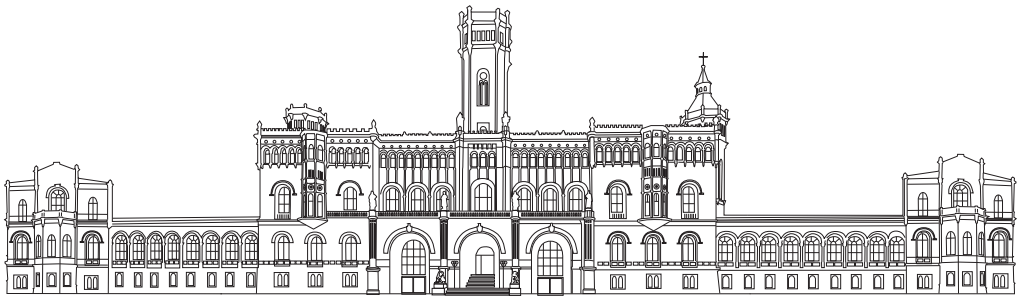
Rechnernetze – Computer Networks

Problem Set 7: Packet Switching

Markus Fidler, Mark Akselrod, Lukas Prause



Institute of Communications Technology
Leibniz Universität Hannover

June 3, 2024

Ethernet Medium Access Control

Ethernet Medium Access Control (MAC) uses 1-persistent CSMA/CD with binary exponential backoff. Explain this access method!

Carrier Sensing:

- If a station wants to send data, first of all it checks whether another station is already transmitting on the shared medium.
  - If the channel is busy, the station waits until it becomes idle
  - If the channel is idle, the station starts transmitting its data

Collision Detection:

- If more than one station accesses the medium, a collision occurs that is detected by the stations involved
  - Noise burst is sent to all stations

Binary exponential backoff:

- After a collision has occurred, each station has to wait a random time in $[0, w-1]$.
- Initially, $w = w_{min} = 2$
- after each subsequent collision w is doubled up to $w_{max} = 1024$
- after a successful transmission w is reset to w_{min}

MAC frame format

- What is the minimum frame size in case of classical Ethernet (10 Mbit/s)?
- Why is there a minimum frame size for Ethernet frames?
- What can be done if a frame is too short?

MAC frame format

- The minimum packet length is 64 Byte
- Classical Ethernet defines a maximal distance of 2500 meters between 2 stations (max. 500 m segment length and 4 repeaters)
  $\rightarrow$ maximal propagation delay $T_p = \frac{d}{v_p} = \frac{2500\ m}{2{\cdot}10^8\ m/s} = 12.5\ \mu s$
- $T_t > 2T_p = 25\ \mu s$ has to be assured in order to be able to detect collisions
- Transmission time of a 64 Byte packet is
  $T_t = \frac{l}{C} = \frac{512\ \text{bit}}{10{\cdot}10^6\ \text{bit/s}} = 51.2\ \mu s \rightarrow T_t > 2T_p$ is guaranteed
- Frames that are too short can be padded to 64 Byte

MAC frame format

An IP packet to be transmitted by Ethernet is 60 Byte long, including all its headers. Is padding needed in the Ethernet frame, and if so, how many bytes?

MAC frame format

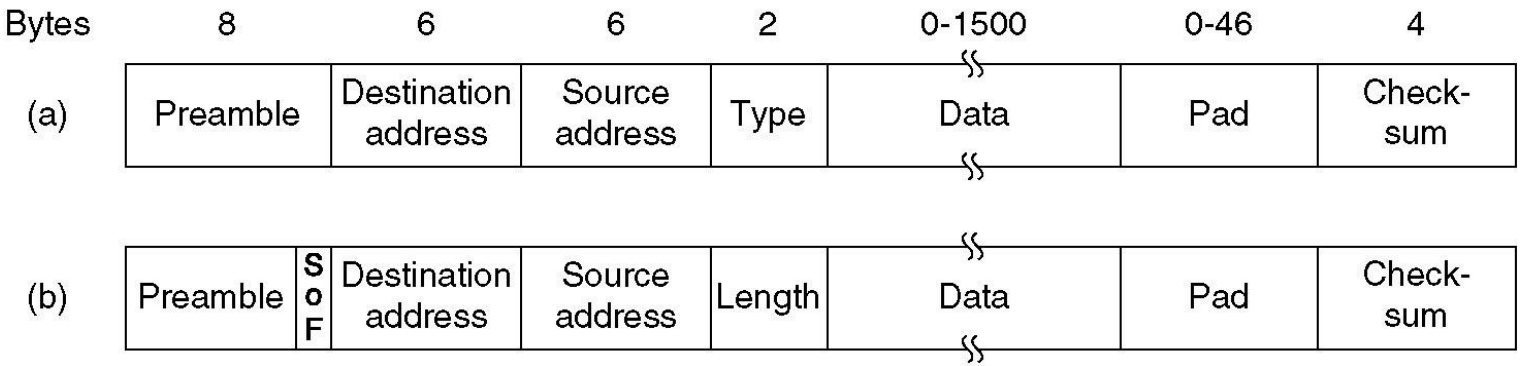
- The minimum Ethernet frame size is 64 Byte, including an 18 Byte overhead
- Adding 18 Byte Ethernet overhead to a 60 Byte long IP packet results in a 78 Byte packet

  $\rightarrow$ No padding is needed

MAC frame format

What is the maximum frame length in case of classical Ethernet (10 Mbit/s)?

MAC frame format



[Source: Tanenbaum, Computer Networks]

Frame format according to DIX (a), respectively, IEEE 802.3 (b)

- 1500 Byte maximum payload
- 18 Byte overhead (without preamble)
  $\rightarrow$ 1518 Byte maximum frame length

Classical Ethernet vs. Gigabit Ethernet

Classical Ethernet and Gigabit Ethernet have the same maximum frame length. Are there any disadvantages to not increasing the frame length for Gigabit Ethernet?

Efficiency of CSMA/CD

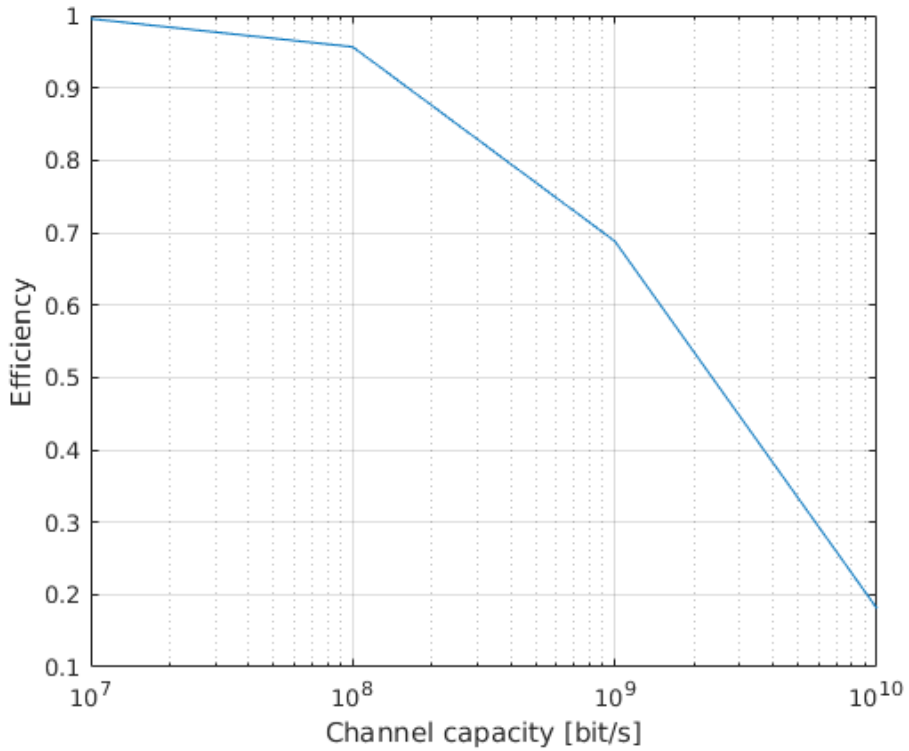
The efficiency η of CSMA/CD is bounded by (without derivation)

$$\eta = \frac{1}{1 + 2e\frac{Cd}{lv_l}}$$

where

- l frame length
- C capacity
- d distance
- v_l speed of light

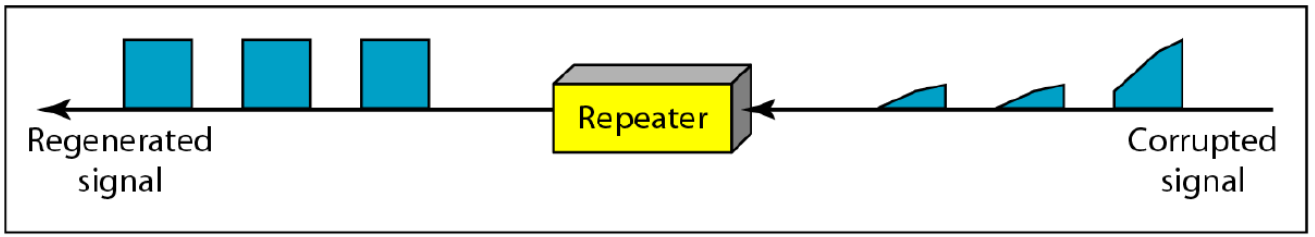
If the maximum frame length is not increased, efficiency of CSMA/CD decreases with an increasing capacity C:



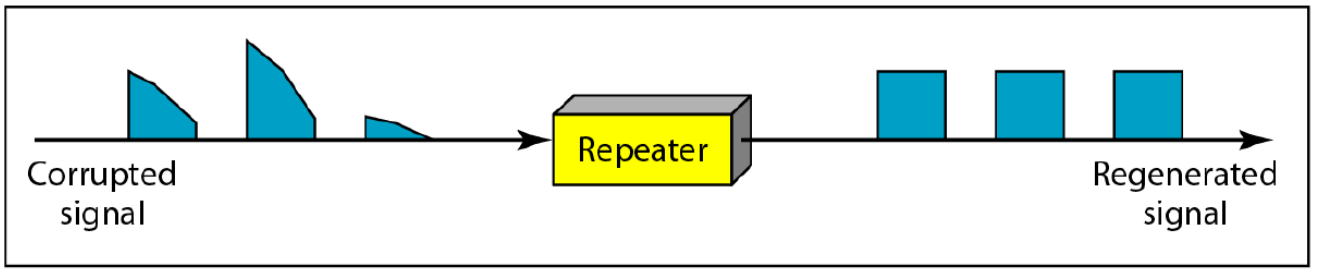
Classification

What is the difference between a repeater, a hub, and a switch?

Repeater

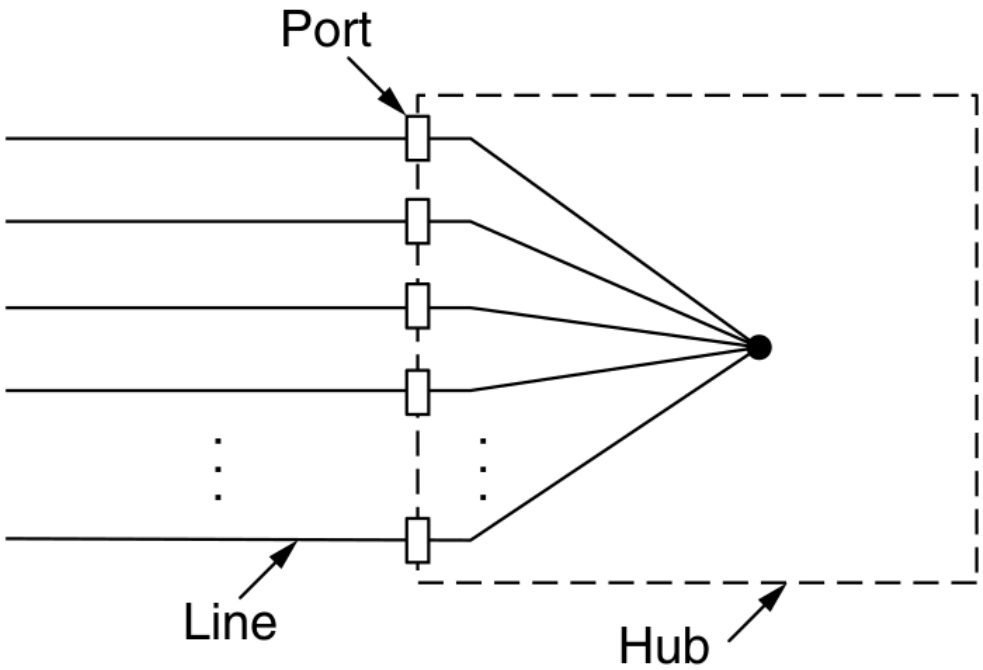


a. Right-to-left transmission.



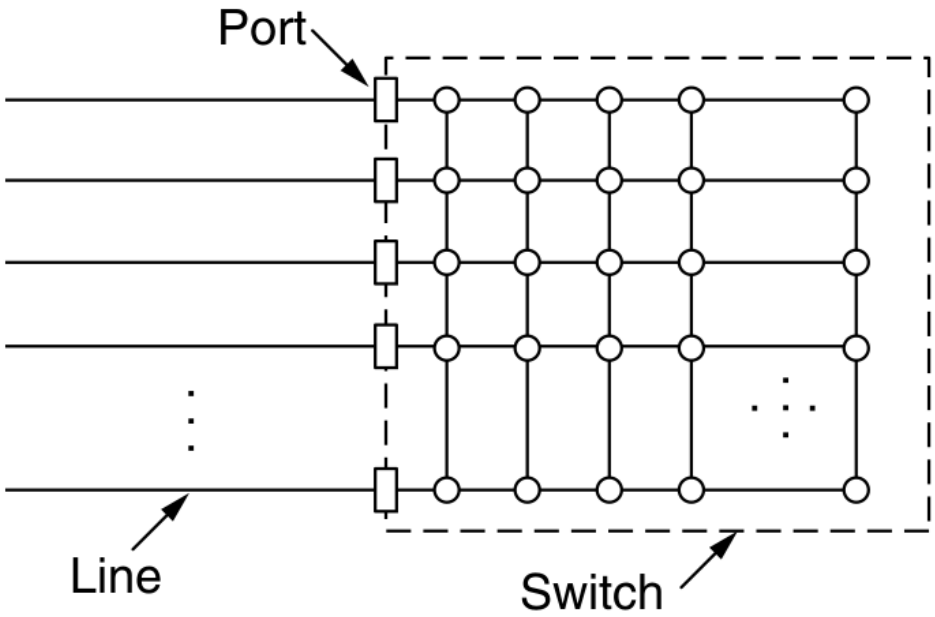
b. Left-to-right transmission.

A repeater connects two cable segments. It regenerates the signal from one segment and puts it on the other segment.



[Source: Tanenbaum, Computer Networks]

A hub electrically joins a number of input lines



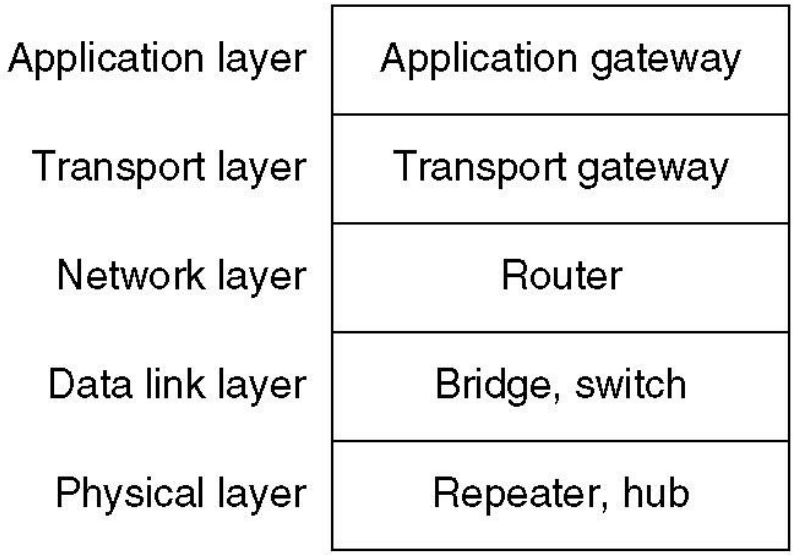
[Source: Tanenbaum, Computer Networks]

A switch filters incoming frames and uses a backplane to only output frames to the ports for which those frames are destined.

Classification: bridges, switches, hubs, and repeaters

Intermediate systems at

- Network layer
  - Router
- data link layer
  - LLC bridges
  - MAC bridges, switches
- physical layer
  - repeater
  - hub



[Source: Tanenbaum, Computer Networks]

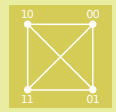
Collision Domain

What is a collision domain? How are collision domains different for hubs and switches?

Collision Domain

Collision Domain is a segment of a network in which a collision occurs if two or more stations transmit at the same time.

- Hub:
  - All stations are in the same collision domain as they are connected electrically
- Switch:
  - All of the stations attached to the same port on a switch belong to the same collision domain
  - Stations connected to different ports are in different collision domains



What is a switching table? How does a transparent (i.e. self-learning) bridge/switch fill its switching table?

Bridging

- A switch table indexes outgoing ports by destination's MAC addresses
- The filtering/forwarding decisions are based on the switch table.
- Initially the switch table is empty
- Bridge stores MAC source address, incoming port and time of arriving packets
- Entries are deleted after some aging time if not renewed

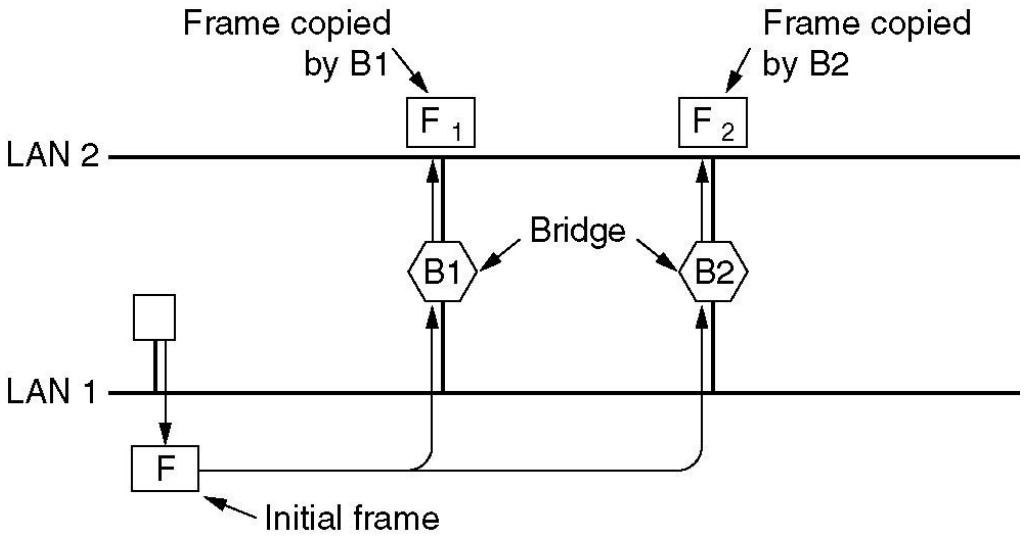
Redundant bridges

Why do we need redundant bridges?

Redundant bridges

If a bridge fails, a redundant bridge can take over and so guarantee the ongoing operation of the network

Redundant bridges



[Source: Tanenbaum, Computer Networks]

Redundant bridges increase reliability but introduce loops

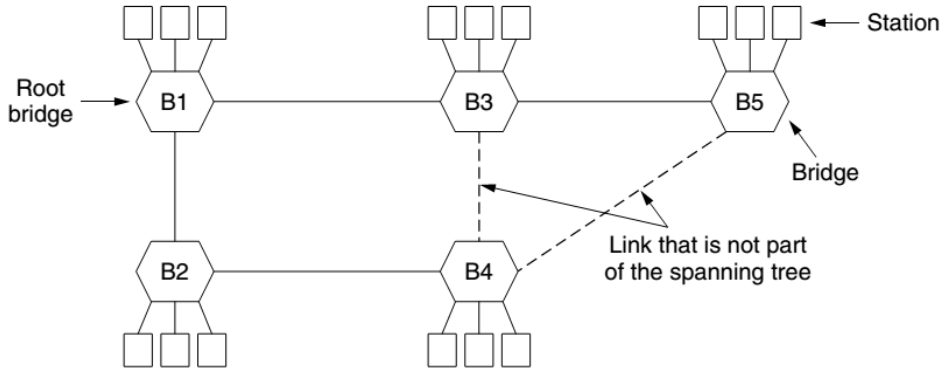
- They introduce loops ⇒ broadcast storm
- destination of frame F is not known to either of the bridges
- both bridges copy frame F to LAN2 resulting in F1 and F2
- B1 sees F2 and B2 sees F1, both with unknown destination
- both bridges copy F2 and F1, respectively, to LAN1

Redundant bridges

How can the loop problem introduced by redundant bridges be solved?

Solution: spanning tree topology

Before starting to forward frames the bridges organize as a tree.



[Source: Tanenbaum, Computer Networks]

- the spanning tree reaches every LAN
- some potential connections between LANs (bridges) are ignored/disabled
- the spanning tree topology is loop-free

The result is a topology where there exists only one unique path for any source-destination pair.

Spanning tree protocol

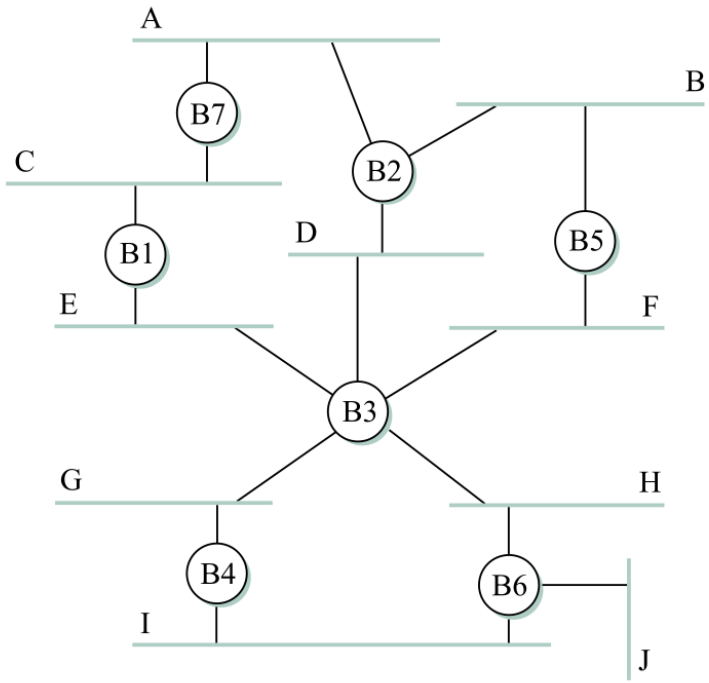
How does the spanning tree algorithm work?

Spanning tree algorithm

Algorithm for construction of the spanning tree

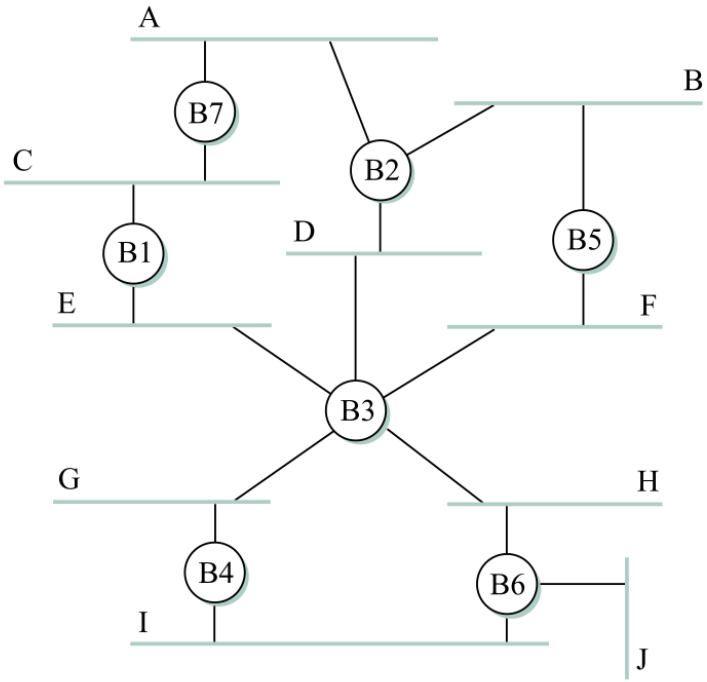
- a **root bridge** is selected to form the root of the tree (bridge with the smallest ID)
- each bridge determines shortest paths to the root bridge
  - bridges identify the port that is on the shortest path to the root as their **root port**
- on each LAN the bridge that offers the shortest path to the root is selected
  - the respective port of the bridge is called the **designated port**
- ports that are not root nor designated ports are blocked from data transmission
- tie-breaking rule: whenever two paths have the same length, the bridge that has the smaller ID wins

Given the extended LAN below, what does its corresponding spanning tree look like?

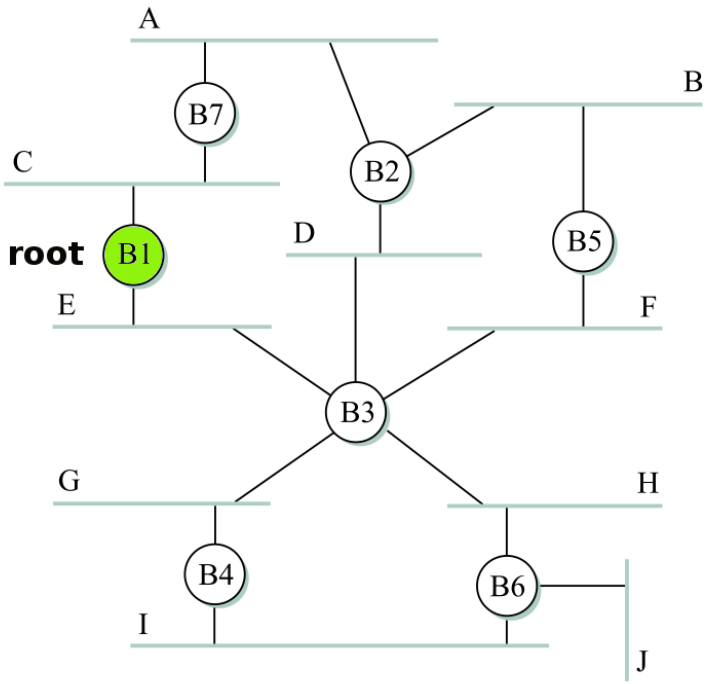


[Source: Peterson, Computer Networks: A Systems Approach]

1. Select root bridge:

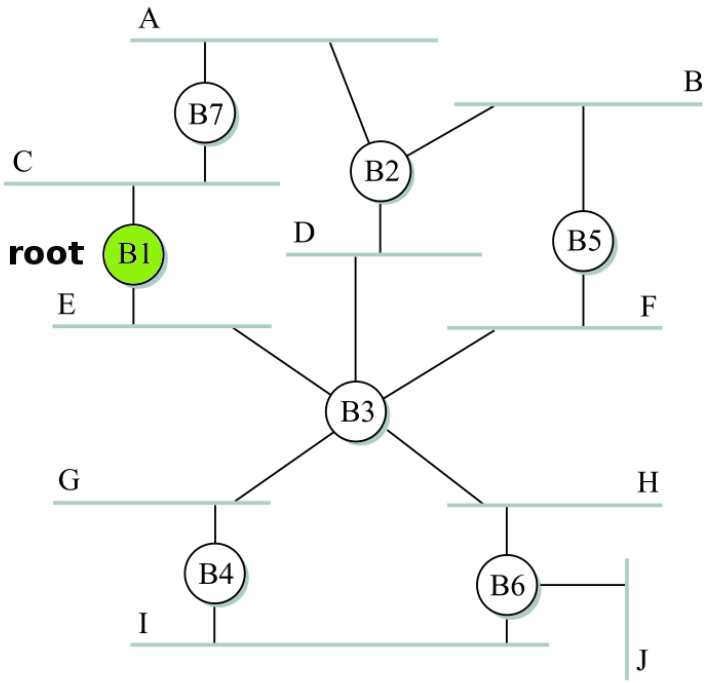


1. Select root bridge:

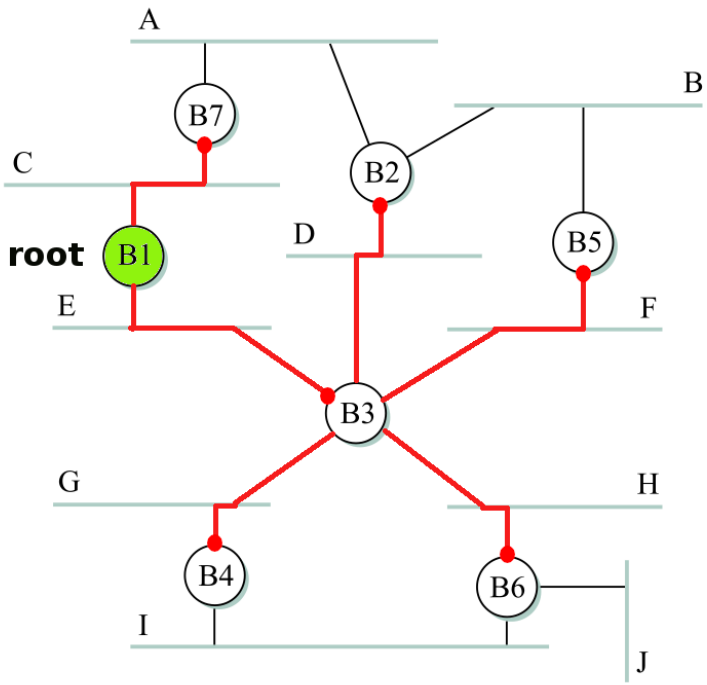


B1 has the smallest ID → B1 is the root bridge.

2. Find the shortest path from each bridge to the root:

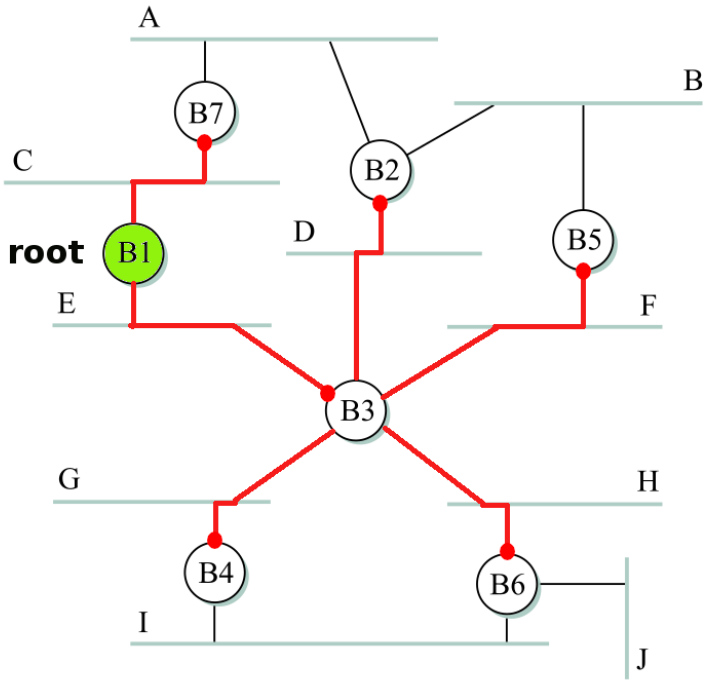


2. Find the shortest path from each bridge to the root:

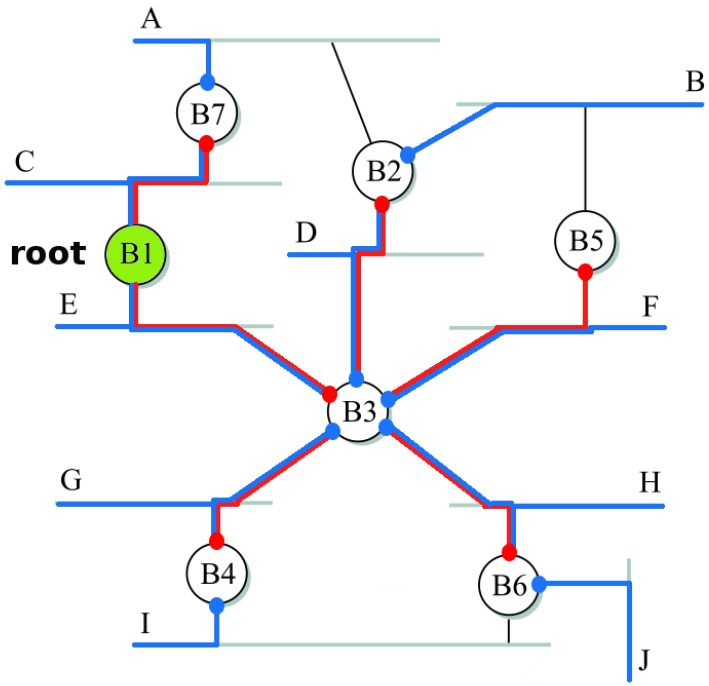


Shortest paths from each bridge to the root and the corresponding **root ports** are marked in red.

3. On each LAN, select the bridge that provides the shortest path to the root:

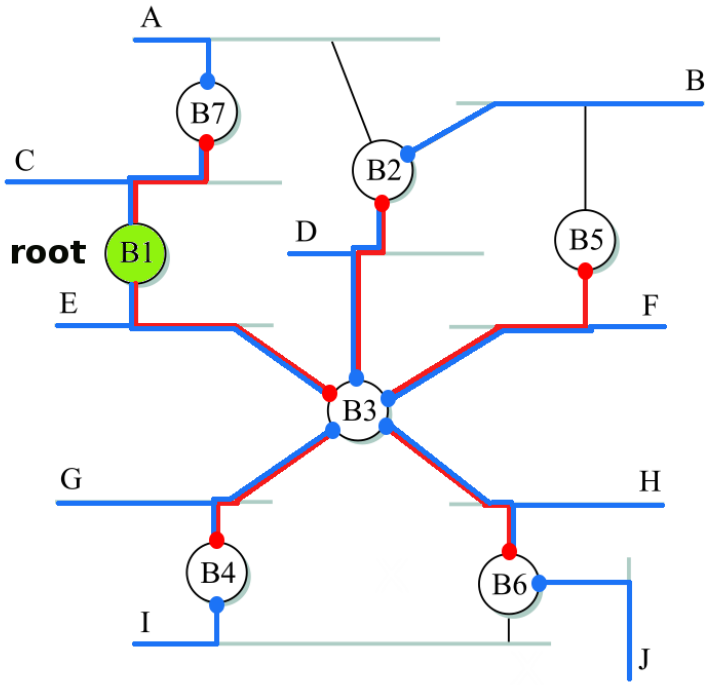


3. On each LAN, select the bridge that provides the shortest path to the root:

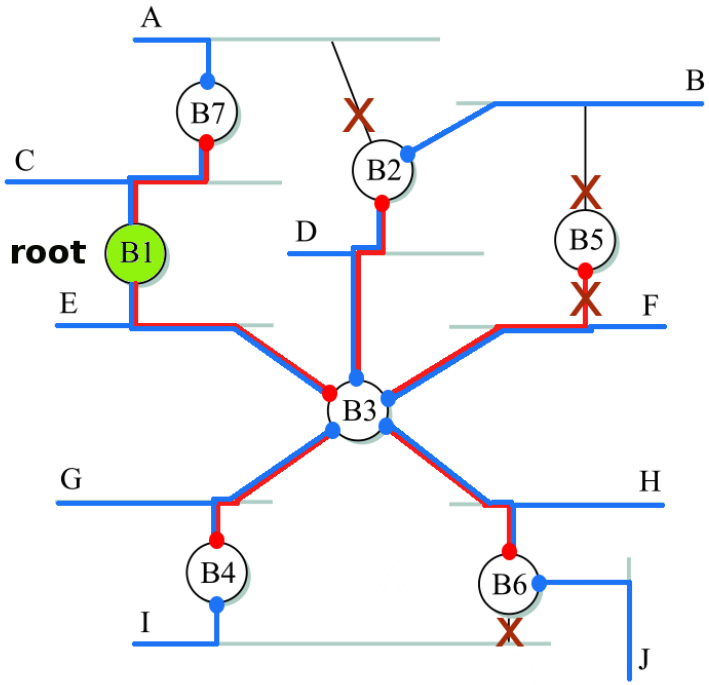


Shortest paths from each LAN to the root and the corresponding **designated ports** are marked in blue.

4. Which ports are never used for data transmission?



4. Which ports are never used for data transmission?



- B2 $\leftrightarrow$ A, B5 $\leftrightarrow$ B and B6 $\leftrightarrow$ I are not root ports or designated ports $\rightarrow$ ports are blocked
- B5 $\leftrightarrow$ F is the root port of B5, but B5 is not used by any LAN (no designated ports)

What is a VLAN? What are some advantages of using VLANs?
How can packets be forwarded to correct VLANs?

Virtual LANs

Need to group users on LANs

- decouple logical from physical topology (organizational structures instead of physical layout of the building)
- organizational changes appear frequently, reconfiguring the logical topology means, however, rewiring the network

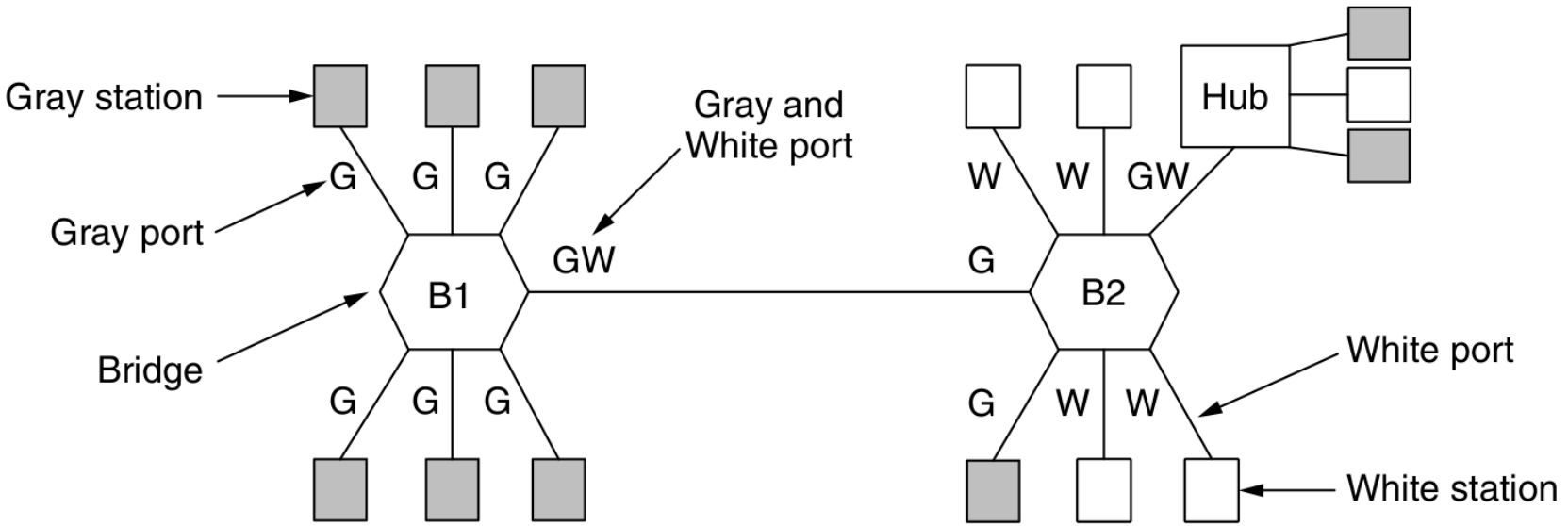
Virtual LANs

- map several logical networks onto one physical network
- perform the 'rewiring' in software

Mark different VLANs by different colors, e.g. gray and white.
VLAN enabled bridges/switches

- map e.g. MAC addresses or incoming ports to VLAN colors
- map VLAN colors to outgoing ports
- broadcast frames only on 'correctly colored' ports

VLAN: Example



[Source: Tanenbaum, Computer Networks]

Virtual LANs are marked by colors: gray (G) and white (W)

Legacy devices in VLANs

How can legacy 802.3 Ethernet cards in PCs be supported in a network that uses the 802.1Q VLAN features?

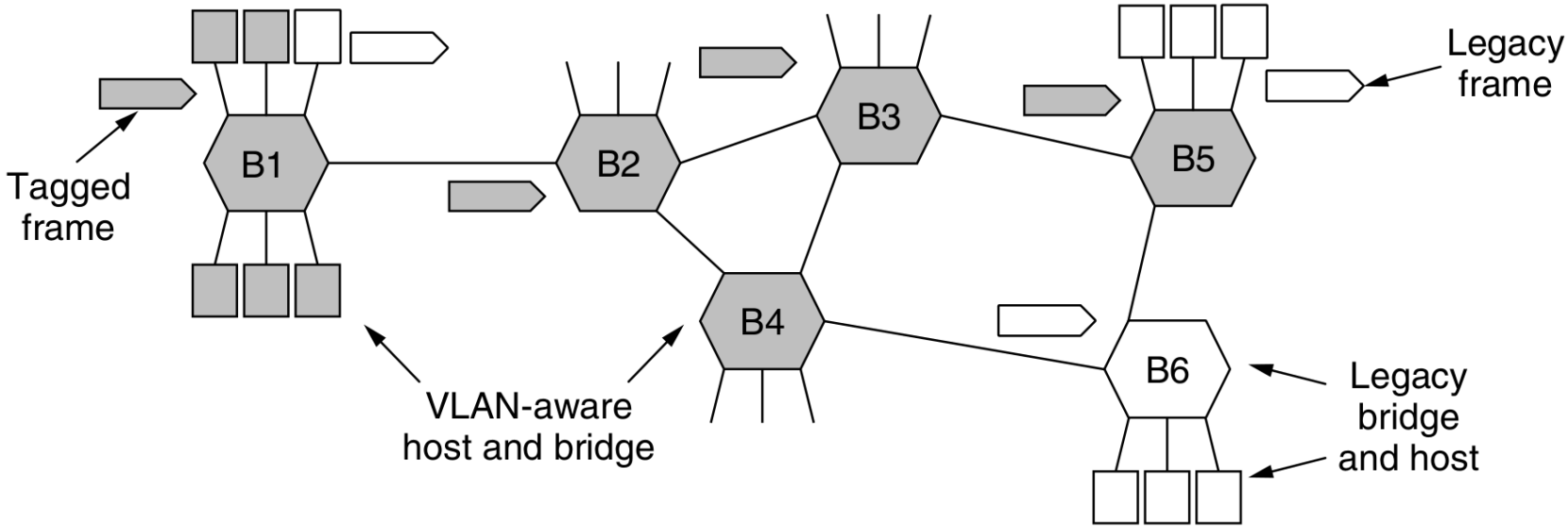


Figure 4-48. Bridged LAN that is only partly VLAN aware. The shaded symbols are VLAN aware. The empty ones are not.

[Source: Tanenbaum, Computer Networks]

Legacy devices in VLANs

- VLAN fields are only used by bridges and switches, not by user machines
- Hence bridges and switches have to be VLAN aware, not the interface cards in the user machines (PCs)
- The first VLAN-aware bridge or switch that touches a frame adds the VLAN fields, the last one removes them
- Assignment in the first bridge/switch can be done by port or MAC address (configuration necessary)