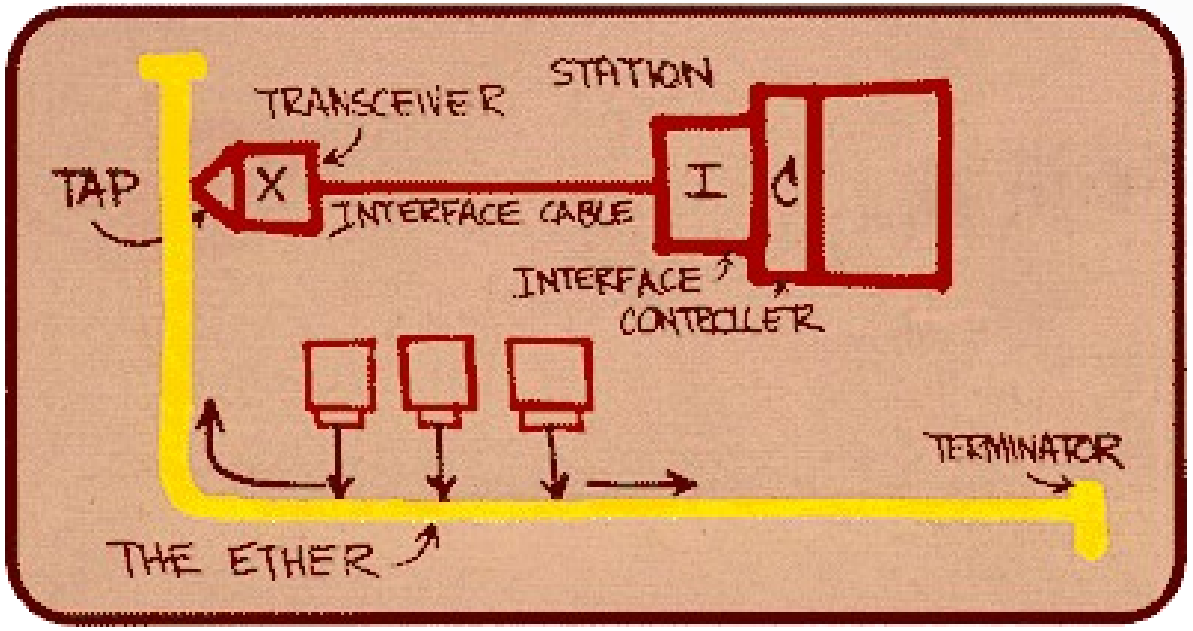
Outline

- Introduction and services
- Error detection and correction
- Multiple access protocols
- LAN addresses and ARP
- **Ethernet**
- Hubs, bridges, and switches
- Wireless links and LANs
- PPP

Ethernet

"dominant" LAN technology:

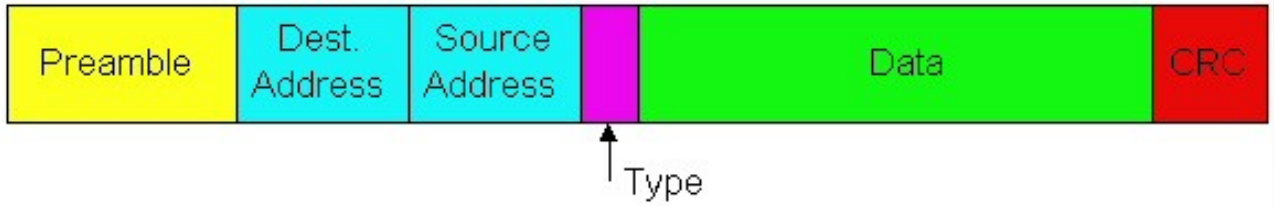
- cheap $20 for 100Mbps !
- first widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10, 100, 1000 Mbps



Metcalfe's Ethernet sketch

Ethernet Frame Structure

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

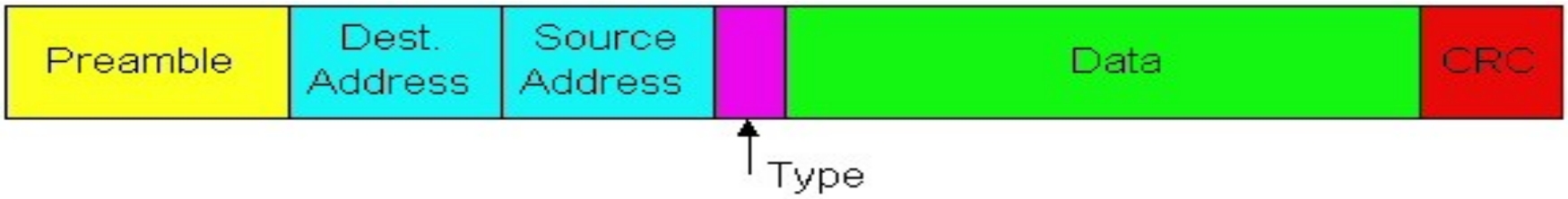


Preamble:

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



Unreliable, connectionless service

- Connectionless: No handshaking between sending and receiving adapter.
- Unreliable: receiving adapter doesn't send *acks* or *nacks* to sending adapter
  - stream of datagrams passed to network layer can have gaps
  - gaps will be filled if app is using TCP
  - otherwise, app will see the gaps

Ethernet uses CSMA/CD

- No slots
- adapter doesn't transmit if it senses that some other adapter is transmitting, that is, *carrier sense*
- transmitting adapter aborts when it senses that another adapter is transmitting, that is, *collision detection*
- Before attempting a retransmission, adapter waits a random time, that is, *random access*

Ethernet CSMA/CD algorithm

0. wait from frame from network layer
1. *Adaptor* gets *datagram* and creates frame
2. **if** *channel idle*, adaptor starts to transmit frame.
   else *channel busy*, wait until channel idle plus *96 bit* times then transmit
3. If adapter transmits entire frame without detecting a collision, then done, go to step 0.
4. *collision detected*, abort transmission and send *48 bit jam signal*
5. After aborting, enters exponential backoff phase: after the n collision, adapter chooses a ***K*** at random from {0,1,2,…,2 -1}, m = min(n,10). Adapter *waits K*(512 bit times*) and returns to Step 2

Ethernet's CSMA/CD (more)

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

Bit time: 0.1 microseconds for 10 Mbps Ethernet ;
for K=1023, wait time is about 50 milliseconds

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 collisions, choose K from {0,1,2,3,4,…,1023}

CSMA/CD efficiency

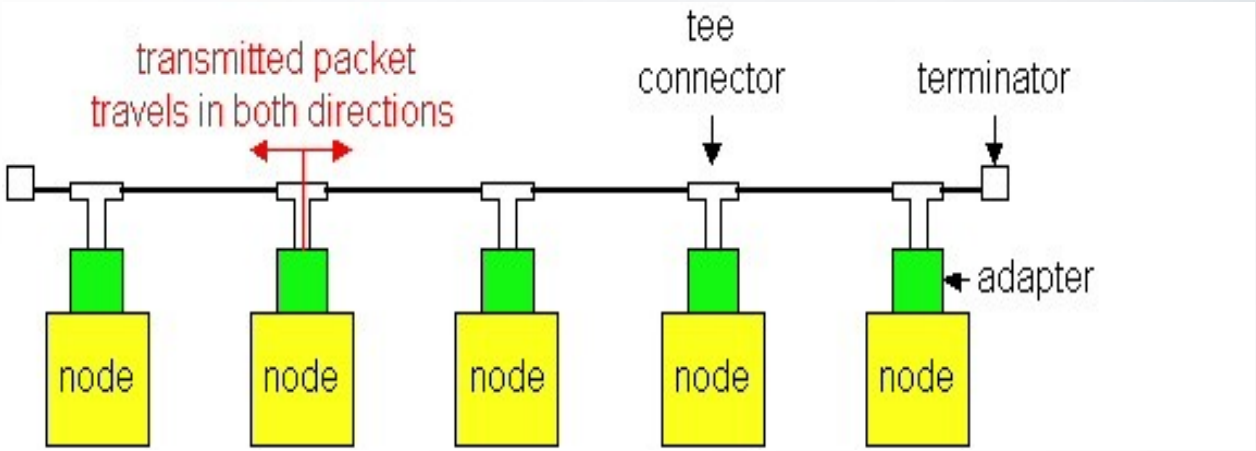
- t_{prop} = max propagation time between 2 nodes in LAN
- t_{trans} = time to transmit max-size Ethernet frame

$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

- Efficiency goes to 1 as t_{prop} goes to 0
- Goes to 1 as t_{trans} goes to ∞

Ethernet Technologies: 10Base2

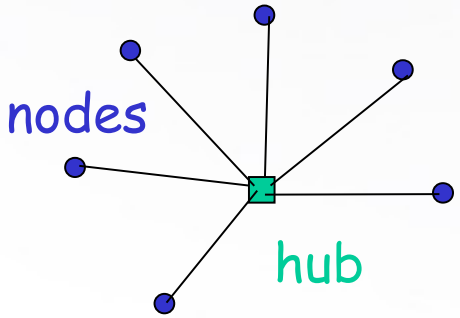
- 10: 10Mbps; 2: under 200 meters maximum cable length
- thin coaxial cable in a bus topology



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

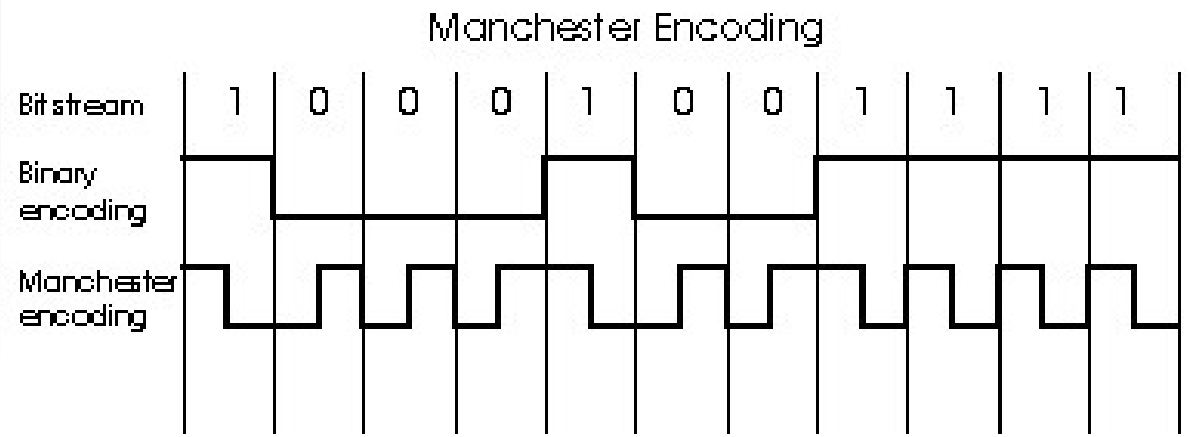
10BaseT and 100BaseT

- 10/100 Mbps rate; latter called “fast ethernet”
- T stands for Twisted Pair
- Nodes connect to a hub: “star topology”; **100 m** max distance between nodes and hub



- Hubs are essentially physical-layer repeaters:
  - bits coming in one link go out all other links
  - no frame buffering
  - no CSMA/CD at hub: adapters detect collisions
  - provides network management functionality

Manchester Encoding



- Used in 10BaseT, 10Base2
- 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!
- This is physical-layer stuff ! *(covered in CAN1101-Data Com)*

Gigabit 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
- 10 Gbps now !

Outline

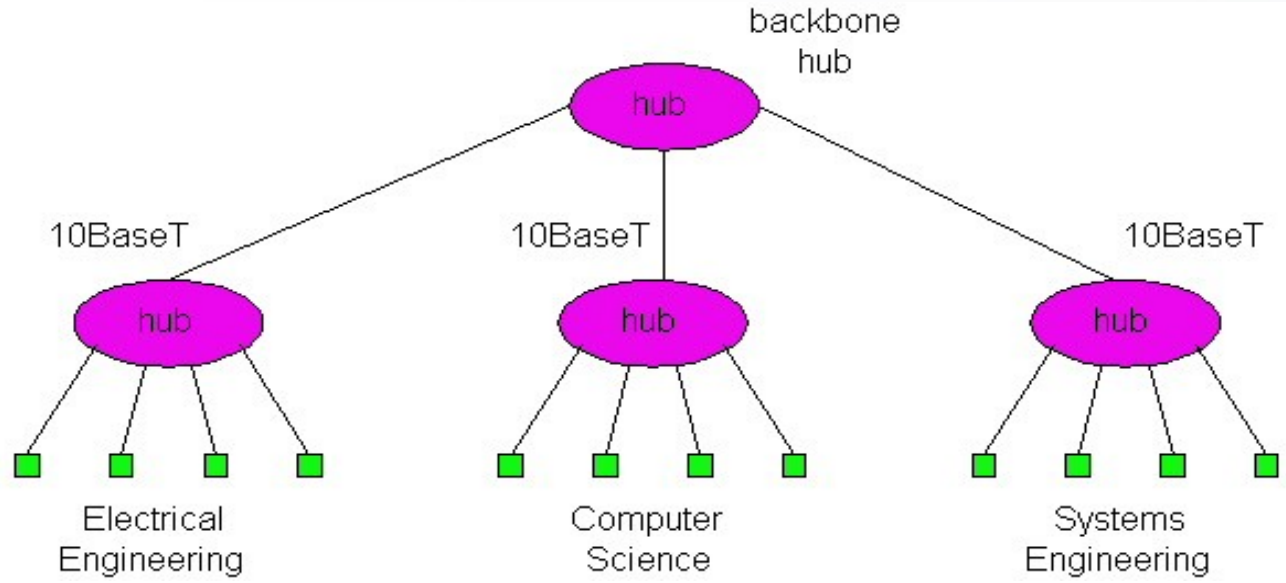
- Introduction and services
- Error detection and correction
- Multiple access protocols
- LAN addresses and ARP
- Ethernet
- **Hubs, bridges, and switches**
- Wireless links and LANs
- PPP

Interconnecting LAN segments

- Hubs
- Bridges
- Switches
  - Remark: switches are essentially multi-port bridges.
  - What we say about bridges also holds for switches!

Interconnecting with hubs

- Backbone hub interconnects LAN segments
- Extends max distance between nodes
- But individual segment collision domains become one large collision domain
  - if a node in CS and a node EE transmit at same time: collision
- Can't interconnect 10BaseT & 100BaseT

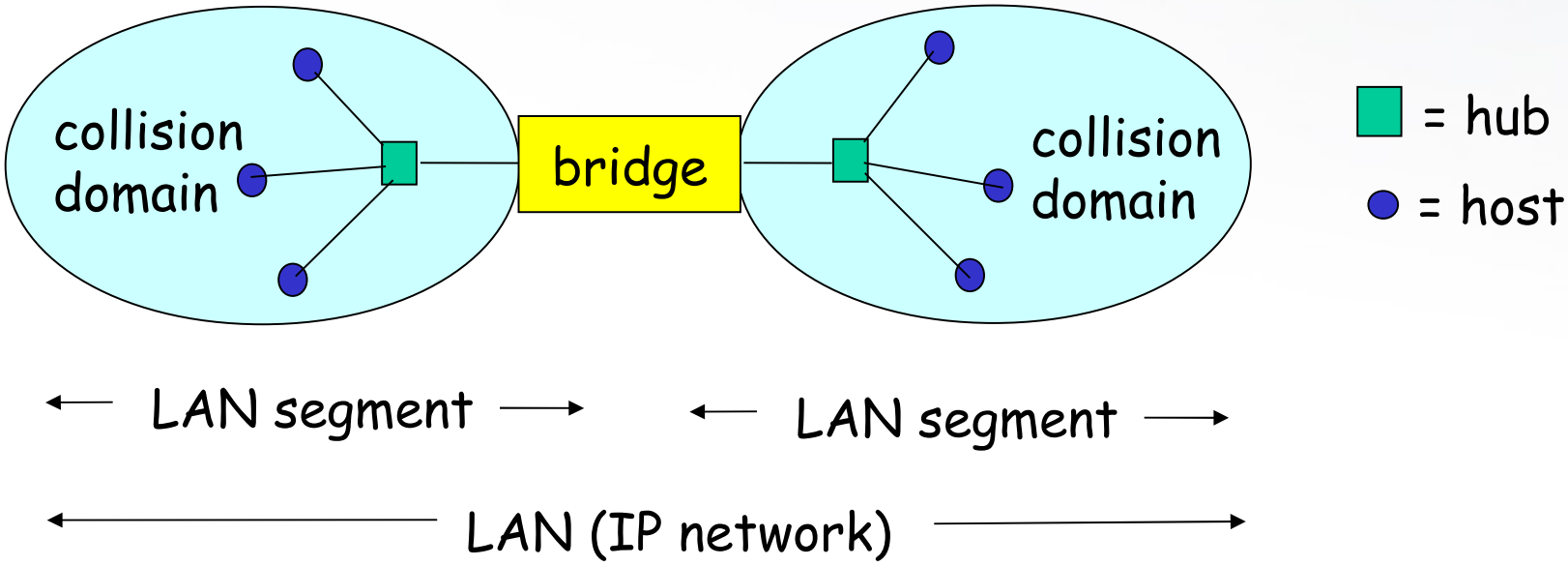


Bridges

- **Link layer device**
  - stores and forwards Ethernet frames
  - examines frame header and selectively forwards frame based on MAC destination address
  - when frame is to be forwarded on segment, uses CSMA/CD to access segment
- transparent
  - hosts are unaware of presence of bridges
- plug-and-play, self-learning
  - bridges do not need to be configured

Bridges: traffic isolation

- Bridge installation breaks LAN into LAN segments
- bridges filter packets:
  - same-LAN-segment frames not usually forwarded onto other LAN segments
  - segments become separate collision domains



Self learning

- A bridge has a bridge table
- entry in bridge table:
  - (*Node LAN Address, Bridge Interface, Time Stamp*)
  - stale entries in table dropped (TTL can be 60 min)
- bridges *learn* which hosts can be reached through which interfaces
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender/location pair in bridge table

Filtering/Forwarding

When bridge receives a frame:

index bridge table using MAC dest address

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

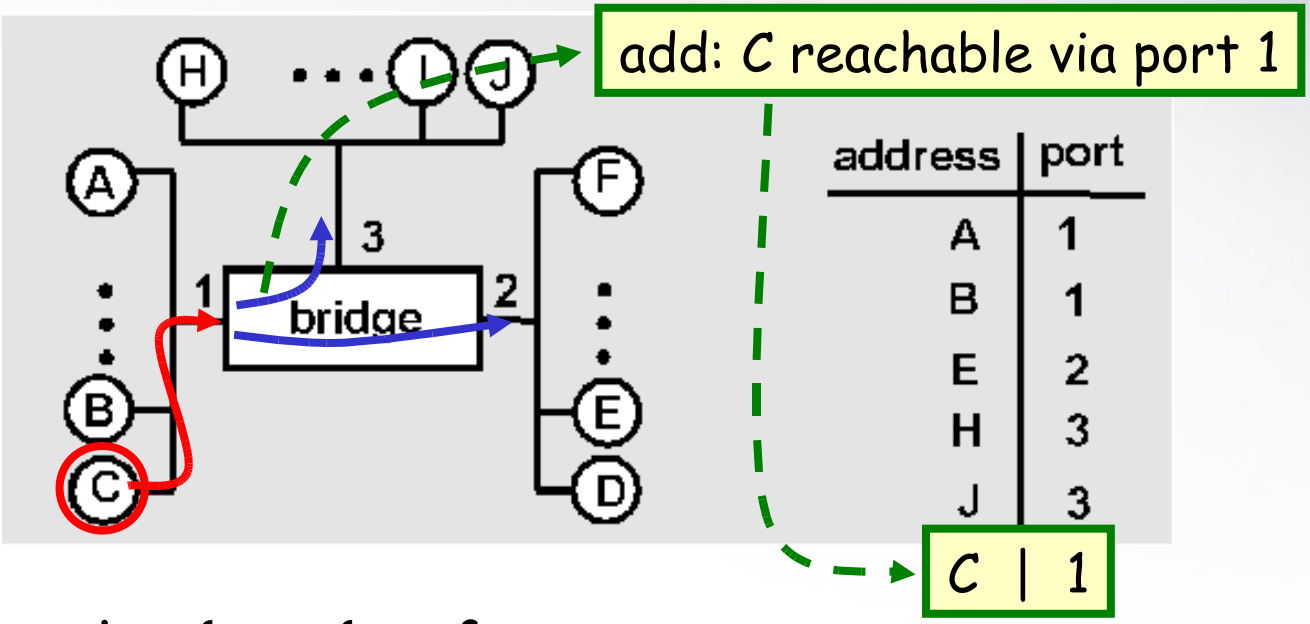
}

else flood

forward on all but the interface on which the frame arrived

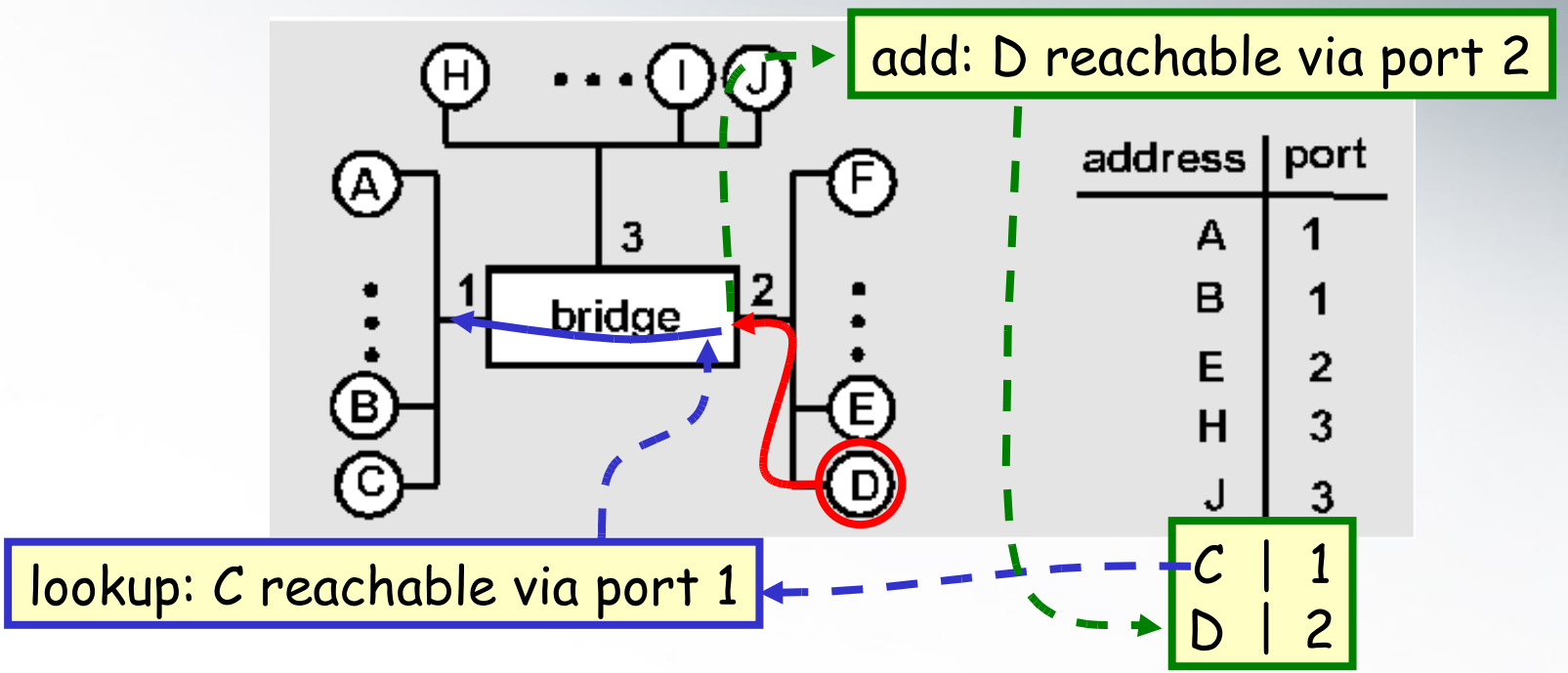
Bridge example

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



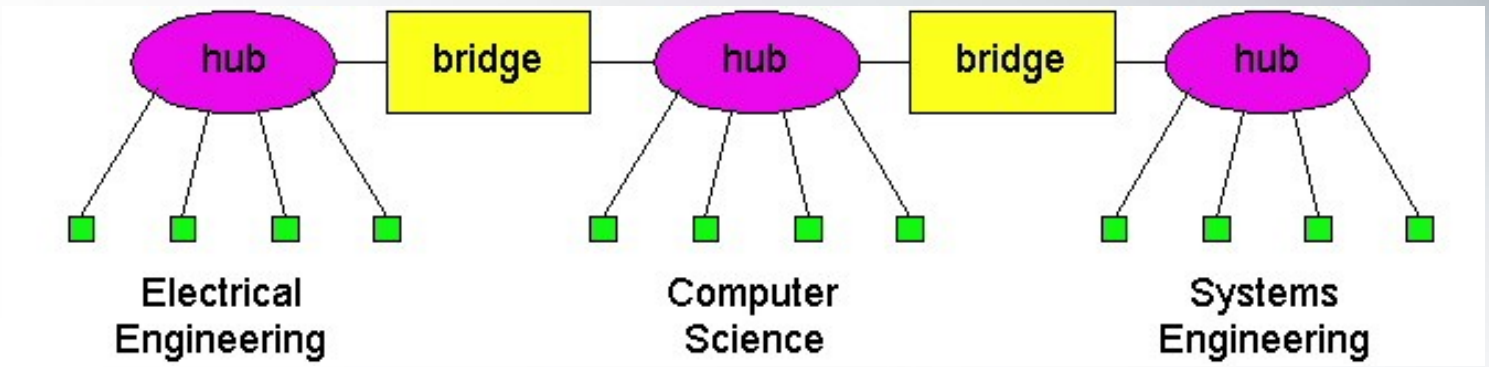
- Bridge receives frame from C
  - –
  - –
- frame received by D

Bridge Learning: example



- D generates frame for C, sends
- bridge receives frame
  - _
  - _

Interconnection without backbone

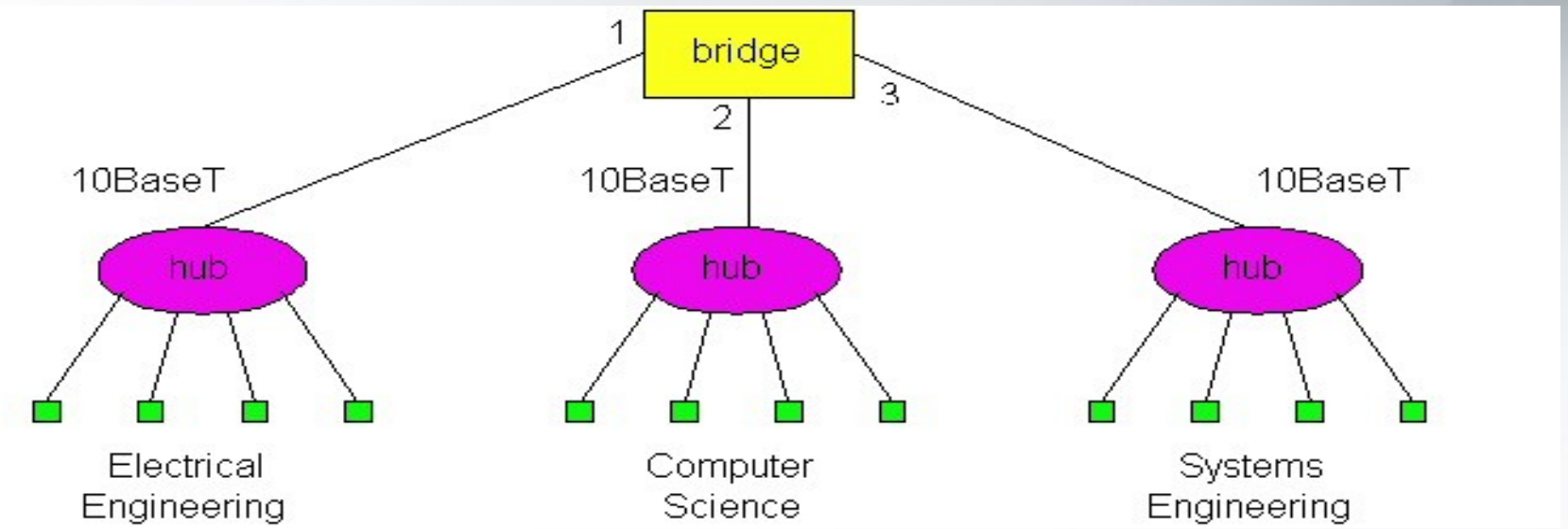


- Not recommended for two reasons:

- single point of failure at Computer Science hub

- all traffic between EE and SE must pass through the CS segment

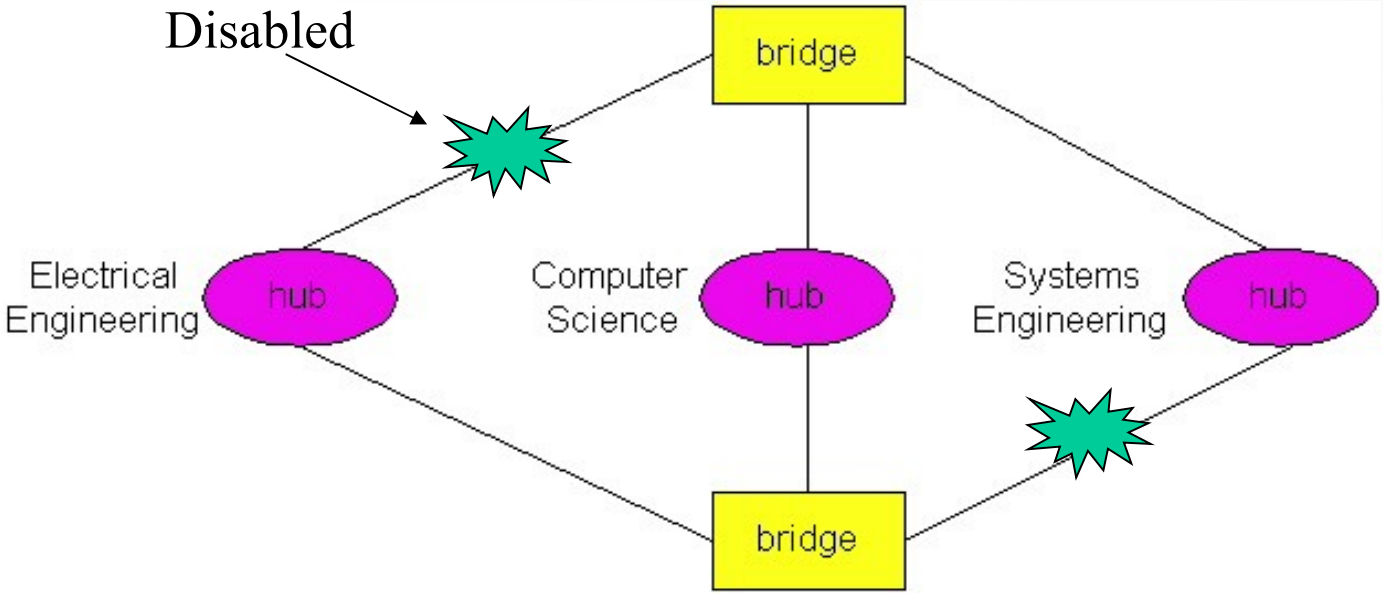
Backbone configuration



Recommended !

Bridges Spanning Tree

- ***Context***: for increased reliability, desirable to have redundant, alternative paths from source to destination
- ***Problem***: with multiple paths, cycles result - bridges may multiply and forward frame forever
- ***Solution***: organize bridges in a *spanning tree* by disabling subset of interfaces

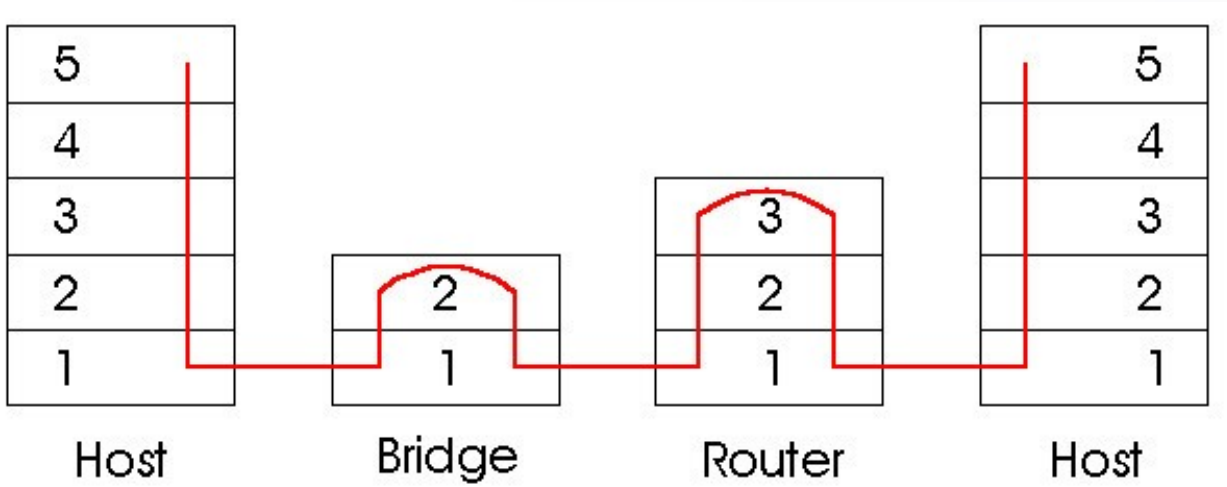


Some bridge features

- Isolates collision domains resulting in higher total maximum throughput
- limitless number of nodes and geographical coverage
- Can connect different Ethernet types
- Transparent (“plug-and-play”): no configuration necessary

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 bridge tables, implement filtering, learning and spanning tree algorithms



Routers vs. Bridges

Bridges + and -

+ Bridge operation is simpler requiring less packet processing

+ Bridge tables are self learning

- All traffic confined to spanning tree, even when alternative bandwidth is available

- Bridges do not offer protection from *broadcast storms*

Routers vs. Bridges

Routers + and -

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

+ provide protection against broadcast storms

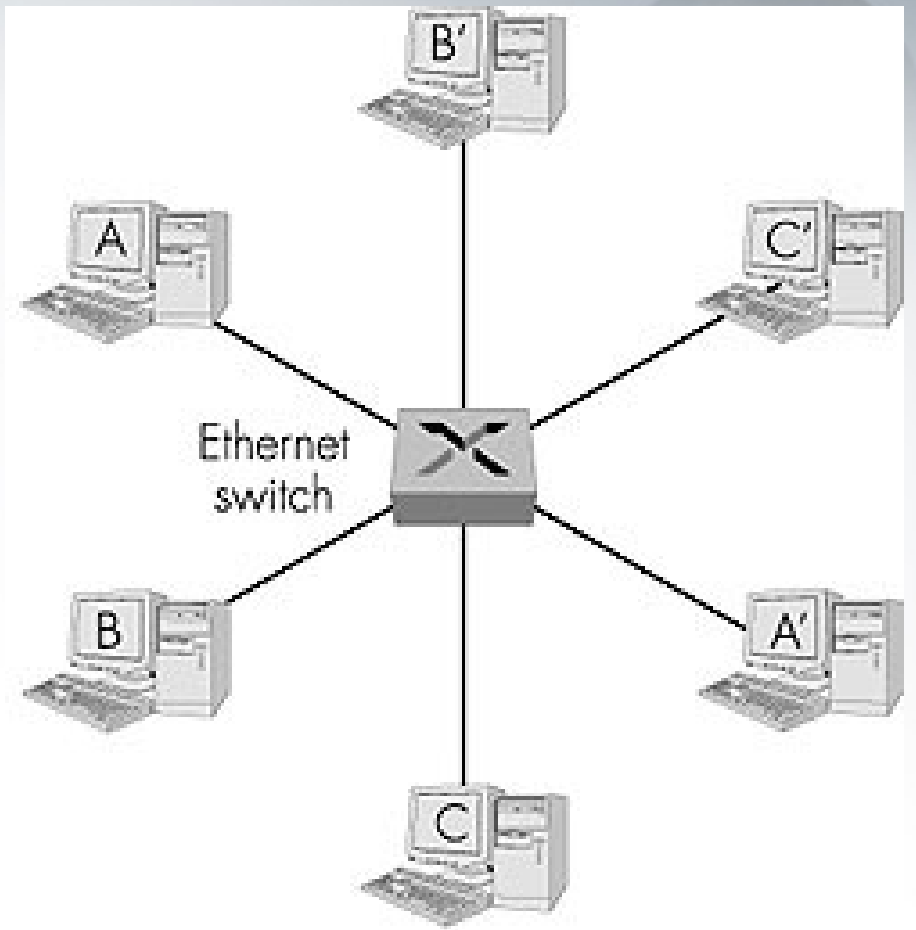
- require IP address configuration (not plug and play)

- require higher packet processing

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

Ethernet Switches

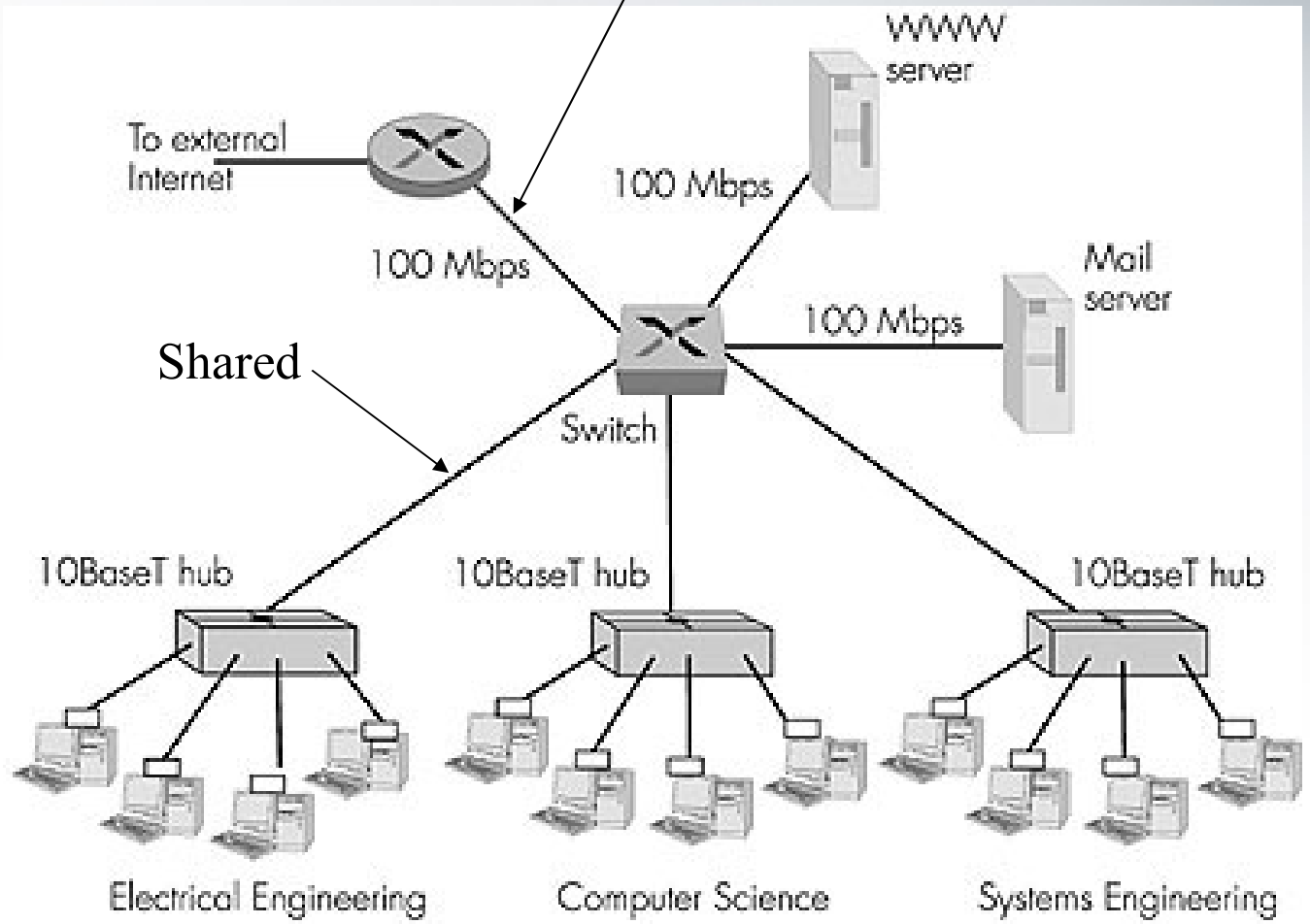
- Essentially a multi-interface bridge
- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-A' and B-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!



Ethernet Switches

- cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- Store-N-Forward switching: frame buffered completely and error-checked (via CRC) before being forwarded.

A typical LAN (IP network)



Summary comparison

	hubs	bridges	routers	switches
traffic isolation	no	yes	yes	yes
plug & play	yes	yes	no	yes
optimal routing	no	no	yes	no
cut through	yes	no	no	yes

Outline

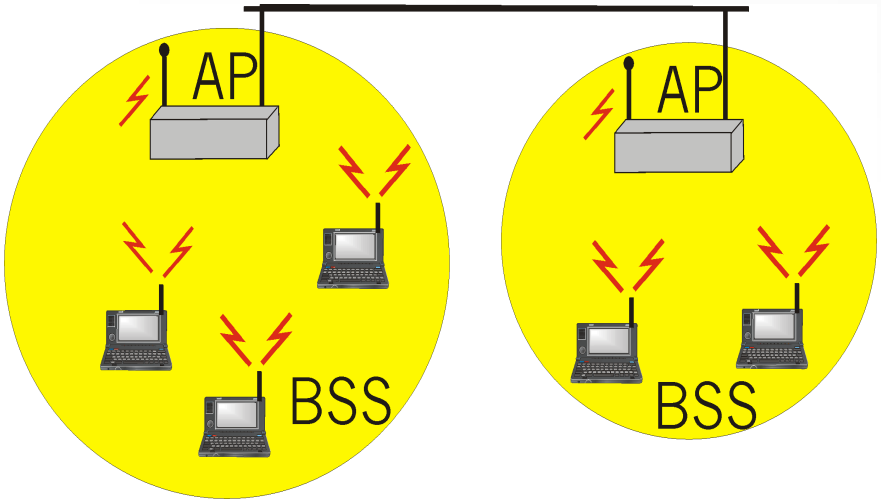
- Introduction and services
- Error detection and correction
- Multiple access protocols
- LAN addresses and ARP
- Ethernet
- Hubs, bridges, and switches
- **Wireless links and LANs**
- PPP

IEEE 802.11x Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed radio spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
  - widely deployed, using base stations
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- All use CSMA/CA for multiple access
- All have base-station (infrastrusture) and Ad-hoc network versions

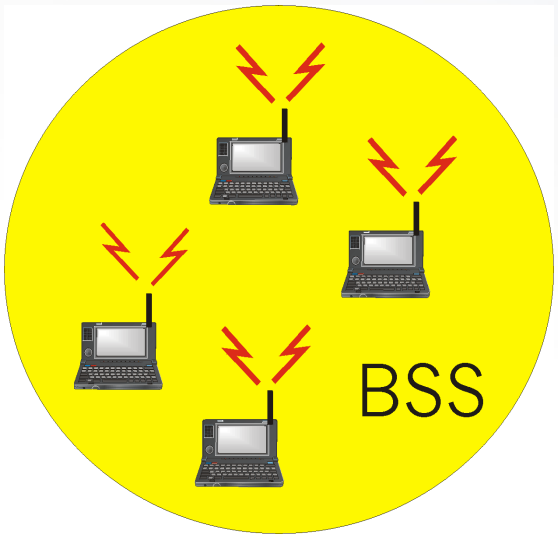
Base station approach

- Wireless host communicates with a base station
- Basic Service Set (BSS) (a.k.a. “cell”) contains:
  - wireless hosts
  - access point (AP): base station
- BSS’s combined to form distribution system (DS)



Ad Hoc Network approach

- No AP (i.e., base station)
- wireless hosts communicate with each other
  - to get packet from wireless host A to B may need to route through wireless hosts X,Y,Z
- Applications:
  - “laptop” meeting in conference room, car
  - interconnection of “personal” devices
  - battlefield
- IETF MANET (Mobile Ad hoc Networks) working group



A word about Bluetooth

- Low-power, small radius, wireless networking technology
  - 10-100 meters
- Omni-directional
  - not line-of-sight like IrDA
- Interconnects gadgets
- 2.4-2.5 GHz unlicensed radio band
- up to 721 kbps

- Interference from wireless LANs, digital cordless phones, microwave ovens:
  - frequency hopping helps
- MAC protocol supports:
  - error correction
  - ARQ
- Each node has a 12-bit address

Outline

- Introduction and services
- Error detection and correction
- Multiple access protocols
- LAN addresses and ARP
- Ethernet
- Hubs, bridges, and switches
- Wireless links and LANs
- **PPP**

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. dial-up 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 non-requirements

- no error correction/recovery
- no flow control
- out of order delivery OK

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 (e.g. PPP-LCP, IP, IPCP, etc)
- info: upper layer data being carried
- check: cyclic redundancy check for error detection