# Switching

- Introduction
  - Technologies
  - Why bridges
- Bridges
  - Between different LANs
  - Transparent bridges
  - Spanning tree bridges
  - Remote bridges
- Virtual LANs

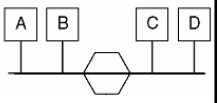




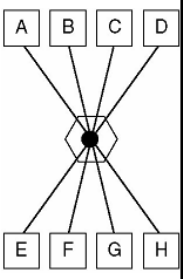


# Repeaters, & Hubs

- Repeater
  - Task: Amplify the signal
  - Layer: Physical Layer
  - Process Volts

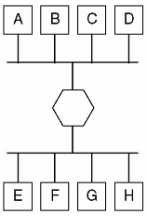



- Hub
  - Task: Join all the cables electrically
  - Layer: Physical Layer
  - Process Volts

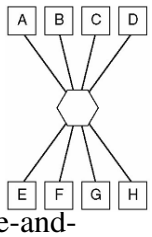


# Bridges & Switches

- Bridges
  - Task: Connect two or more LANs
  - Layer: Data Link Layer
  - Process Frames




- Switches
  - Task: Similar to a bridge but connects individual stations
  - Layer: Data Link Layer (Frames)
  - Process Frames
  - Cut-through switches and rarely used store-and-forward switches which read entire frames and then forward them to the relevant location.









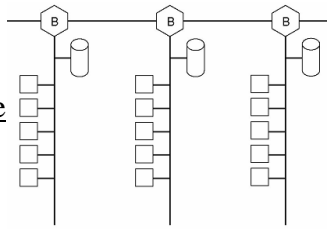

# Routers & Gateways

- Routers
  - Task: Route incoming packets
  - Layer: Network Layer
  - Process Packets

- Gateways
  - Task: Translate/reformat different transport (e.g., TCP <-> ATM) or application layer (e.g., email <-> SMS)
  - Layer: Both Transport and Application Layers

# Why bridges?

- History : Interconnection between large organisations (e.g., Corporations, Universities)
- Geographical spread…
  - Cost: It is cheaper to buy several LANs and connect them
  - Overall distance: Would be above what allowed by the LAN standard (2.5km for 802.3)
- Overall load
  - Restrict traffic locally
- Reliability: If one LAN exhibits problems, it does not effect the other LANs,
- Security: Bridges allow for reduction in the potential for sensitive information being snooped off the network



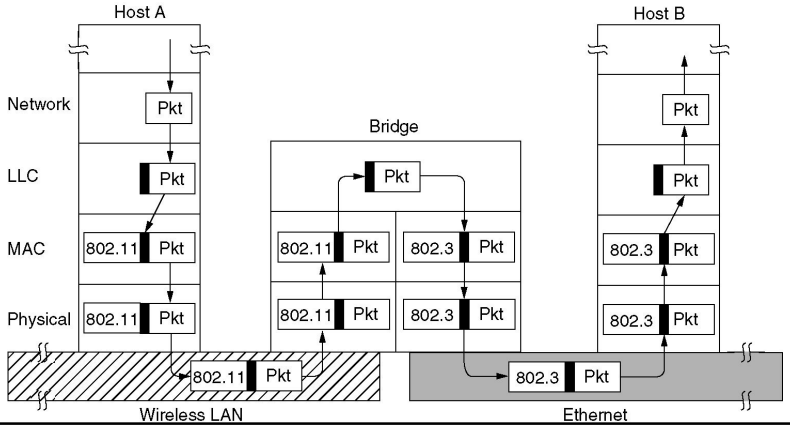






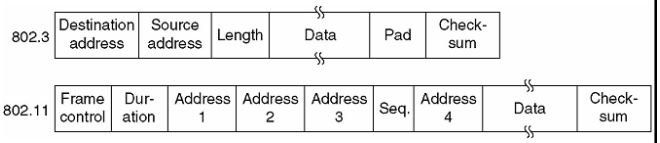

# 802.x to 802.y bridges

- Packet in Host A
- LLC header at the LLC layer
- MAC header is added by the 802.11 protocol, striped off by the bridge and put on a 802.3 (Ethernet) header



# Problems

- Different formats
  - Meaning of fields? Some fields (e.g. duration in 802.11) have no meaning in 802.3
  - CPU time: Reformatting and new checksum need CPU time




- Buffering:

LANs connected by the bridge may operate at very different speeds,

- Security:

802.11 supports encryption but 802.3 (ethernet) does not.

- Quality of Service:

Some QoS is provided by the PCF in 802.11, which is lost when traffic is transferred to ethernet.

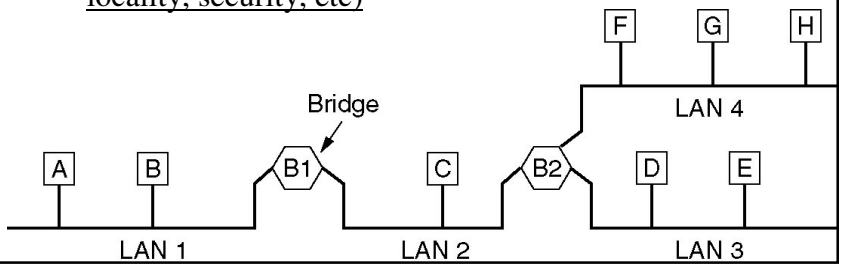






# Setting up bridges

- Connecting bridges
  - We would like to just plug and play
  - But initially routing tables are empty
- Use Promiscuous mode?
  - Send everything everywhere
  - Pros & Cons: We guarantee that all frames go to destination but we lose the advantage of a bridge (traffic locality, security, etc)



# Transparent bridges

- Start in promiscuous mode
- Learn routings from frames which pass,
  - Backward learning: Learn which LAN a frame comes from, route frames to that destination on that LAN.
- Routing logic
  - $LAN_{Destination} = LAN_{Source}$ Do nothing
  - $LAN_{Destination}$ != $LAN_{Source}$ Forward the frame on the relevant LAN,
  - $LAN_{Destination}$ unknown use flooding
- Dynamic topologies? What happens when stations move between LANs
  - Maintain times: routing table holds the last time a frame was received from a station,
  - Purge old entries: if no frame is received for some period of time

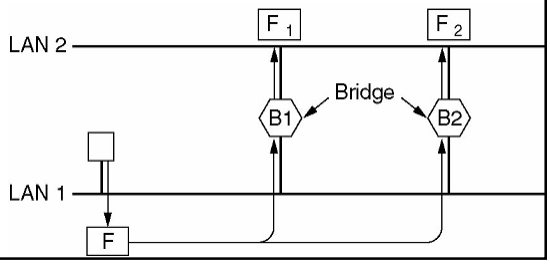






# Parallel Bridges

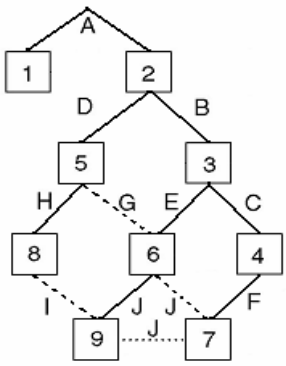
- Reliability:
  - Multiple paths from one LAN to another,
- Example (problem):
  - $F \rightarrow F_1$ and $F_2$
  - $F_1 \rightarrow F_{12}$
  - $F_2 \rightarrow F_{21}$
  - …



# Spanning Tree Bridges



- Solution: Bridges communicate
  - Extract a loop free topology to use
  - Then ignore some of the connections (dotted lines, i.e., G I J J)
  - Pros & Cons: no loops, but there are redundant bridges and traffic travels further for certain destinations




- General Solution: Spanning tree
  - Nominate the root: bridge with lowest serial number
  - Find the shortest paths from root to each bridge and LAN and these paths is the spanning tree

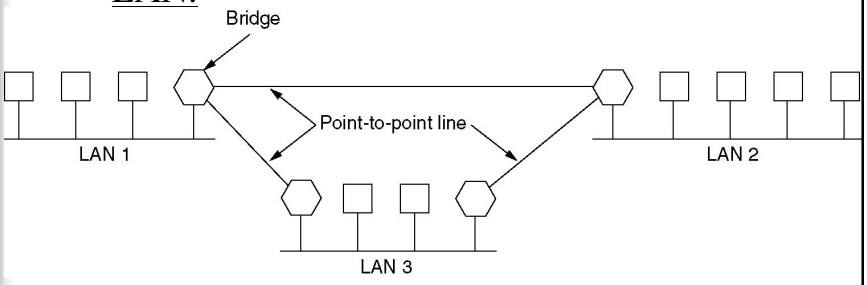




# Remote Bridges



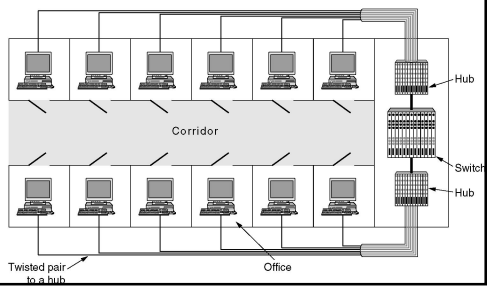
- Remote LANs:
  - Often connected using point-to-point lines
  - To create one large LAN place bridges at each connection-point,
  - Each Point-to-point line is treated as a hostless LAN.



# LAN organisation



- Originally LAN membership was based on physical location
  - LANs based on Multidrop lines
- Want LAN membership based on organisational structure rather than physical layout.
  - This is more feasible due to the use of hubs and switches








# LAN membership issues

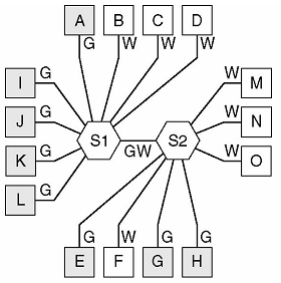


- Security: Who can hear the messages?
- Load: Can we keep the traffic local?
- Broadcasting: Can we cope if stations start broadcasting messages?

- More flexibility needed
  - Pulling out plugs is not a long term solutions
  - What if related users are connected to different wiring closets,
  - How can we react quickly to organisational change
  - Can we solve the problem in software?

# VLANs Virtual LAN

- Decisions:
  - Number of VLANs
  - VLAN members
  - VLAN names




- Based on VLAN aware switches:
  i.e., the switches need to understand the concept of a VLAN
  - VLAN ↔ Port / Line
  - Where traffic is from?
    - Every port => VLAN Only works if all machines on a port belong to the same VLAN,
    - Every MAC address => VLAN Possible to mix VLANs on a physical LAN
    - Every IP address => VLAN Violates layer independence







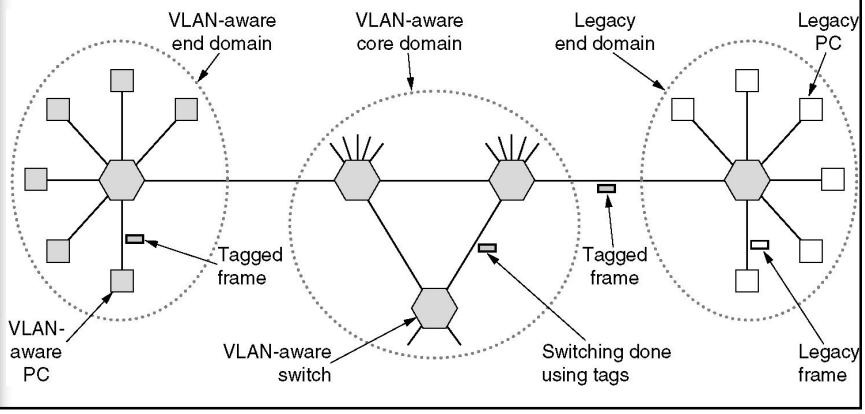
# Identifying Payload

- Which VLAN? We need to identify the VLAN of the frame, rather than the sender's VLAN
  - Frame header? Identify the VLAN in the frame header
- Solution
  - 802.1Q – Change the Ethernet frame format!
- Problems
  - Throw away all existing Ethernet cards? No, it is the switches and bridges that use the new format
  - If not, who generates the fields? They can be added by the 1st switch/bridge and stripped off by the last one,
  - What if a frame is already at max. size. IEEE changed the max size very slightly to allow for the new fields

# Transition to 802.1Q



- Legacy and VLAN aware MUST WORK TOGETHER
  - End domains can be VLAN aware or legacy
  - Switches in a legacy domain must strip off and add VLAN id based on MAC or IP address








# 802.1Q frame format



- Two 2-byte additions
  - VLAN protocol ID constant (0x8100)
  - Tag containing:
    - Pri (3 bits) – to distinguish hard and soft real time traffic
    - CFI (Canonical Format Indicator, 1bit) ?
    - VLAN identifier (12 bits) The main purpose of the change