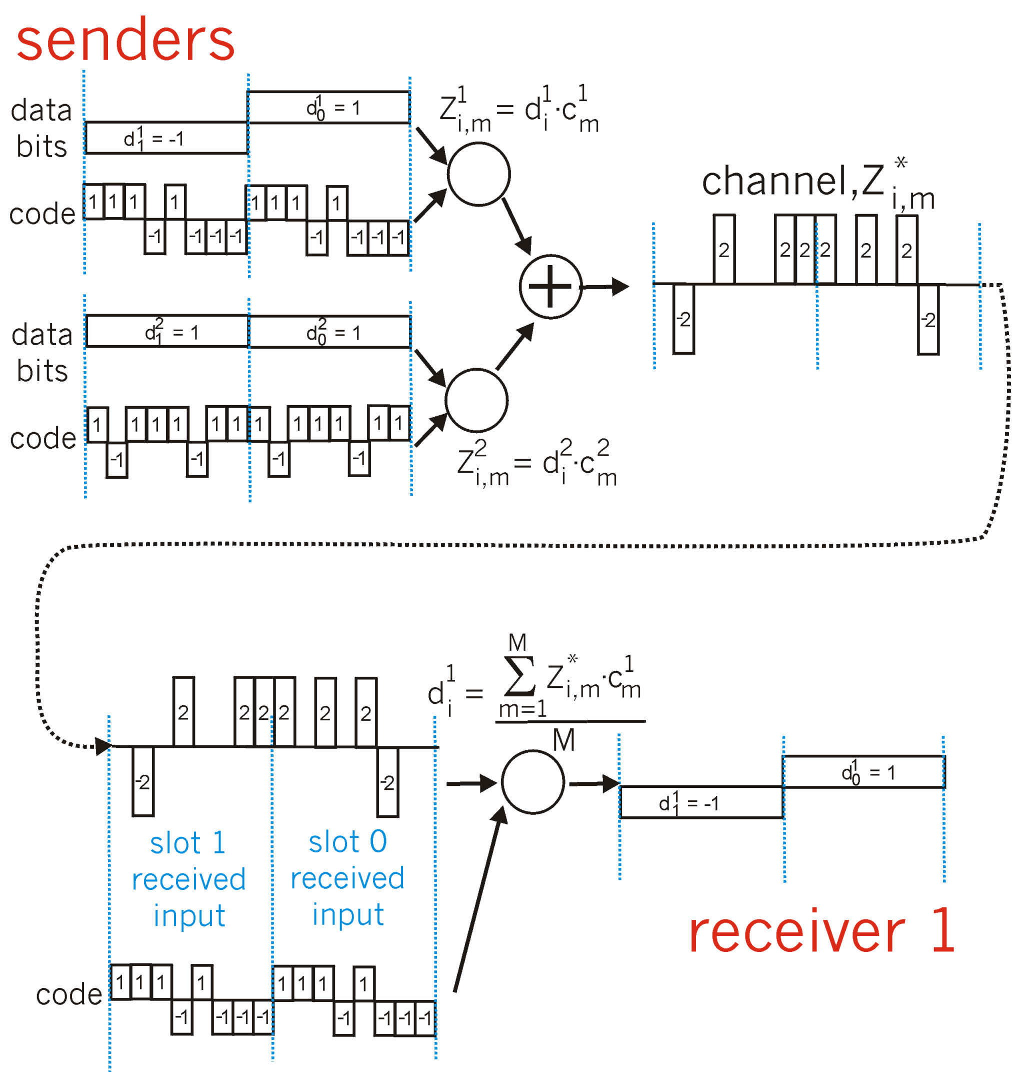


- TDM (Time Division Multiplexing): channel divided into N time slots, one per user; inefficient with low duty cycle users and at light load.
- FDM (Frequency Division Multiplexing): frequency subdivided.

Channel Partitioning (CDMA)

- **CDMA (Code Division Multiple Access)**: exploits **spread spectrum** (DS or FH) encoding scheme
- unique "code" assigned to each user; ie, **code set** partitioning
- Used mostly in **wireless** broadcast channels (cellular, satellite,etc)
- All users share the **same frequency**, but each user has **own "chipping" sequence** (ie, code)
- Chipping sequence like a **mask**: used to **encode** the signal
- **encoded signal** = (original signal) X (chipping sequence)
- **decoding**: innerproduct of encoded signal and chipping sequence (note, the innerproduct is the sum of the component-by-component products)
- To make CDMA work, chipping sequences must be chosen orthogonal to each other (i.e., innerproduct = 0)

CDMA: two-sender interference



CDMA (cont'd)

CDMA Properties:

- ☐ protects users from interference and jamming (used in WW II)
- ☐ protects users from radio multipath fading
- ☐ allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

Random Access protocols

- A node transmits **at random** (ie, no a priory coordination among nodes) at **full** channel data rate R.
- If two or more nodes "**collide**", they retransmit at random times
- The **random access MAC** protocol specifies how to detect collisions and how to recover from them (via delayed retransmissions, for example)
- Examples of random access MAC protocols:

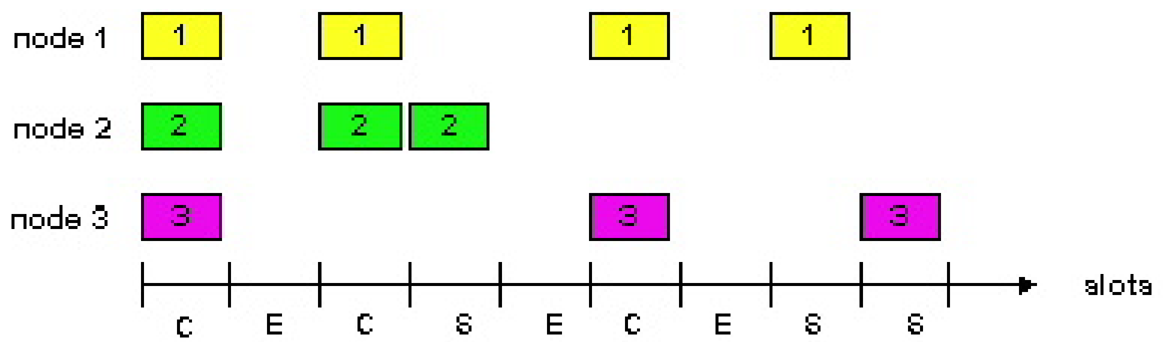
(a) SLOTTED ALOHA

(b) ALOHA

(c) CSMA and CSMA/CD

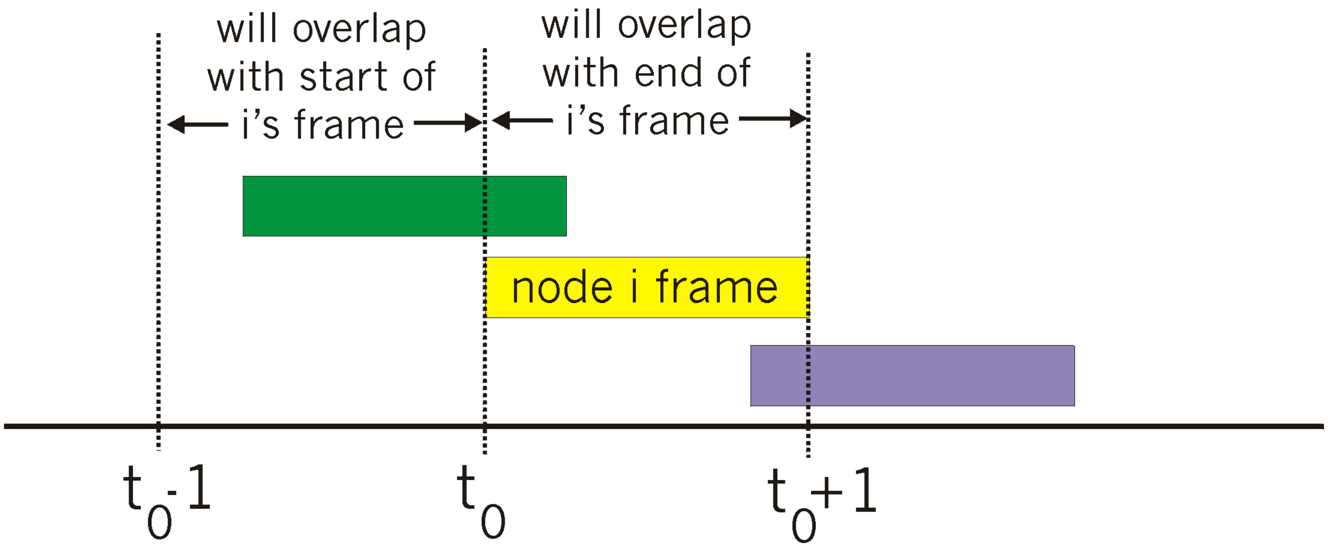
Slotted Aloha

- Time is divided into equal size slots (= full packet size)
- a newly arriving station transmits a the beginning of the next slot
- if collision occurs (assume channel feedback, eg the receiver informs the source of a collision), the source retransmits the packet at each slot with probability P, until successful.
- Success (S), Collision (C), Empty (E) slots
- S-ALOHA is channel utilization efficient; it is fully decentralized.



Pure (unslotted) ALOHA

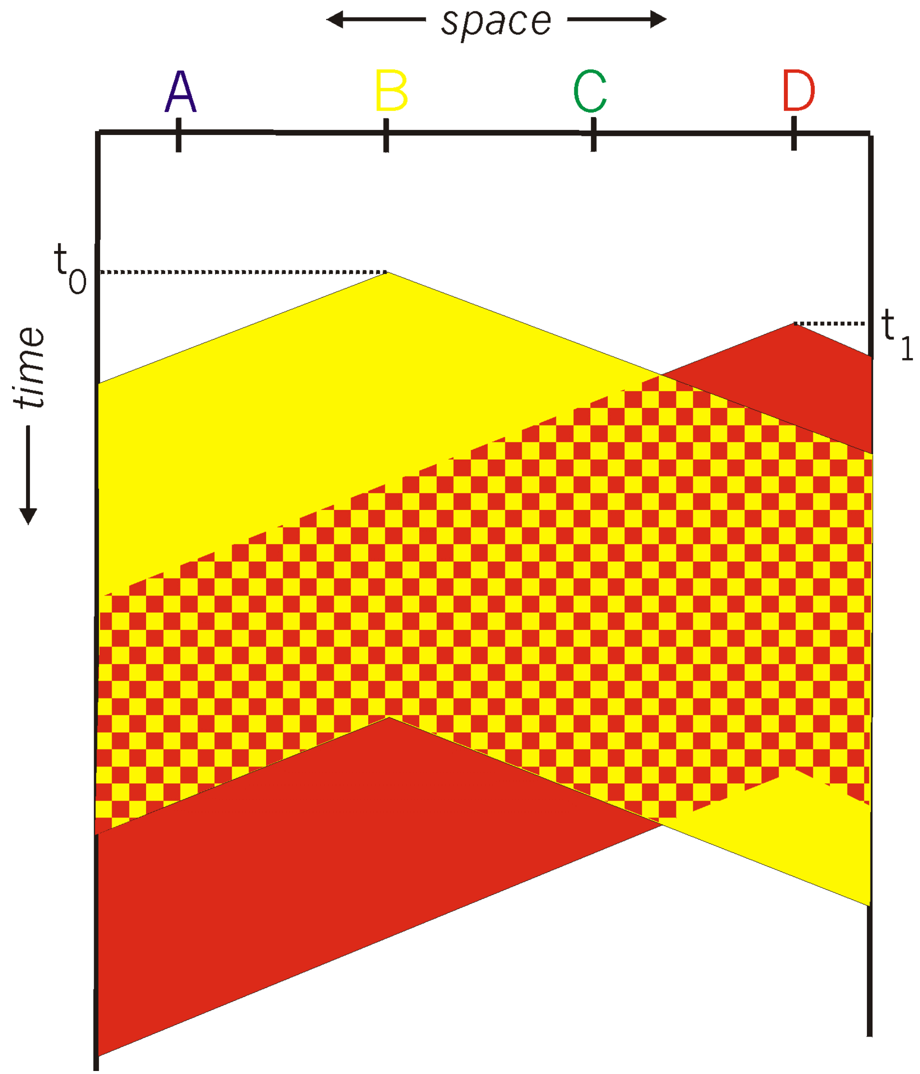
- Slotted ALOHA requires slot synchronization
- A simpler version, pure ALOHA, does not require slots
- A node transmits without awaiting for the beginning of a slot
- Collision probability increases (packet can collide with other packets which are transmitted within a window twice as large as in S-Aloha)
- Throughput is reduced by one half, ie S= 1/(2e)



CSMA (Carrier Sense Multiple Access)

- **CSMA**: listen before transmit. If channel is sensed busy, defer transmission
- **Persistent** CSMA: retry immediately when channel becomes idle (this may cause instability)
- **Non persistent CSMA**: retry after random interval
- Note: collisions may still exist, since two stations may sense the channel idle at the same time (or better, within a "vulnerable" window = round trip delay)
- In case of collision, the entire pkt transmission time is wasted

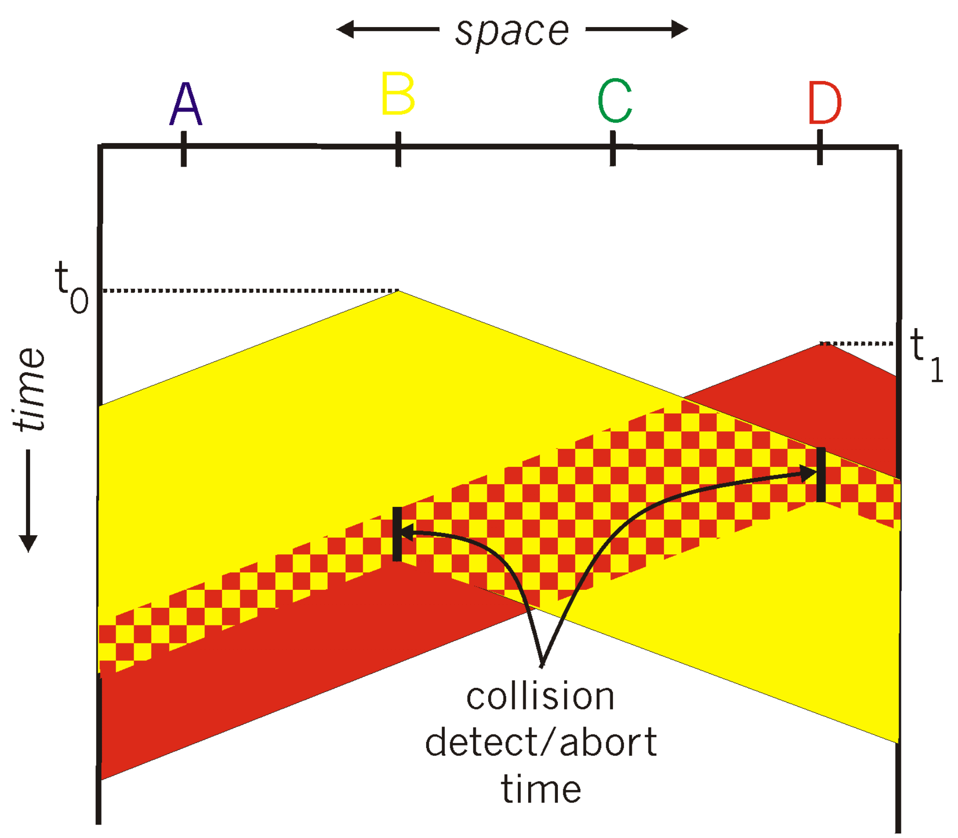
CSMA collisions



CSMA/CD (Collision Detection)

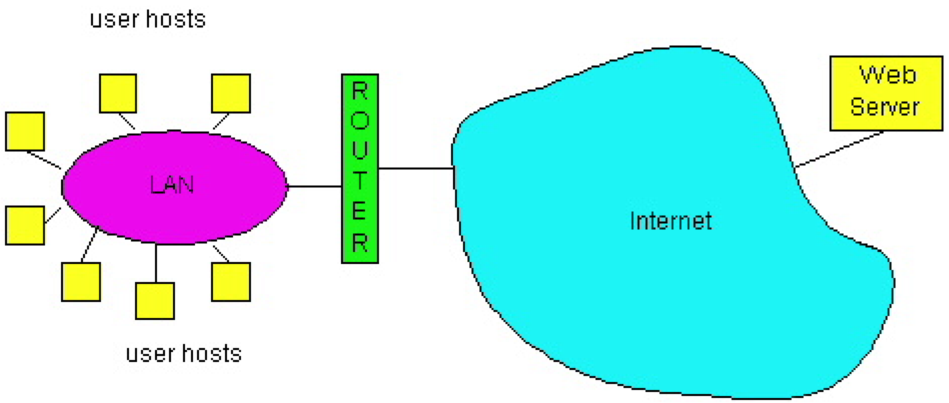
- **CSMA/CD**: carrier sensing and deferral like in CSMA. But, collisions are detected within a few bit times.
- Transmission is then aborted, reducing the channel wastage considerably.
- Typically, **persistent** retransmission is implemented
- Collision detection is **easy in wired LANs** (eg, E-net): can measure signal strength on the line, or code violations, or compare tx and receive signals
- Collision detection **cannot be done in wireless LANs** (the receiver is shut off while transmitting, to avoid damaging it with excess power)
- CSMA/CD can approach channel utilization =1 in LANs (low ratio of propagation over packet transmission time)

CSMA/CD collision detection



LAN technologies

- MAC protocols used in LANs, to control access to the channel
- **Token Rings**: IEEE 802.5 (IBM token ring), for computer room, or Department connectivity, up to 16Mbps; FDDI (Fiber Distributed Data Interface), for Campus and Metro connectivity, up to 200 stations, at 100Mbps.
- **Ethernets**: employ the CSMA/CD protocol; 10Mbps (IEEE 802.3), Fast E-net (100Mbps), Giga E-net (1,000 Mbps); by far the most popular LAN technology



Summary of MAC protocols

- What do you do with a shared media?
  - Channel Partitioning, by time or frequency
    - Code Division MA, Wave Division MA
  - Random partitioning (dynamic),
    - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - Taking Turns
    - polling from a central cite, token passing

- For satellites, sensing if the channel is busy (if the channel is carrying a signal) is hard: ALOHA
- For LANs, carrier sensing is easier, but no perfect): CSMA
- Improve things is Collision Detection exists (CSMA/CD)
- 802.3 (ethernet) is CSMA/CD

LAN Address (more)

- MAC address allocation administered by IEEE
- A manufacturer buys a portion of the address space (to assure uniqueness)
- Analogy:

  (a) MAC address: like Social Security Number

  (b) IP address: like postal address

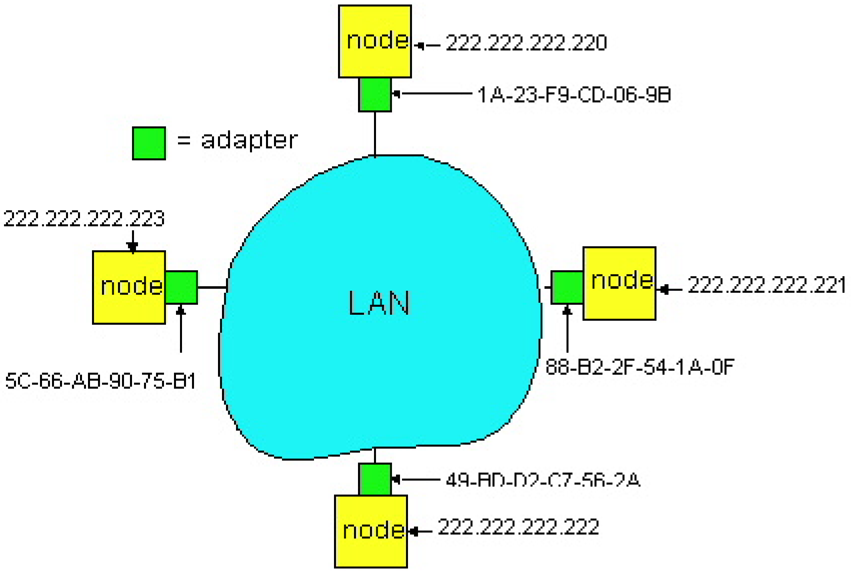
- MAC flat address => portability
- IP hierarchical address NOT portable (need mobile IP)
- Broadcast LAN address: 1111............1111

ARP: Address Resolution Protocol

- Each IP node (Host, Router) on the LAN has **ARP** module and Table
- ARP Table: IP/MAC address mappings for **some** LAN nodes

  < IP address; MAC address; TTL>

  < .... >
- TTL (Time To Live): timer, typically 20 min



ARP (more)

- Host A wants to send packet to destination IP addr XYZ on same LAN
- Source Host first checks own ARP Table for IP addr XYZ
- If XYZ **not** in the ARP Table, ARP module **broadcasts** ARP pkt:

< XYZ, MAC (?) >

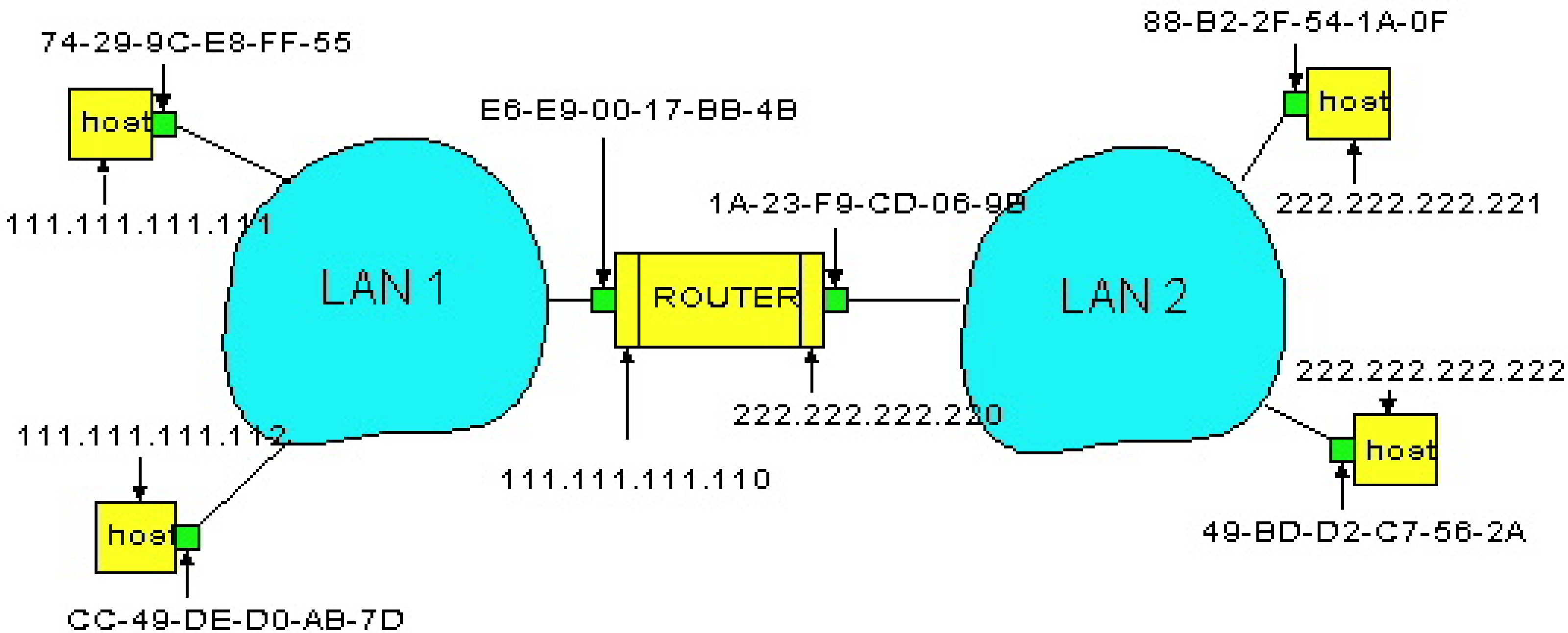
- ALL nodes on the LAN accept and inspect the ARP pkt
- Node XYZ responds with **unicast** ARP pkt carrying own MAC addr:

< XYZ, MAC (XYZ) >

- MAC address **cached** in ARP Table

Routing pkt to another LAN

- Say, route packet from source IP addr <111.111.111.111> to destination addr <222.222.222.222>



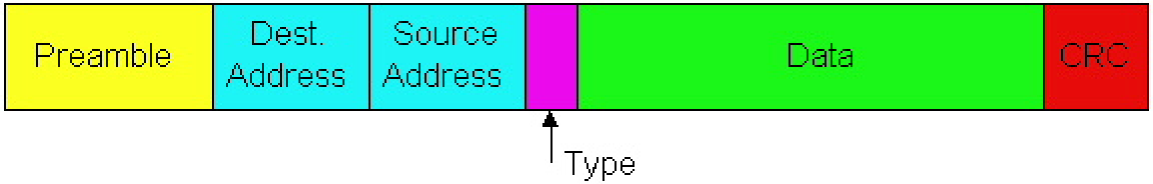
- In routing table at source Host, find router 111.111.111.110
- In ARP table at source, find MAC address E6-E9-00-17-BB-4B, etc

Ethernet

- Widely deployed because:
  - Cheap as dirt! $20 for 100Mbs!
  - First LAN technology
  - Simpler and less expensive than token LANs and ATM
  - Kept up with the speed race: 10, 100, 1000 Mbps
  - Many E-net technologies (cable, fiber etc). But they all share common characteristics

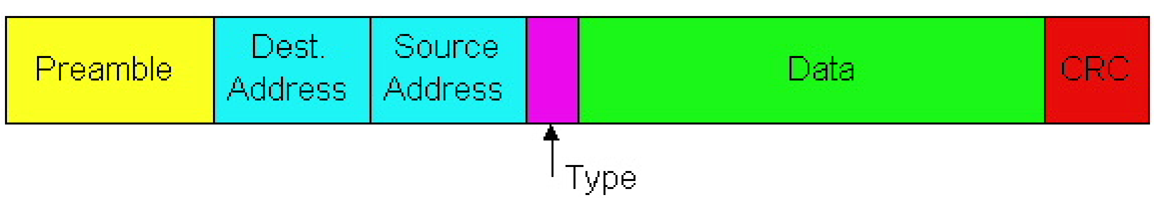
Ethernet Frame Structure

- Sending adapter encapsulates an IP datagram (or other network layer protocol packet) in **Ethernet Frame** which contains a Preamble, a Header, Data, and CRC fields
- **Preamble**: 7 bytes with the pattern 10101010 followed by one byte with the pattern 10101011; used for synchronizing receiver to sender clock (clocks are never exact, some drift is highly likely)



Ethernet Frame Structure (more)

- Header contains Destination and Source Addresses and a Type field
- **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



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}
```

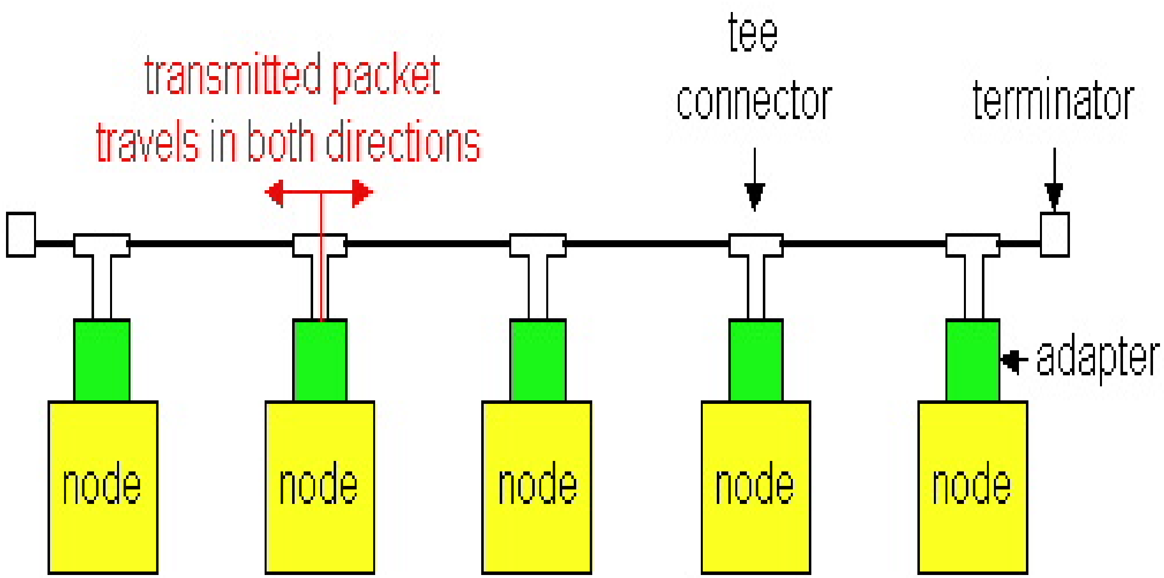
CSMA/CD (more)

- **Jam Signal**: to make sure all other transmitters are aware of the collision; 48 bits;

- **Exponential Backoff**:
  - Goal is too adapt the offered rate by transmitters to the estimated current load (ie backoff when load is heavy)
  - After the 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}

Ethernet Technologies: 10Base2

- 10==10Mbps; 2==under 200 meters maximum length of a cable segment; also referred to as "Cheapnet"
- Uses thin coaxial cable in a bus topology
- Repeaters are used to connect multiple segments (up to 5); a repeater repeats the bits it hears on one interface to its other interfaces, ie a 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 the Hub

10BaseT and 100BaseT (more)

- Max distance from node to Hub is 100 meters
- Hub can disconnect a “jabbering adapter”; 10base2 would not work if an adapter does not stop transmitting on the cable
- Hub can gather monitoring information and statistics for display to LAN administrators
- 100BaseT does not use Manchester encoding; it uses 4B5B for better coding efficiency

Gbit Ethernet

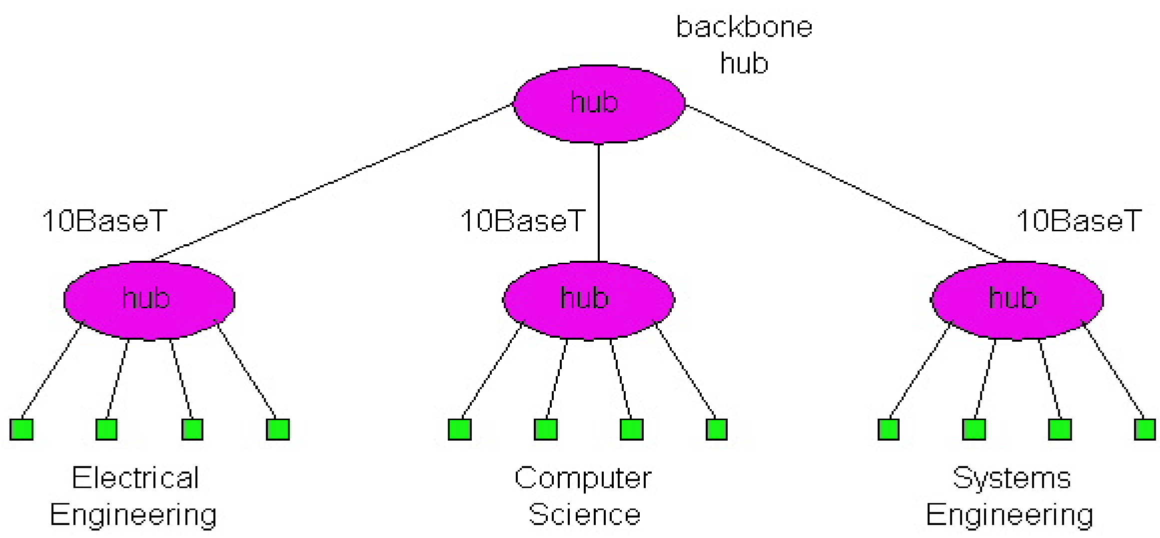
- Use standard Ethernet frame format
- Allows for Point-to-point links and shared broadcast channels
- In shared mode, CSMA/CD is used; short distances between nodes to be efficient
- Uses Hubs called here "Buffered Distributors"
- Full-Duplex at 1 Gbps for point-to-point links

Hubs, Bridges, and Switches

- Used for extending LANs in terms of geographical coverage, number of nodes, administration capabilities, etc.
- Differ in regards to:
  - collision domain isolation
  - layer at which they operate
- Different than routers
  - plug and play
  - don’t provide optimal routing of IP packets

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 a **backbone** hub at its top



Hubs (more)

- Each connected LAN is referred to as a LAN **segment**
- Hubs **do not isolate** collision domains: a node may collide with any node residing at any segment in the LAN

- Hub Advantages:
  - Simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one of the hubs malfunction
  - Extends maximum distance between node pairs (100m per Hub)

Hubs (more)

- Hub Limitations:
  - Single collision domain results in no increase in max throughput; the multi-tier throughput same as the the single segment throughput
  - Individual LAN restrictions pose limits on the number of nodes in the same collision domain (thus, per Hub); and on the total allowed geographical coverage
  - Cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)

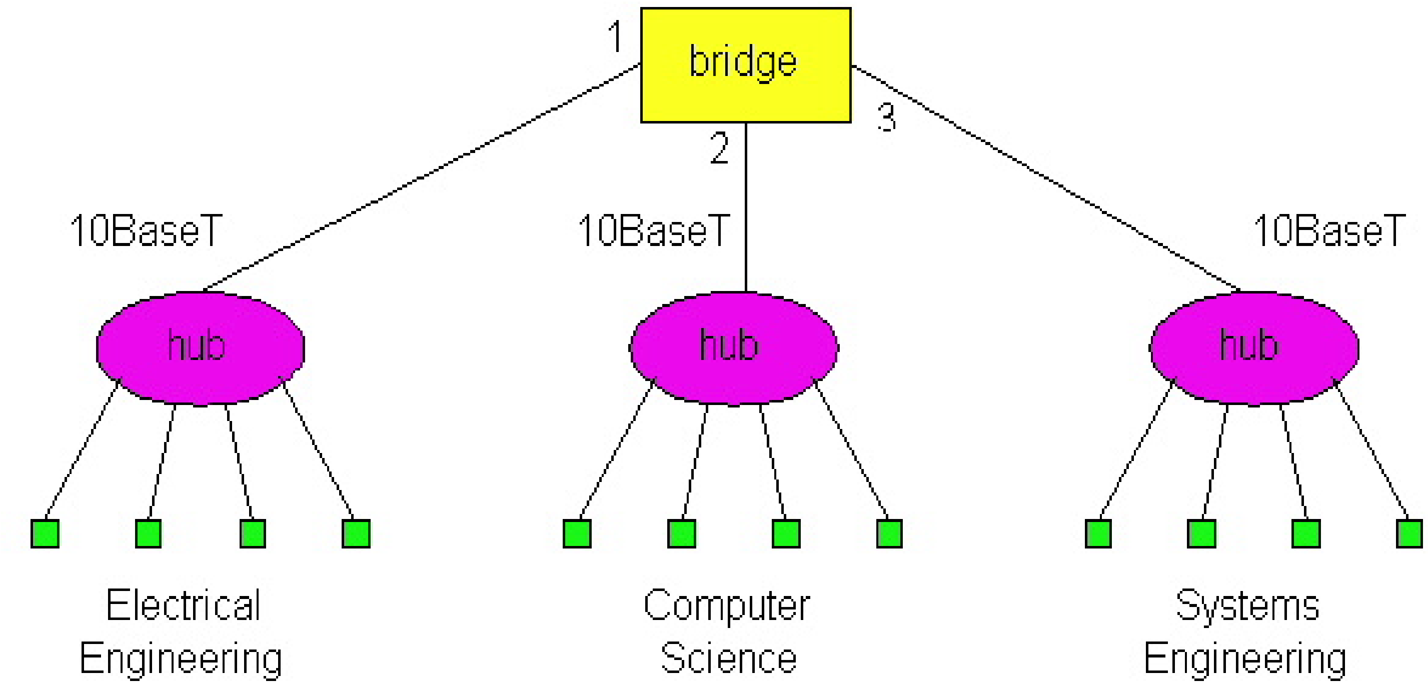
Bridges

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

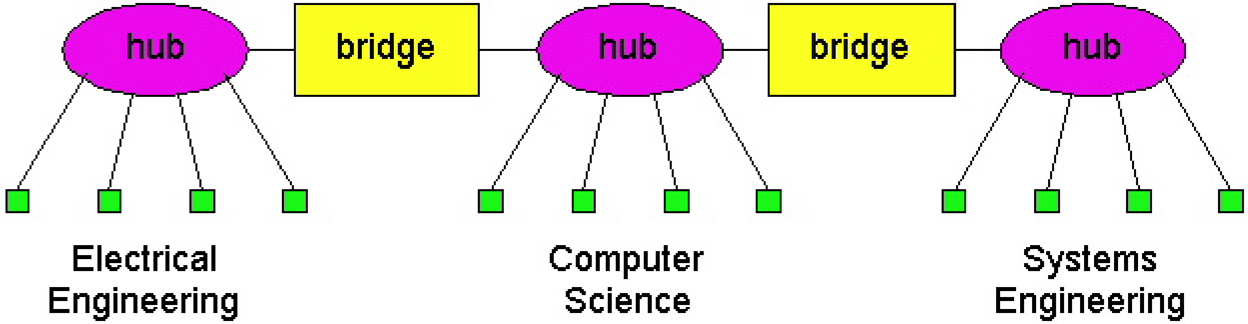
Bridges (more)

- 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

Backbone Bridge



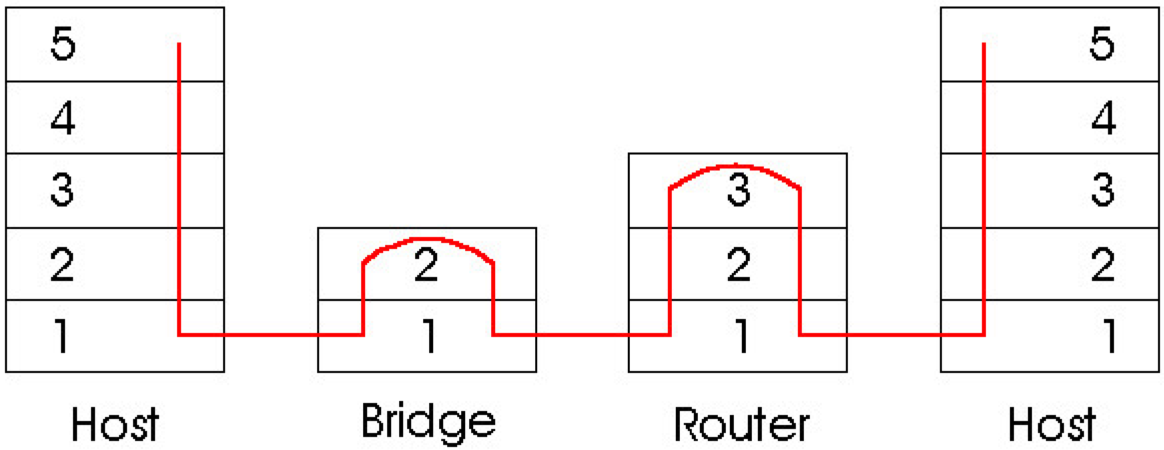
Interconnection Without Backbone



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

Bridges vs. Routers

- Both are store-and-forward devices, but Routers are Network Layer devices (examine network layer headers) and Bridges are Link Layer devices
- Routers maintain routing tables and implement routing algorithms, bridges maintain filtering tables and 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 prots)

+ 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 are required in large networks (thousands of hosts)

Ethernet Switches

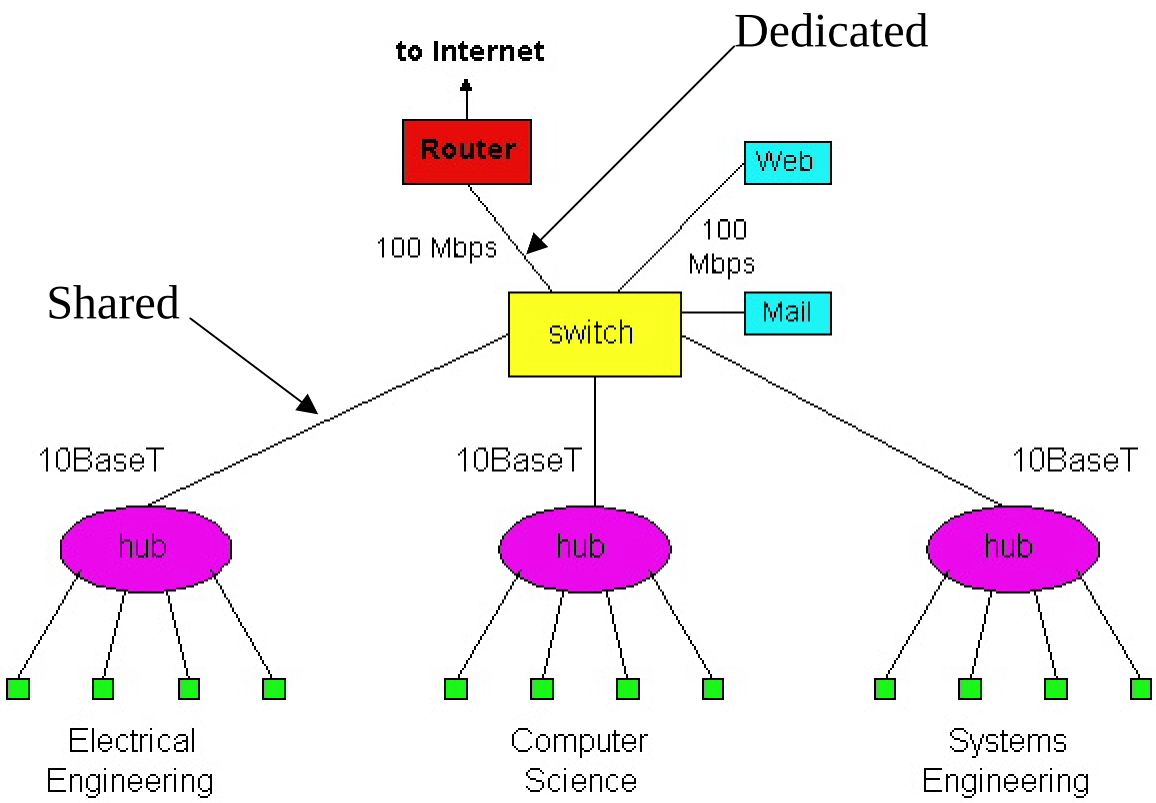
- A switch is a device that incorporates bridge functions as well as point-to-point 'dedicated connections'
- A host attached to a switch via a dedicated point-to-point connection; will always sense the medium as idle; no collisions ever!
- Ethernet Switches provide a combinations of shared/dedicated, 10/100/1000 Mbps connections

Ethernet

- Some E-net switches support cut-through switching: frame forwarded immediately to destination without awaiting for assembly of the entire frame in the switch buffer; slight reduction in latency

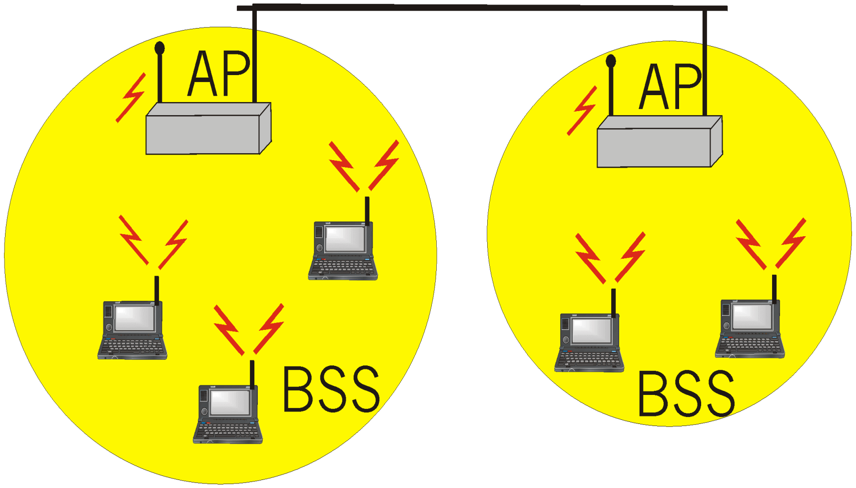
- Ethernet switches vary in size, with the largest ones incorporating a high bandwidth interconnection network

Ethernet Switches (more)



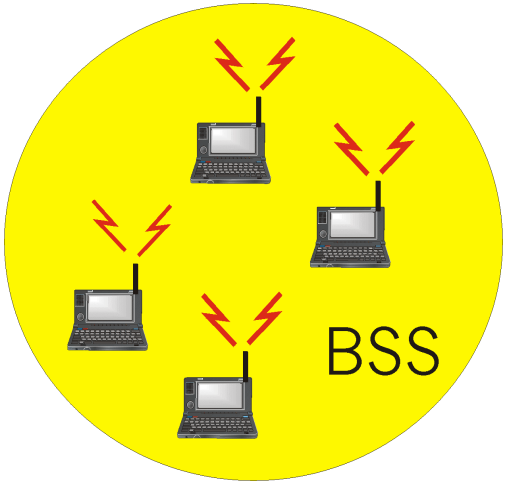
IEEE 802.11 Wireless LAN

- Wireless LANs are becoming popular for mobile Internet access
- Applications: nomadic Internet access, portable computing, ad hoc networking (multihopping)
- IEEE 802.11 standards defines MAC protocol; unlicensed frequency spectrum bands: 900Mhz, 2.4Ghz
- **Basic Service Sets + Access Points => Distribution System**
- Like a bridged LAN (flat MAC address)



Ad Hoc Networks

- IEEE 802.11 stations can dynamically form a group without AP
- Ad Hoc Network: no pre-existing infrastructure
- Applications: “laptop” meeting in conference room, car, airport; interconnection of “personal” devices (see bluetooth.com); battelfield; pervasive computing (smart spaces)
- IETF MANET (Mobile Ad hoc Networks) working group

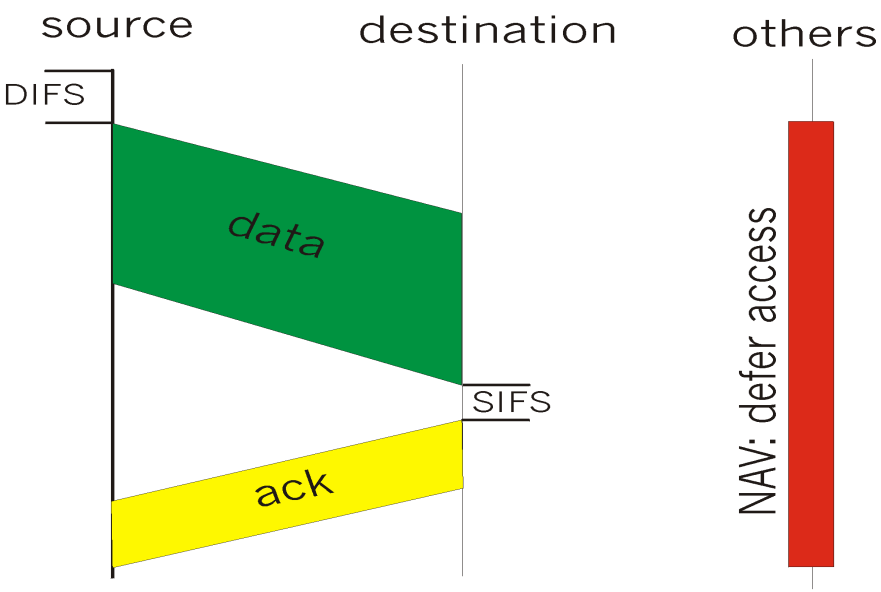


IEEE 802.11 MAC Protocol

CSMA Protocol:

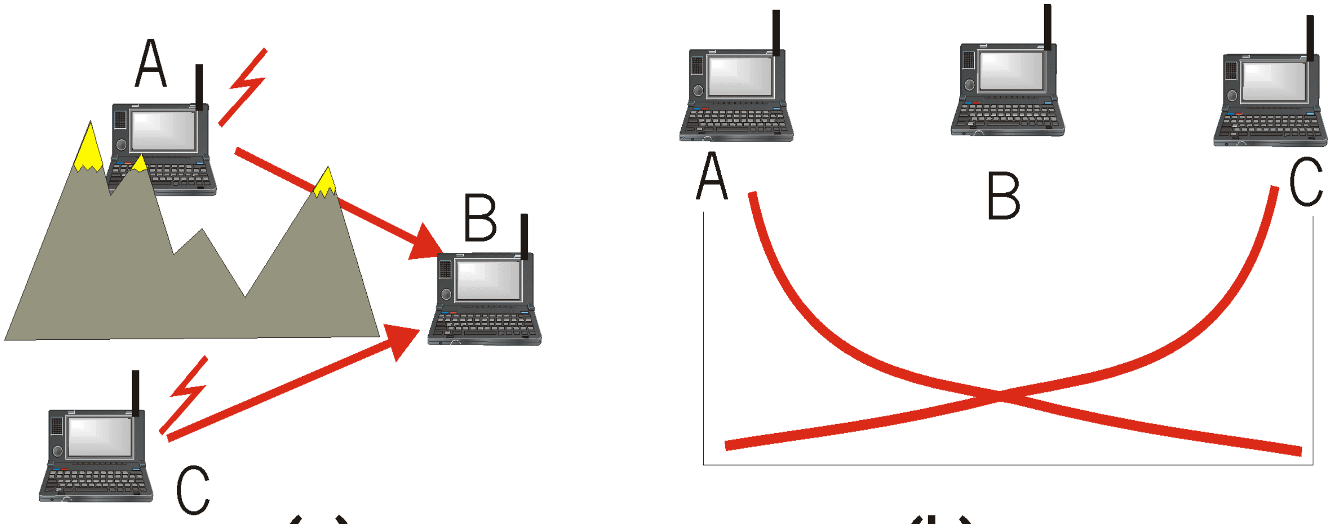
- sense channel idle for **DISF** sec (Distributed Inter Frame Space)
  - transmit frame (no Collision Detection)
  - receiver returns ACK after **SIFS** (Short Inter Frame Space)
- if channel sensed busy then binary backoff

NAV: Network Allocation Vector
(min time of deferral)



Hidden Terminal effect

- CSMA inefficient in presence of hidden terminals
- Hidden terminals: A and B cannot hear eachother because of obstacles or signal attenuation; so, their packets collide at B
- Solution? **CSMA/CA**
- **CA** = Collision Avoidance



(a) (b)