Applied Networks & Security

Wired Local Area Networks (LANs)

http://condor.depaul.edu/~jkristof/it263/

John Kristoff
jtk@depaul.edu

Local Area Network (LAN)

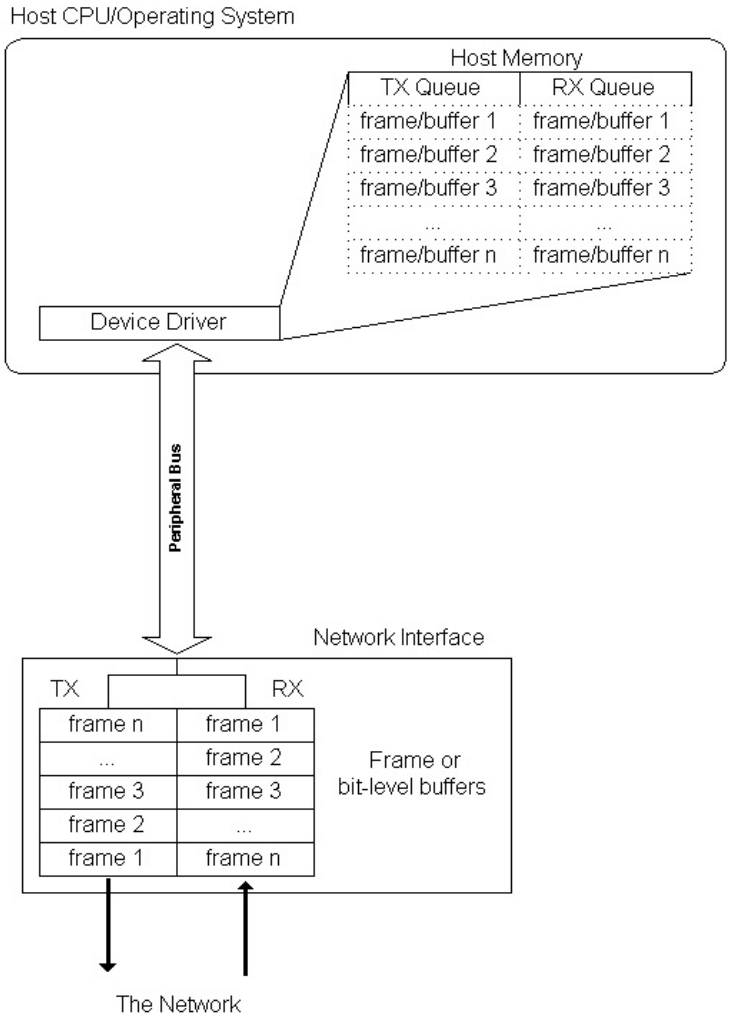
- LAN can be a difficult term to define
- Generally speaking...
  - Most computers have a LAN link interface
  - Ethernet, by far, most popular link technology
  - Good capacity, measured in Mb/s minimally
  - Most LAN links cover short distances
  - Historically shared medium access
    - Increasingly less true today

Cabling demonstration

- Let's look at and talk about some basic cabling, connectors and installation practices
- If you're just looking at these slides outside of class with no video, well, you should have been here

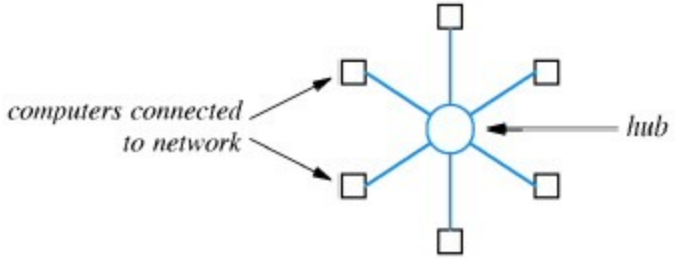
The data link interface

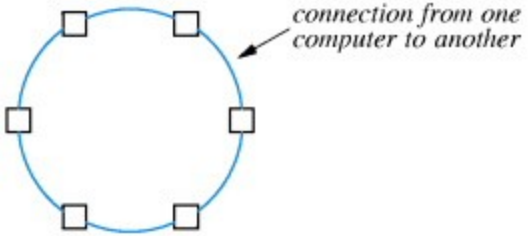
I don't remember where I swiped this diagram from :-(

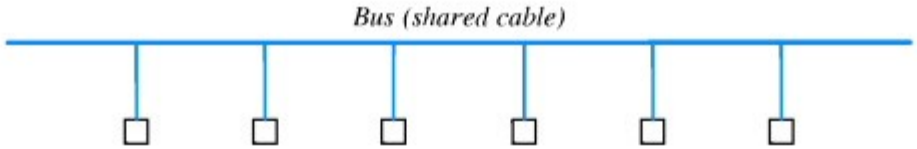


Physical (and logical) topologies

diagrams courtesy of http://www.netbook.cs.purdue.edu







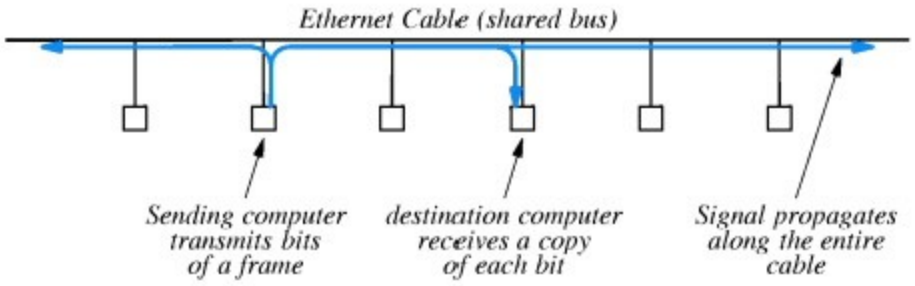
Ethernet

- Most popular link technology by far
- IEEE standardized as IEEE 802.3
- Several generations and updates
  - Mostly same frame format
  - Updates mainly to increase transmission rate
  - Physical layer requirement changes as needed

Ethernet transmission

diagram courtesy of http://www.netbook.cs.purdue.edu

- One station successfully transmits at a time
- Signal propagates the entire cable length (bus)
- All stations receive all transmissions
- CSMA/CD medium access control



CSMA/CD

- Carrier sense (CS)
  - Wait until channel is idle, then transmit
- Multiple access (MA)
  - All stations on channel use same MAC protocol
- Collision detection (CD)
  - Listen to medium while transmitting
  - Detect if another station transmits simultaneously
  - If collision, enter back-off algorithm

Exponential back-off algorithm

- Sending station backs-off after collision is detected
- Let 1 slot time = 512 bit times (64 byte min. frame)
- Upon 1st collision, randomly choose {0,1} slot delay
- Upon 2nd collision, randomly choose {0,1,2,3}
- Choose from [0 to 2^n–1], N=transmission attempt
- Up to a maximum of 16 retransmission attempts
- And up to a maximum of 1023 * slot delay time
- Give up after 16 retransmission attempts
- Capture effect: brief, unfair advantage for busy sender, in practice a non-problem

Collision domain

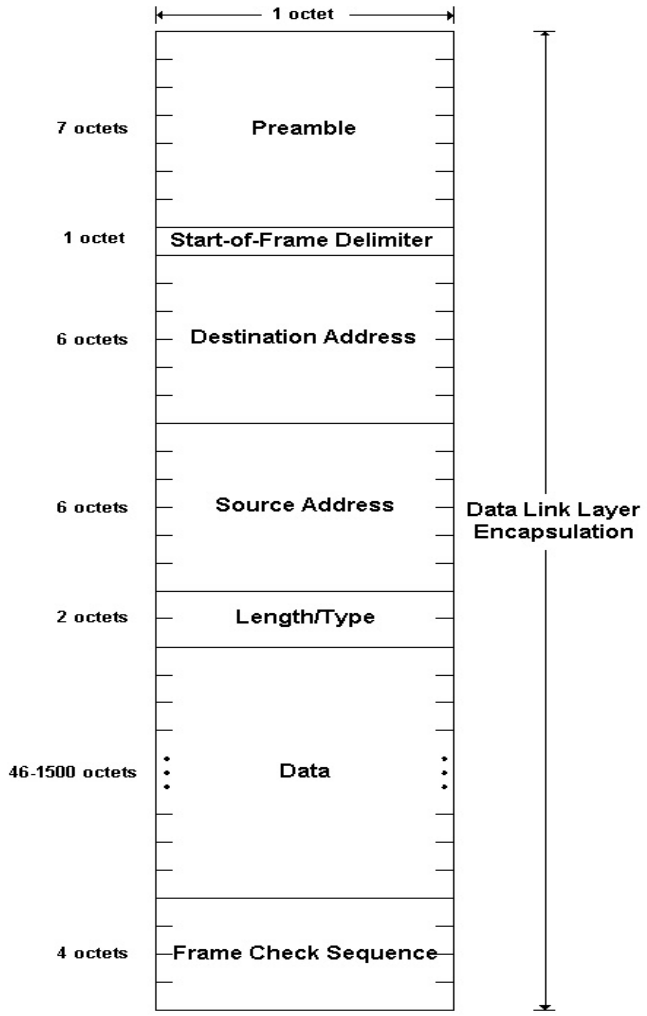
- Min length frame must be >= than the maximum round trip time (RTT) of the entire ethernet segment
- Must hear collision before transmission completes
- Historically minimum frame was 512 bits (64 bytes)
  - Requires 46 payload bytes, pad if unavailable
- Cabling distance decreases as speed increases
- Use of full-duplex removes collision domain restriction

Are collisions bad?

- Collision stats are usually meaningless
  - Unless the collisions are late
  - Or you see them on full-duplex links
- Collisions are an efficient arbitration scheme
- Collisions resolved and detected within the round trip time (RTT) of the channel (that is, quickly), stations do not finish their frame transmissions
- Short answer, no, collisions usually aren't bad

Ethernet frame format

- Sender fills in:
  - It's own src address
  - Target dst address
  - Type (next protocol)
  - Payload
  - Calculated FCS



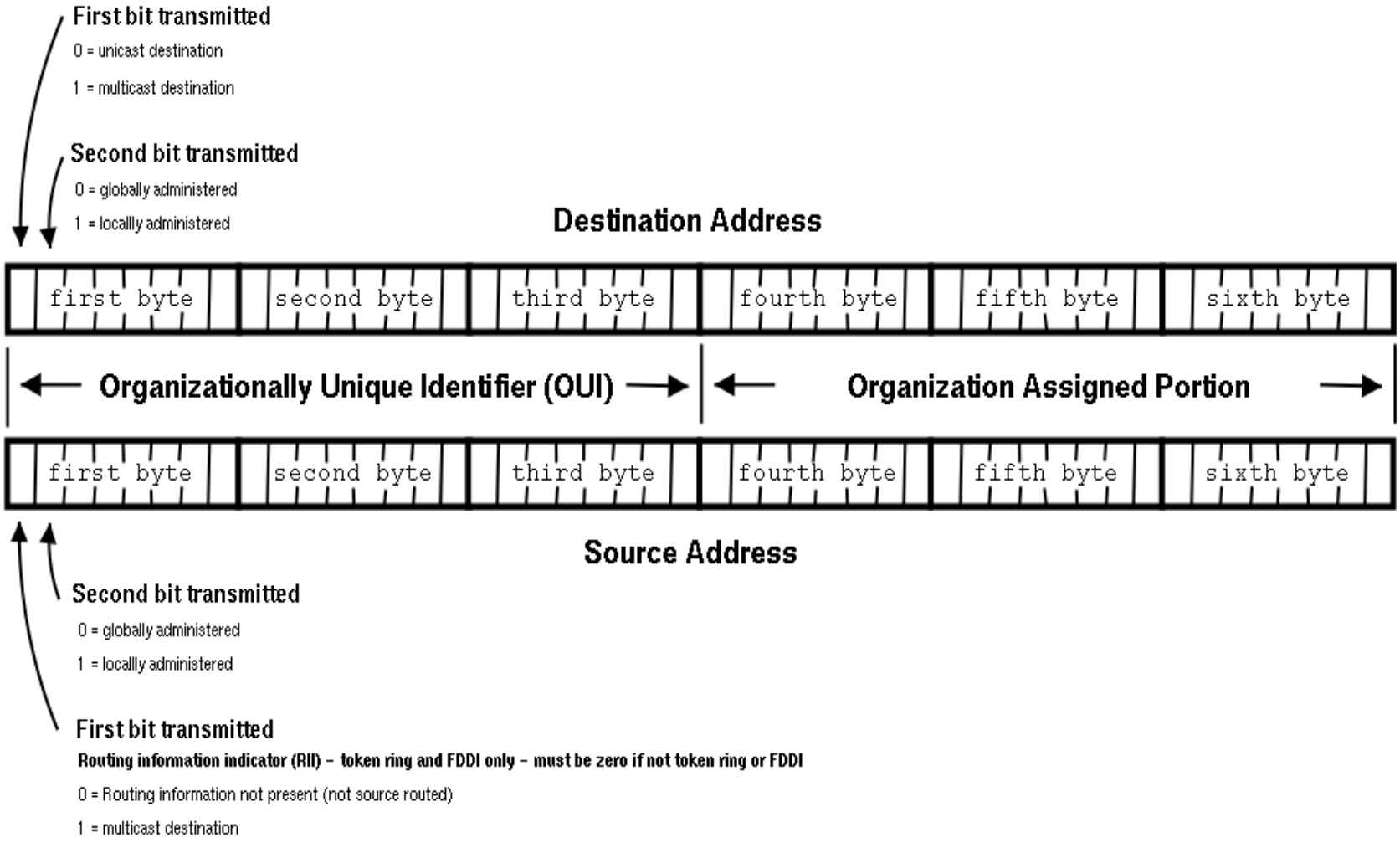
Promiscuous mode

- Interface accepts all frames regardless of destination address
- Useful for debugging
- Available on most wired adapters, some wireless chipsets do not support it

Ethernet addressing

- IEEE standard address is 48 bits long
- Written as 12 hexadecimal digits (e.g. ff:ff:ff:ff:ff:ff)
- Also known as:
  - Layer 2 address
  - Hardware address
  - MAC address
  - Data link address

Visualizing ethernet addresses

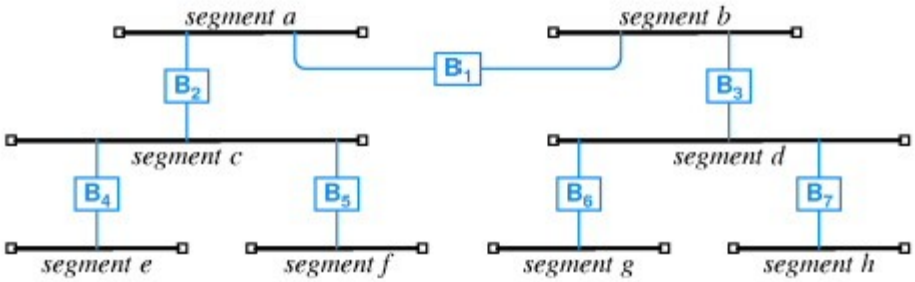


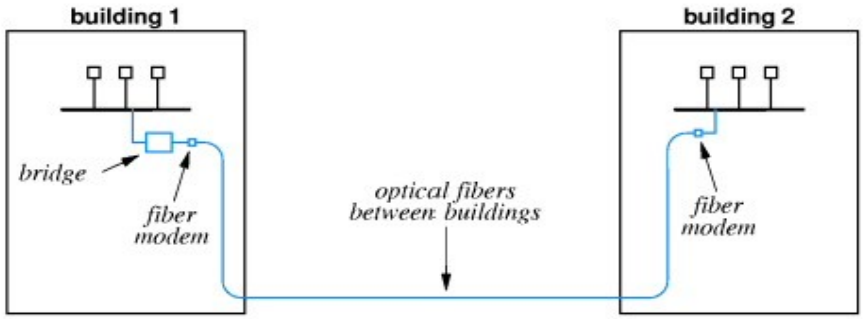
Why bridge?

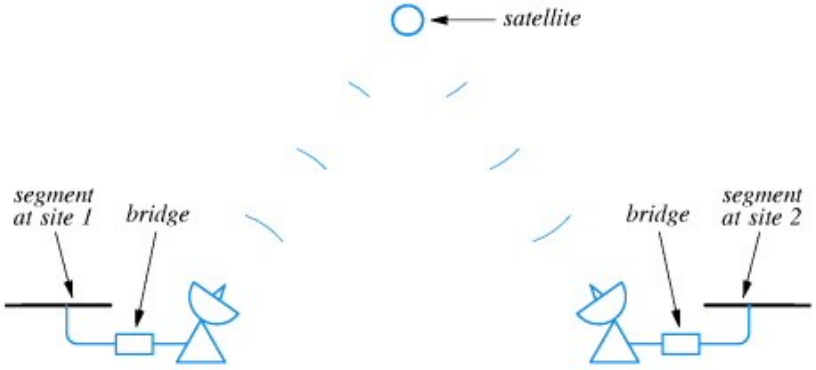
- LANs may have physical distance limitations
- Limitation on the number of hosts per LAN
- Allocate more capacity per station
- Contain traffic to local LAN segment
- Accommodate hosts with no layer 3 protocol
- Support any layer 3 protocol
- Connect dispersed LANs together

Visualizing bridges

diagrams courtesy of http://www.netbook.cs.purdue.edu



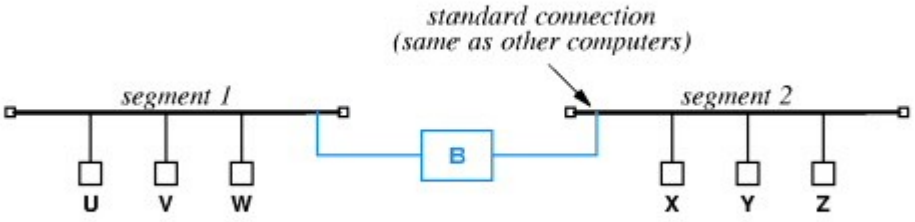




Transparent bridging

diagram courtesy of http://www.netbook.cs.purdue.edu

- Bridge listens to each interface promiscuously
- Bridge inspects layer 2 information
- Forward frames to other interfaces if necessary

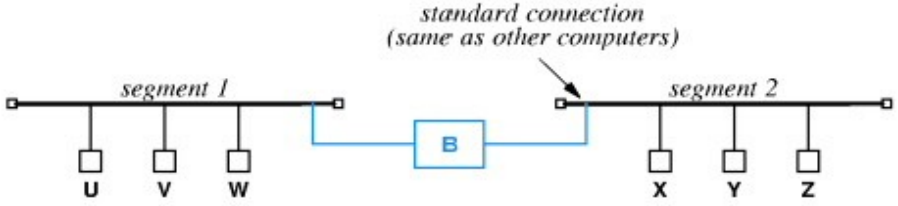


Bridge forwarding and filtering

- Receive a frame on an ingress interface
- Inspect destination address
- If multicast/broadcast, forward to all except incoming (ingress) interface
- Query address table (cache) for destination address
  - If found, forward out (egress) associated port
    - Except when ingress = egress, just drop it
  - If not found, flood to all interfaces except the incoming (ingress) interface

Source address learning

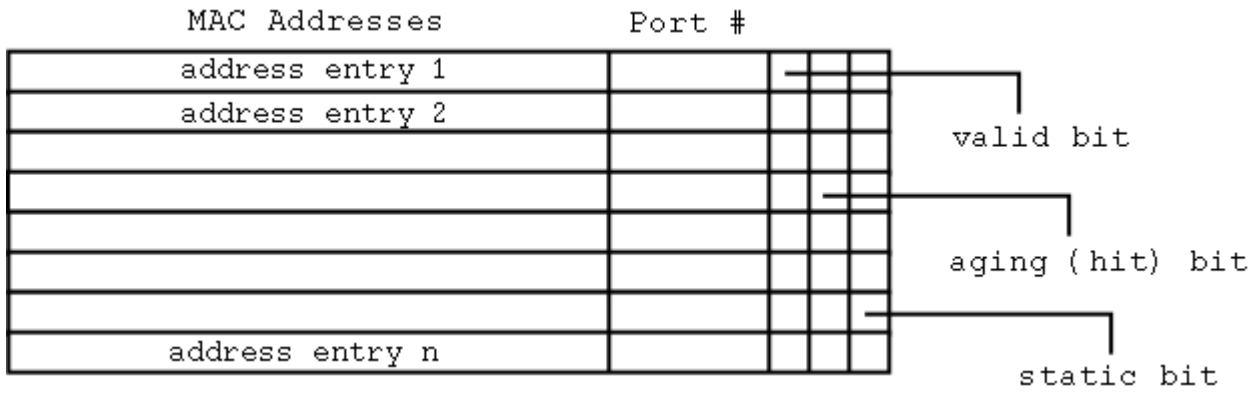
- Bridge listens promiscuously on all interfaces
- Store source address and associated ingress interface port in address table (cache)



Event	Segment 1 List	Segment 2 List
Bridge boots	–	–
U sends to V	U	–
V sends to U	U, V	–
Z broadcasts	U, V	Z
Y sends to V	U, V	Z, Y
Y sends to X	U, V	Z, Y
X sends to W	U, V	Z, Y, X
W sends to Z	U, V, W	Z, Y, X

Bridge table (cache) entry aging

- Low-priority or non-time critical operation
- Allows station mobility and small table size
- Aging process periodically clears the H bit
- If H bit is clear, clear the V bit
- If H and V bits are clear, remove the table entry



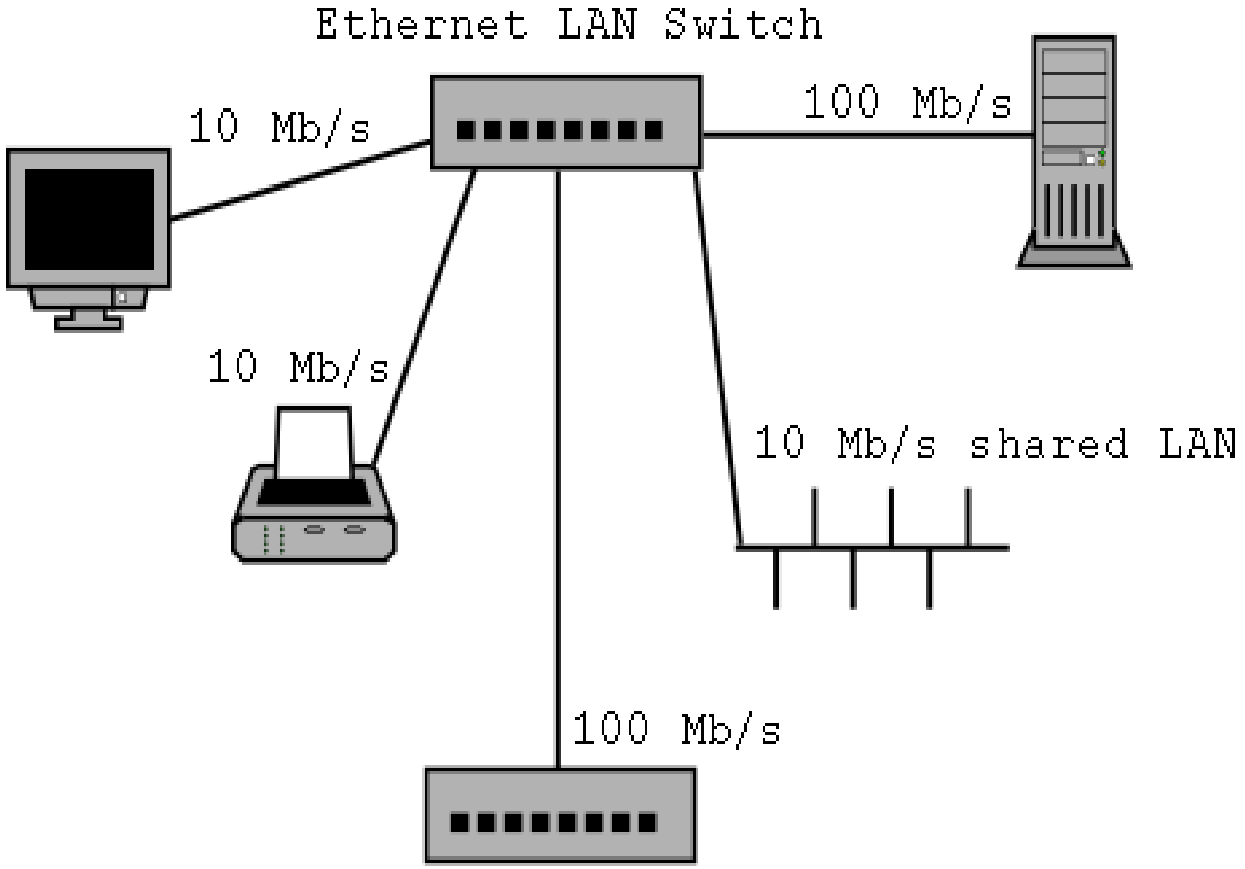
LAN switches

- LAN switches = LAN bridges
- Switches imply newer, better, faster, bigger, etc.
- Switching is a successful marketing term
- Often used to further segment shared LANs
- Switch port per device/customer becoming the norm
- Most LAN switches are relatively simple and cheap

Why switch?

- Reduce/remove shared medium contention
- Maximize aggregate capacity
- Extend distance limitations
- Data rate flexibility

Visualizing LAN switches



Store and forward switching

- Completely receive frame on ingress port
- Check frame check sequence (FCS) for validity
- Perform address learning
- Make forwarding/filtering decision

Cut-through switching

- Begin making forwarding decision as soon as you get the destination address (do not wait for the entire frame)
- Goal is to improve switch latency
- More successful marketing

Cut-through switching fallacies

- Latency only improves if outgoing (egress) port is free, this is not when you need the improvement
- Switch latency is the least of your problems
- Multicast/broadcast cut-through too?
- Input (ingress) and output (egress) port rate must match
- Propagates errors (but generally not a problem)
- Store-and-forward is usually the default (good choice)

LAN switch configurations

- Bounded/stand-alone
- Stack-able
- Chassis