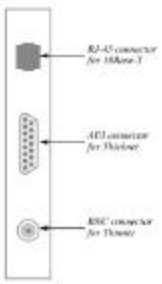
# More on LANS

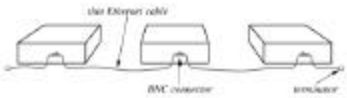
Chapters 10-11

# LAN Wiring, Interface

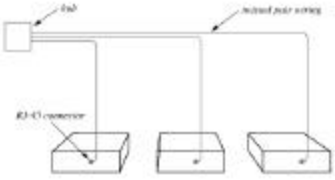
- Mostly covered this material already
  - NIC = Network Interface Card
    - Separate processor, buffers incoming/outgoing data
    - CPU might not be able to keep up network speeds!
    - Distributes processing to avoid overburdening CPU
    - Typically has DMA access
  - Wiring
    - ThickNet – 10Base5 ; Thick coax cable
    - ThinNet – 10Base2 ; "Thin" coax cable
      - Use BNC connectors, "T" connectors for bus
    - 10BaseT, 100BaseT ; Twisted Pair
      - Use central hub



## ThinNet



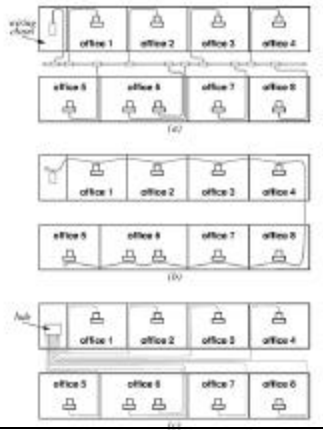
## 10BaseT



# Comparison of Wiring Schemes

- 10Base2
  - Separate transceiver allows computer to be powered off or disconnected from network without disrupting other communication
  - Transceiver may be located in an inconvenient place
  - Finding malfunctioning transceiver can be hard
  - Thin coax takes minimum of cable
  - Disconnecting one computer (or one loose connection) can disrupt entire network
- 10BaseT
  - Hub wiring centralizes electronics and connections, making management easier
  - Easier to pull cable
  - Bottom line - 10Base-T most popular because of cost

# Wiring Schemes



## Extending LANs

- LANs were designed with constraints of speed, distance, cost, and usage
  - Typical distance = 100 to 500 meters
  - CSMA/CD optimal with bursty traffic
  - Works best to connect computers in a single floor or building
- Possible to improve on LAN performance
  - Scale up to larger amounts of traffic
  - Extend to connect computers across longer distances

## LAN Distance

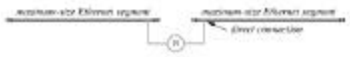
- Length of medium affects strength of electrical signals and noise immunity
- LANs use shared medium - Ethernet, token ring
  - Length of medium affects consistency and fair, shared access to medium
    - Token passing - circulation time for token increases with long cable
    - CSMA/CD –with minimum frame size, if propagation delay too long we won't detect collision while transmitting
- Standards set a maximum distance for LANs
  - 100 meters for UTP
  - 200 to 500 meters for coax
- Can extend distances with fiber optic connections
  - Install a fiber modem from computer to transceiver, perhaps in a different building

# Fiber Modems

- Fiber modems
  - Convert Ethernet signals to digital signal for fiber
  - Transmit digital signals via fiber optic cable to other modem
  - Most often used to connect two LANs - typically through a bridge - different buildings
  - Fiber is a good choice due to low latency and high bandwidth
  - Extending distance from interface to physical layer

# Repeaters

- May want to extend LAN medium
  - Ethernet - timing constraints allow longer medium
  - Signal strength constraints limit length
- *Repeater* – simplest form is a bidirectional, analog amplifier that retransmits analog signals
  - Simply copy signals between segments; includes noise/collision
  - Do not understand frame formats or addresses
    - Not the case with digital repeaters
  - Hub acts as a repeater
- One repeater can effectively double the length of an LAN s



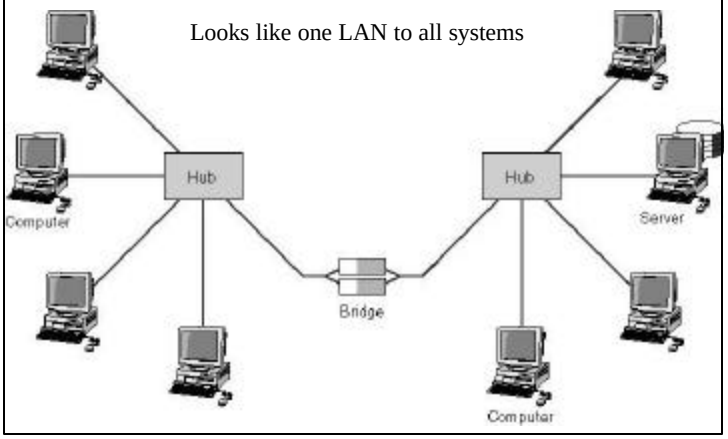
## Limits on Repeaters

- Can't extend Ethernet with repeaters indefinitely
- CSMA/CD requires low delay; if medium is too long, CSMA/CD won't work
  - Run into the problem of not being able to detect collisions while transmitting the frame
- Ethernet standard includes limit of 4 repeaters between any two Ethernet stations
- Reasons for limitations
  - Ethernet was designed to connect a floor of a building, or a couple floors, but not across wider distances
  - Will need to go to routers to cross larger distances (connect two separate LANs)
- Aside from hubs, **bridges** are used today in favor of repeaters

## Bridges

- Bridges operate **transparently** at the data link layer. They connect two LAN segments that use the same data link and network protocol. They may use the same or different types of cables although generally the media is the same.
- Bridges "learn" whether to forward packets, and only forward those messages that need to go to other network segments.

# Bridges



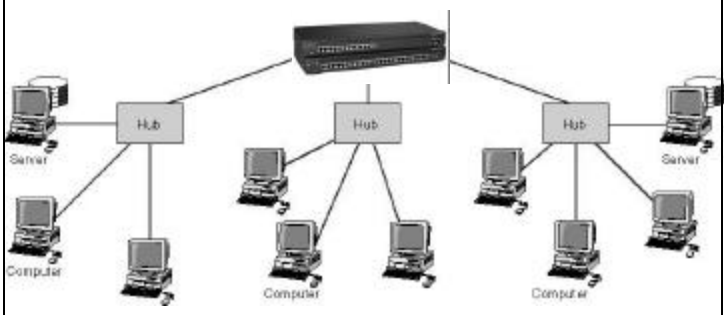

# Bridges

- Bridges are a combination of both hardware and software, typically a “black box” that sits between the two networks, but can also be a computer with two NICs and special software.
- Bridges can perform filtering and can be used to segment a LAN as we will see in a moment

# Switches

- Like bridges, switches operate at the data link layer (generally). Switches connect two or more computers or network segments that use the same data link and network protocol. They may connect the same or different types of cable.
- Incoming frame switches to appropriate outgoing line
- Most switches enable all ports to be in use simultaneously, making them faster than bridges.
  - Unused lines can also be used to switch other traffic
  - Ex: with two pairs of lines in use, overall capacity is now 20Mbps instead of 10Mbps
- Switches are currently the hot thing in LANs!

# Switches



## Switched Hubs

- No change to software or hardware of devices
- Each device has dedicated capacity
- Scales well

- Store and forward switch
  - Accept input, buffer it briefly, then output
- Cut through switch
  - Take advantage of the destination address being at the start of the frame
  - Begin repeating incoming frame onto output line as soon as address recognized
  - May propagate some bad frames

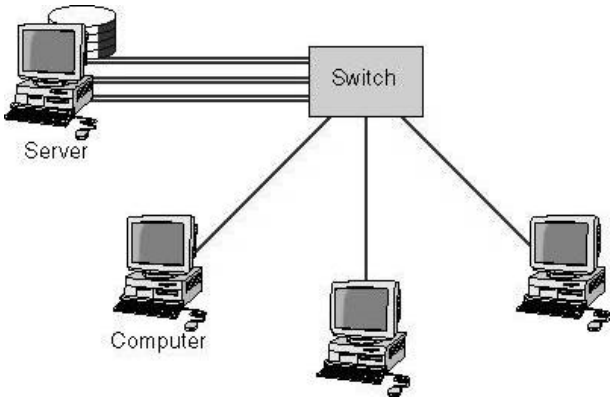
- How do switches know which input line to connect to which output line?

## Switched Ethernet

Other solutions include to speed up server access:

- Full Duplex Ethernet - full duplex over traditional 10BaseT.
- 10/100 Switched Ethernet (combines 10Base-T and 100Base-T). This is often used to provide 10 Mbps to the clients and 100 Mbps to the server.

## Full Duplex Ethernet




## Intel Express 460T Switch – about $800

- ***24 Ports***
- ***Auto-negotiating 10/100 Ports***
- ***Auto-configuration***
- ***Built-in management via web browser***
- ***Expansion modules***— Extend with the 100Base-FX expansion module or uplink to Gigabit Ethernet
- ***IGMP Snooping***— Reduce congestion when multicasting traffic to multiple desktops.
- ***Wire-speed performance***— Each user receives dedicated 100Mbps full-duplex performance even during high traffic bursts.

## Bridges

- Ability to expand beyond single LAN
- Provide interconnection to other LANs/WANs
- Use Bridge or router
- Bridge is simpler
  - Connects similar LANs
  - Identical protocols for physical and link layers
- Router more general purpose
  - Interconnect various LANs and WANs
  - Can even change data link protocols (but same network protocol)
  - see later

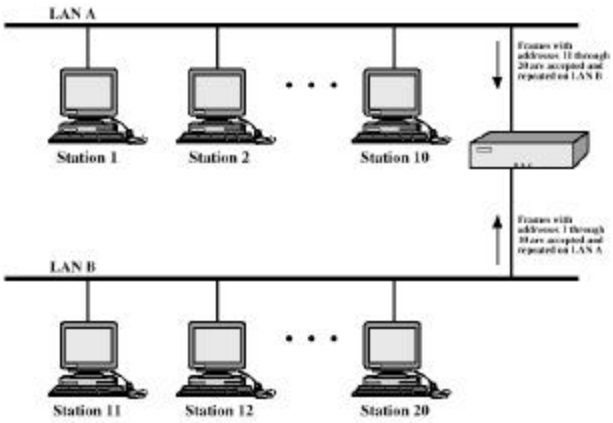
## Why Bridge?

- Reliability
  - Partition network into self-containing units
- Performance
  - Cluster internetworks together, performance decreases as the number of devices on the wire increases
- Security
  - Can keep different traffic (e.g. accounting, strategic planning) on different networks
- Geography
  - Need a way to support networks in two different locations, could use a bridge to link them

## Functions of a Bridge

- Bridge interfaces are promiscuous and read all packets
- Collisions aren't forwarded meaning:
  - Network isolation
- Bridges learn which packets belong to which side
  - More network isolation
- Bridges have a spanning tree algorithm with own link-layer protocols, dynamically forms a tree to prevent loops – allows redundant bridges

## Bridge Operation



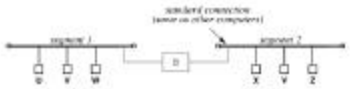
## Bridge Learning Algorithm

- Receive some data packet on some input port
- Look at the packet's source MAC address. If it's not a broadcast or multicast address then:
  - Lookup address in internal lookup table
  - If not in the table, store it in the table using the address and the port it is on
  - If it is in the table, change the entry if it's on a different port

## Bridge Forwarding Algorithm

- Receive some data packet on some input port
- Look at the packet's destination MAC address.
  - If it's a broadcast or multicast address then forward it to the other port
  - Lookup destination address in internal lookup table
  - If not in the table, forward it to the other port
  - If it is in the table
    - If the destination address is on the same segment as the input segment, discard the packet
    - Otherwise, forward the packet to the other port

## Bridge Operation Example

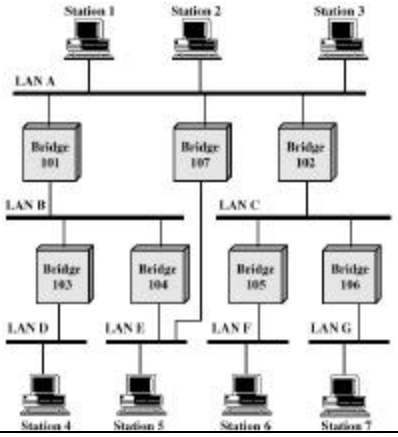


| Event | Segment 1 List | Segment 2 List |
|---|---|---|
| Bridge boots | – | – |
| U sends to V | U | – |
| V sends to U | U, V | – |
| Z broadcasts | U, V | Z |
| Y sends to V | U, V | Z, Y |
| Y sends to X | U, V | Z, Y |
| X sends to W | U, V | Z, Y, X |
| W sends to Z | U, V, W | Z, Y, X |

## Bridge Protocol Architecture

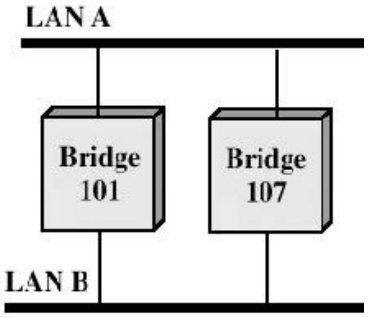
- IEEE 802.1D
  - Pretty complex, IEEE spec 378 pages long
- MAC level
  - Station address is at this level
- Bridge does not need LLC layer
  - It is relaying MAC frames

## Multiple LANs




## Multiple Bridges

- Anything wrong with this picture?



## Bridge Routing

- Complex large LANs need alternative routes
  - Load balancing
  - Fault tolerance
- Bridge must decide whether to forward frame
- Bridge must decide which LAN to forward frame on
- Fixed Routing - Routing selected for each source-destination pair of LANs
  - Done in configuration
  - Usually least hop route
  - Only changed when topology changes

## Spanning Tree

- Bridge automatically develops routing table
- Automatically update in response to changes

- Done by constructing a spanning tree
- For any connected graph there is a spanning tree that maintains connectivity but contains no closed loops
- Each bridge assigned unique identifier (MAC address), used to identify other bridges in the tree
- Initially block normal data traffic, exchange BPDU (bridge protocol data units) between bridges to establish spanning tree

## Switches and Bridges?

- Most switches (at least store-and-forward) also act just like a bridge
  - Segments traffic
  - Typically implements spanning tree algorithm
  - Has more ports than a bridge