Computer Networks
-Ethernet, LAN-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W7 short test (1)

- Explain the process of the three-way handshake in a "normal" situation (without duplicates, etc.)!
  - Host 1 sends a connection request (CR) with a certain sequence number (seq=x) to Host 2. Host 2 acknowledges this (ACK) with a different sequence number (seq=y), but acknowledging the sequence number of the connection request (ACK=x). Then Host 1 sends the data with its original sequence number (seq=x), acknowledging the sequence number of Host 2 (ACK=y).
- In case of the three-way handshake, if there is an old duplicate of a connection request, the connection won't be established. Why?
  - The duplicate CR from Host 1 has a certain sequence number (seq=x), and after the other host acknowledges this (seq=y, ACK=x), Host 1 will know it is a duplicate from the acknowledged sequence number, so it rejects the connection (ACK=y).

W7 short test (2)

- What is the mechanism that ensures that connections are released, even if disconnect requests or acknowledgments of disconnect requests are lost?
  - Timer (with timeout/*n* timeouts)
- While TCP is connection-oriented, UDP is *connectionless*.
- The TCP service is obtained by both the sender and the receiver creating endpoints called *sockets*.
- What does it mean that TCP connections are full duplex?
  - Traffic can go in both directions at the same time.
- Which well-known port is associated with SSH via TCP or UDP?
  - 22
- The TCP connection is identified by a tuple of five elements. List these elements!
  - protocol, source IP, destination IP, source port, destination port

W7 short test (3)

- While the TCP flag *SYN* is used to establish connections, the *FIN* flag is used to release connections.
- Name of the the error detection mechanism to check the integrity of the data transmitted:
  - checksum
- Why do we need window management for TCP?
  - 1. For the acknowledgement of the correct receipt of segments: if a segment is correctly received, the receiver will acknowledge this. 2. Receiver buffer allocation: the receiver will advertise its buffer space (window) based on the received segments (and what have been read by the application).

W7 recap (1)

- The data link layer uses the services of the physical layer below it to send and receive bits over communication channels
- Communication channels make errors occasionally, data may be lost
- The data link layer takes the packets it gets from the network layer and encapsulates them info frames for transmission
  1. Provide a well-defined service interface to the network layer
  2. Framing sequences of bytes as self-contained segments
  3. Detecting and correcting transmission errors
  4. Regulating the flow of data
- Three main types of possible services: unacknowledged, acknowledged connectionless, acknowledged connection-oriented
- To provide a service to the network layer, the link layer must use the service provided to it by the physical layer

W7 recap (2)

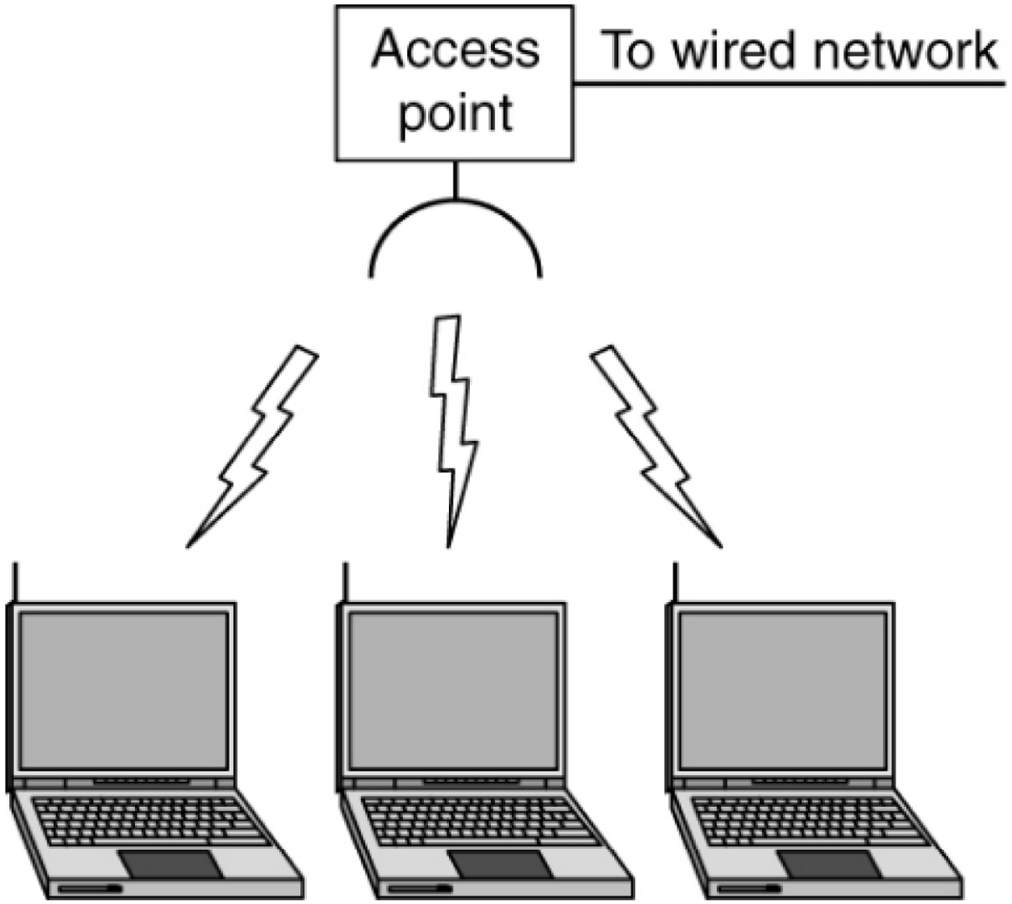
- Methods for breaking up the bit stream into discrete frames: byte count, flag bytes with byte stuffing or bit stuffing, and invalid characters
- Error control is mainly about ensuring all frames are eventually delivered to ensure a reliable service
- Flow control is about controlling the sending of transmission frames at a faster pace than they can be accepted
- FEC include enough redundant information to enable the receiver to deduce what the transmitted data must have been (e.g., Hamming codes)
- Error-detecting codes include only enough redundancy to allow the receiver to deduce that an error has occurred (but not which error) and have it request a retransmission (e.g., checksum, parity bits)
- PPP is about establishing a direct connection between two nodes without any host or any other networking device in between over many types of physical networks

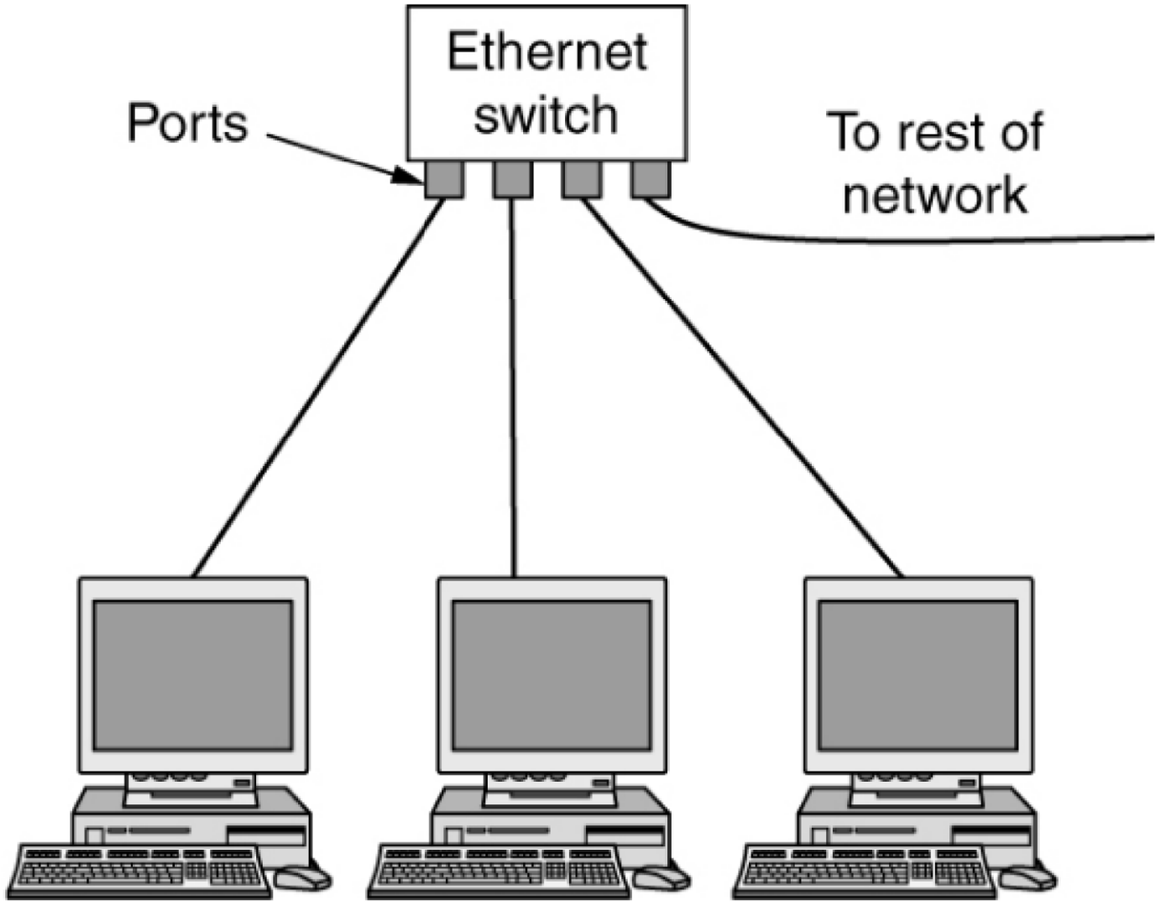
Agenda

- LAN review from W1
- The Medium Access Control Sublayer
- Ethernet
- Switching
- Virtual LANs
- Summary

LAN and VLAN

- **LAN** (Local Area Network) is a private network that operates within and nearby a single building
  - In case of wireless LANs, each computer talks to an **AP** (Access Point), **wireless router**, or **base station**
  - the IEEE 802.11 standard running from 11 Mbps to 7 Gbps is called **WiFi**
  - the **Ethernet** (IEEE 802.3) is the most common wired LAN (generally faster, and lower latency)
  - when each computer connects to a **switch** with a point-to-point link, it is a **switched Ethernet** topology
  - a switch has multiple **ports**, each of which connect to one other device
- It is possible to divide one large physical LAN into two smaller logical LANs: **VLAN** (Virtual LAN)
  - e.g., the layout of a network equipment does not match the organization's structure


Access point
To wired network


Ethernet switch
Ports
To rest of network

Home networks

- Home network LAN
  - broad, diverse range of Internet-connected devices
- Internet of things
  - allows almost any device to connect
- Required home network properties
  - easy to install and maintain
  - secure and reliable
  - interfaces work between all products
  - reduced consumer device costs

Multiaccess channels

- Many link layer protocols rely on a broadcast communication medium to transmit data
  - have to allow multiple senders to efficiently and fairly share the broadcast medium
- In any broadcast network, they key issue involves determining who gets to use the channel when there is "competition" for it
  - broadcast channels are often referred to as **multiaccess channels** or random access channels
- The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called **MAC** (Medium Access Control)
  - important for LAN, WAN

The channel allocation problem

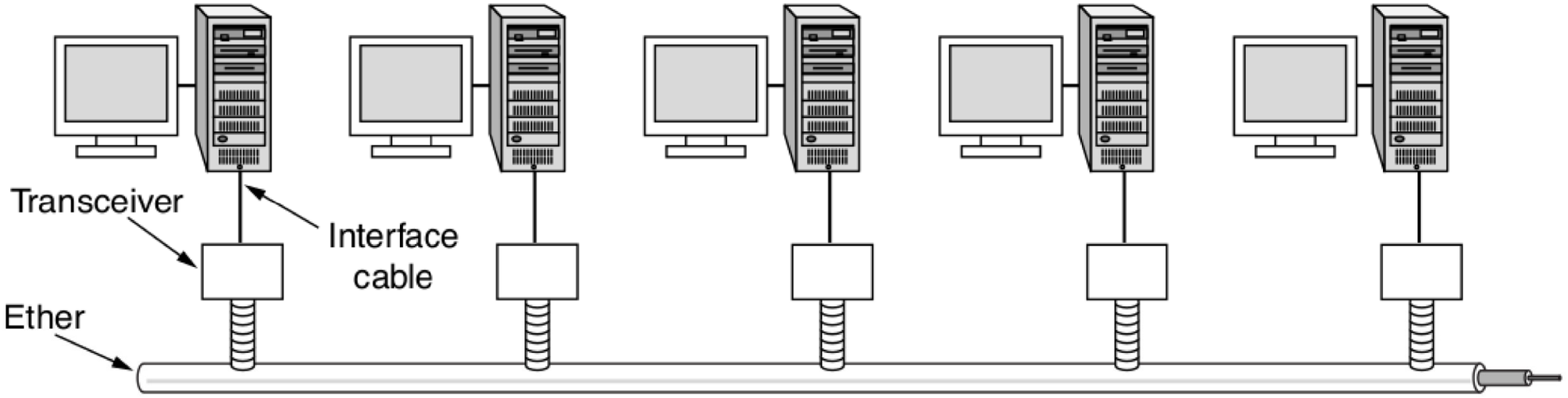
- How to allocate a single broadcast channel among competing users?
  - the channel might be a portion of the wireless spectrum in a geographic region, or a single wire or optical fiber to which multiple nodes are connected
  - the channel connects each user to all other users and any user who makes full use of the channel interferes with other users who also want to use the channel
- **Static channel allocation**: e.g., chop up the channels capacity using multiplexing (bandwidth is divided into N equal-sized portions for N users)
  - poor fit to computer systems with extremely bursty data traffic
  - most channels will be idle most of the time
- **Dynamic allocation** tries to resolve static allocation problems

Multiple access protocols

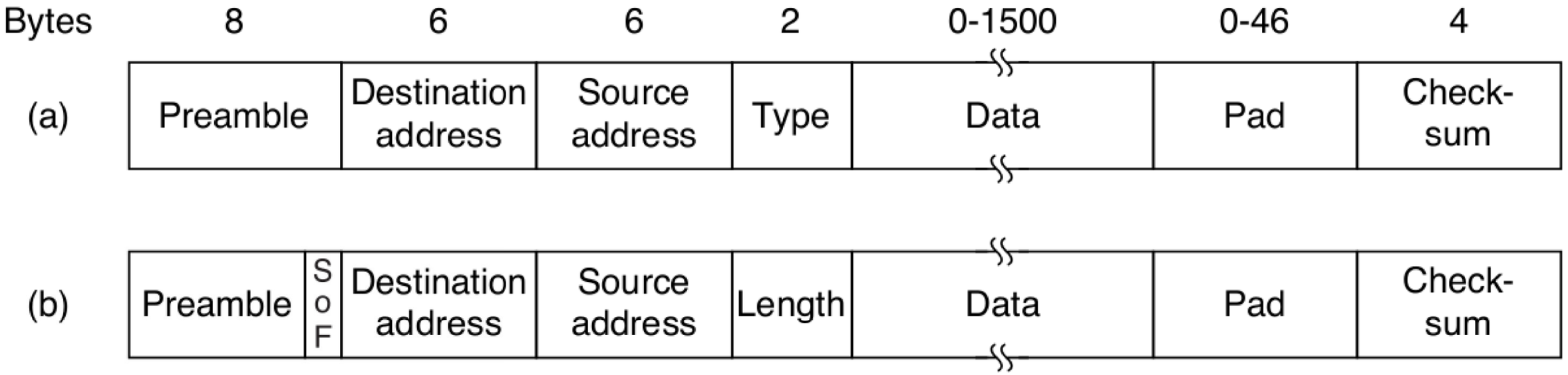
- Many algorithms for allocating multiple access channels exist
- The **ALOHA** protocol with many of its derivatives are used in many systems such as DOCSIS (Data over cable service interface specification) networks
  - **CSMA** (Carrier Sense Multiple Access) protocols for LANs, MANs is the basis for classic Ethernet and 802.11 networks: when the state of the channel can be sensed, stations can avoid starting a transmission while another station is transmitting
- **CD** (Collision detection): quickly detect collision between stations and abruptly stop transmitting
- **Limited-contention protocols** eliminate or reduce contention considerably

Classic Ethernet architecture

- **Classic Ethernet**
  - 3 to 10 Mpbs, originally with a single, thick coaxial cable to connect PCs
  - each version of Ethernet has a maximum cable length per segment over which the signal will propagate
  - to allow larger networks, multiple cables can be connected by **repeaters** to amplify and retransmit signals
  - DIX standard $\rightarrow$ IEEE 802.3



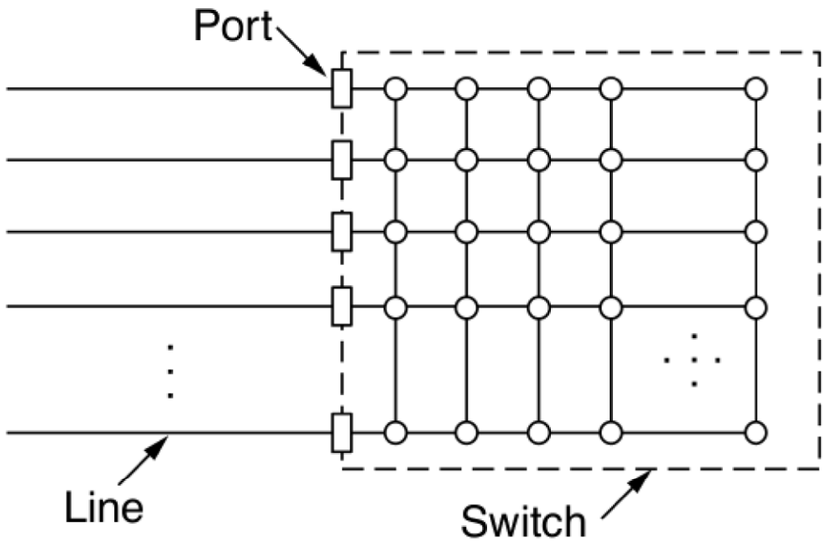
Frame formats: DIX and IEEE 802.3

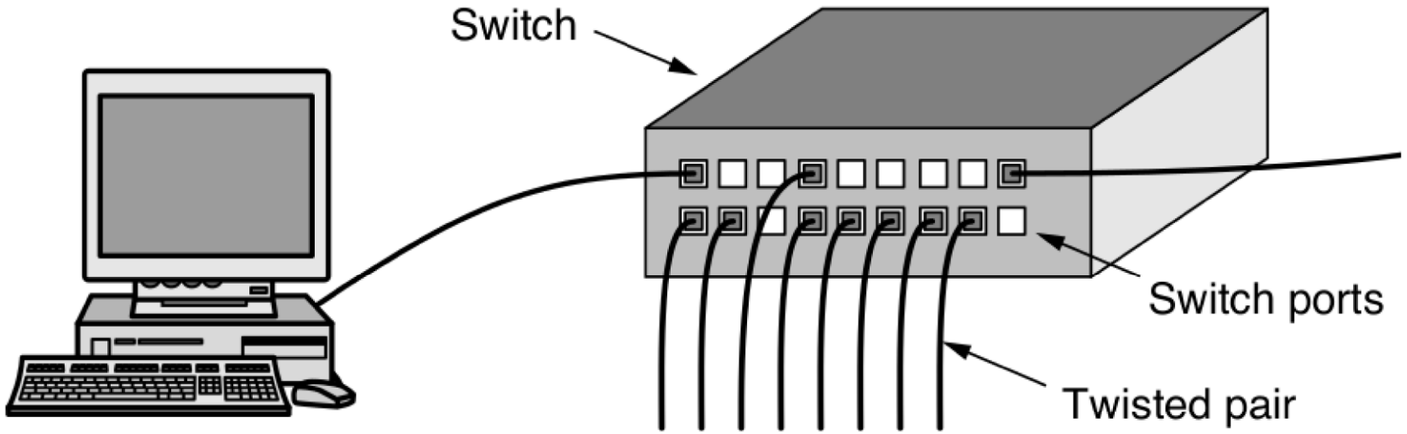


Switched Ethernet

- To deal with the increased load: **switched Ethernet**
- The **switch** contains a high-speed backplane that connects all of the ports
  - easy to add or remove a new station by plugging or unplugging a wire
  - easy to troubleshoot
- Switches only output frames to the ports for which those frames are destined: when a switch port receives an Ethernet frame from a station, the switch checks the Ethernet addresses to see which port the frame is destined for
- The destination port transmits the frame on the wire so that is reaches the intended destination
  - each port has its own **collision domain**

Ethernet switch





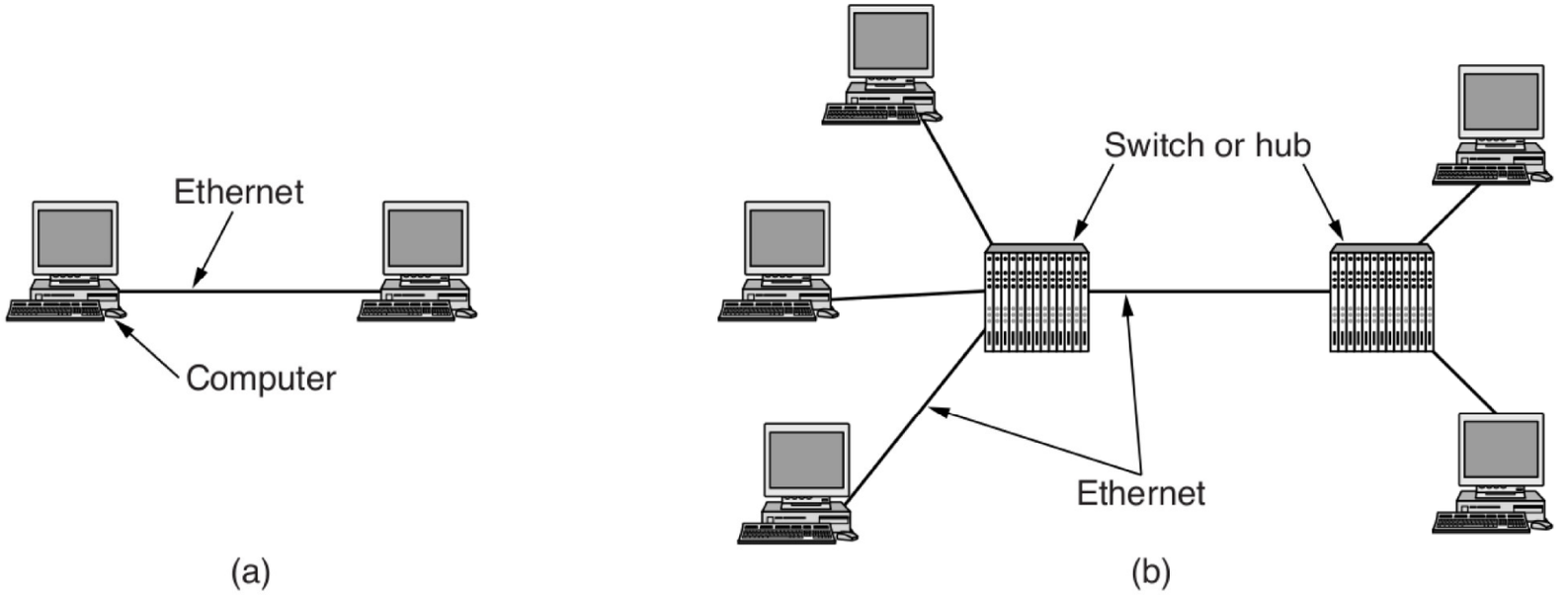
Fast Ethernet

- With the emergence of switches, the speed of 10-Mbps Ethernet started to get unsatisfactory
  - many installations needed more bandwidth, had to use many repeaters, hubs, switches
- Increase performance while maintaining compatibility

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Gigabit Ethernet

- Like fast Ethernet, all configurations of gigabit Ethernet use point-to-point links, and support full-duplex and half-duplex modes



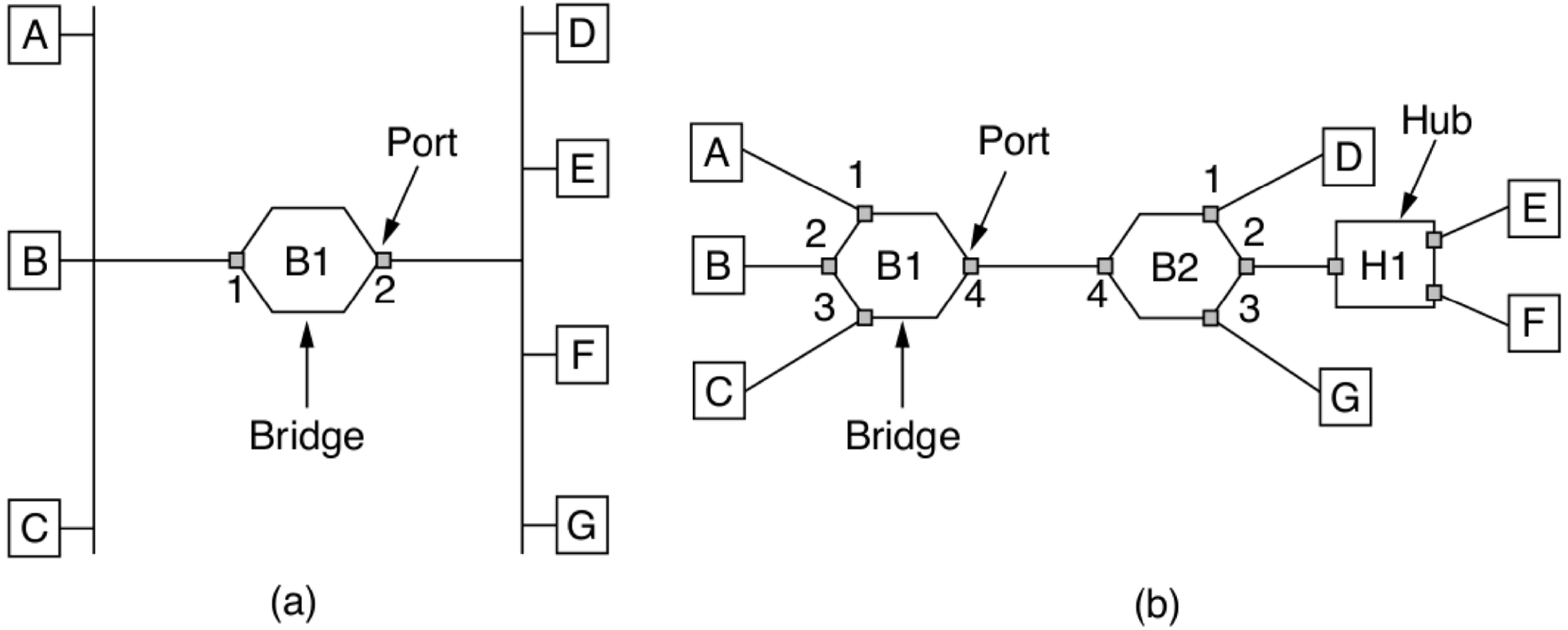
Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

10-, 40-, 100-Gigabit Ethernet

- 10-Gigabit: Connect high-end routers, switches, and servers, long-distance high bandwidth trunks between offices that are enabling entire MANs based on Ethernet
  - long distance connections use optical fiber, short connections may use copper or fiber
- 40-Gigabit: internal connections in data centers
- 100-Gigabit: Internet backbone (optical-network running over thousands of kms)

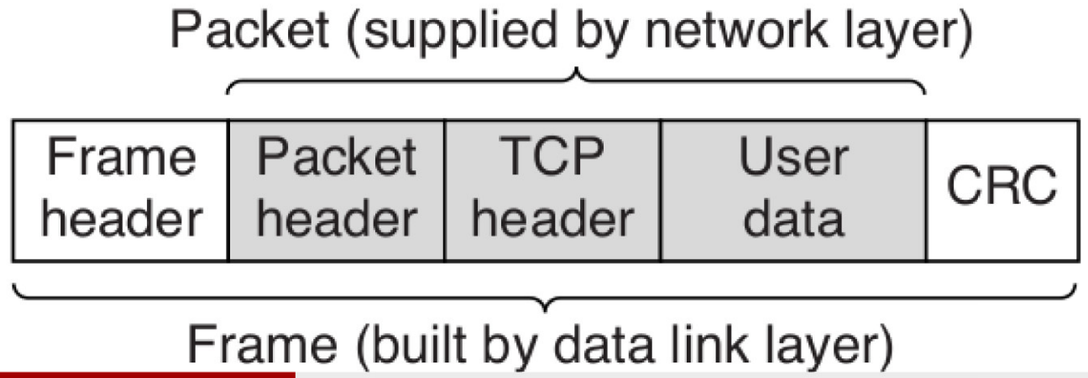
Bridges

- Many organizations have multiple LANs and wish to connect them
- Using **bridges** to join/connect LANs
  - switches are "modern" bridges, and in the case of Ethernet, commonly referred to as Ethernet switches



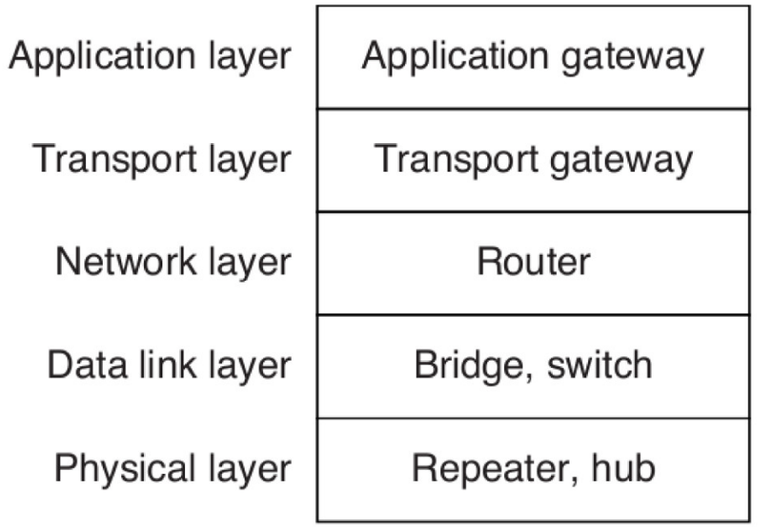
Switching in different layers

- Devices to get frames and packets from one computer to another: operating in different layers
  1. The user generates some data to be sent to a remote machine
  2. The data are passed to the transport layer, adding a header (e.g., TCP header) and passes the resulting unit to the network layer
  3. The network layer adds its own header to form a network layer packet (e.g., an IP packet)
  4. The packet goes to the data link layer that adds its own header and checksum (CRC), and gives the resulting frame to the physical layer for transmission (e.g., over a LAN)



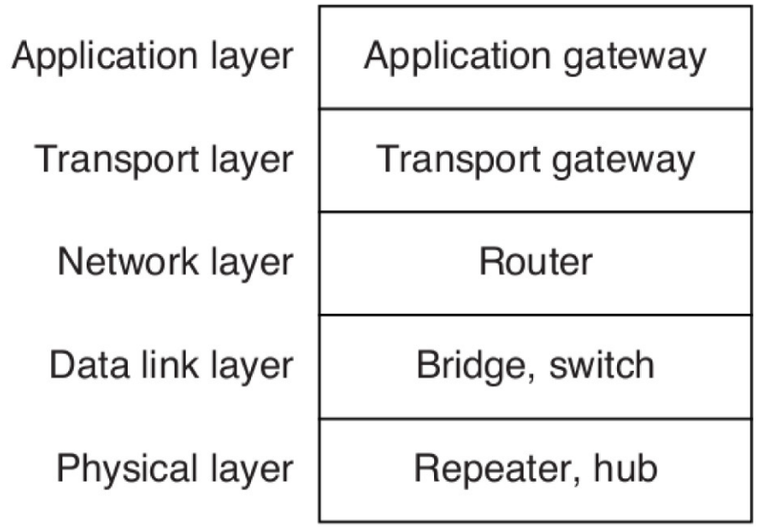
Devices in different layers (1)

- Repeaters are analog devices that clean up and amplify signals and put them out on another cable (does not understand frames, packets, or headers)
- A hub has a number of input lines that it joins electrically: frames arriving on any of the lines are sent out on all the others
- The bridge at the data link layer outputs the frame on the port where it is needed and can forward multiple frames at the same time



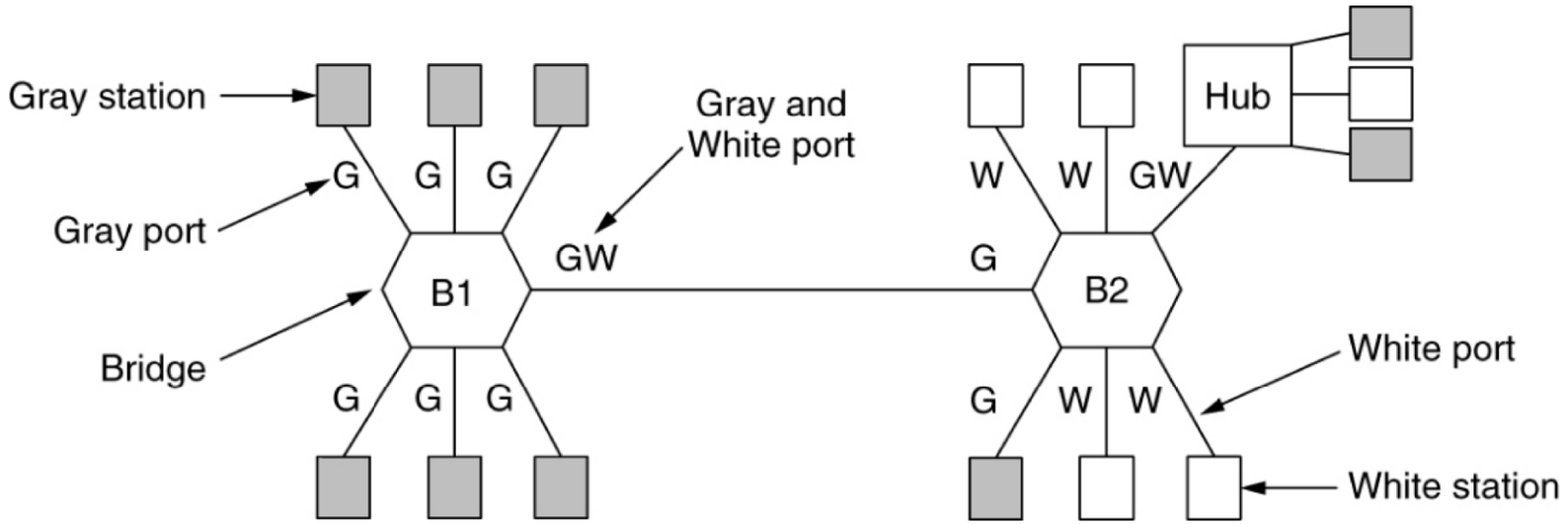
Devices in different layers (2)

- When a packet comes to a router, the frame header and trailer are stripped off and the packet located in the frame's payload field is passed to the routing software (uses the packet header to choose an output line)
- The routing software does not see the frame addresses and does not know how the packet came in
  - Transport gateways connect two computers that use different connection-oriented transport protocols by copying and reformatting packets (e.g., TCP/IP with SCTP)
  - Application gateways understand the format and contents of the data and can translate messages from one format to another (e.g., and email gateway could translate Internet messages into SMS)



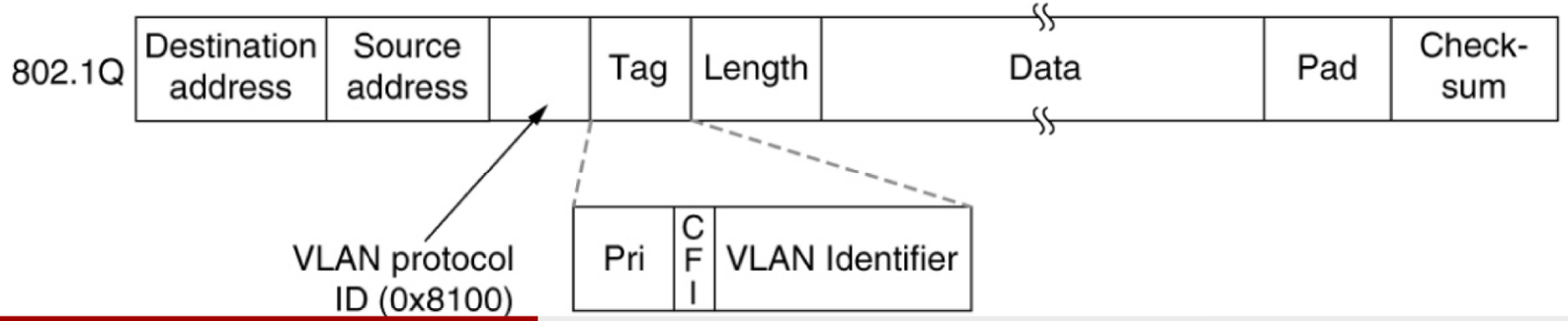
Logical connection

- LANs can be configured logically rather than physically
  - users are often grouped to reflect the organizational structure rather than the physical layout of a building
  - security, load, broadcast traffic
- **VLAN**s (Virtual LANs) are often named by colors
- Which VLANs are accessible via which ports: configuration tables have to be set up in the bridges



The IEEE 802.1Q Standard

- Bridges need to know which VLAN an incoming frame belongs
- The Ethernet header was changed to contain a VLAN tag
  - VLAN fields are only used by the bridges/switches, and not by the user machines
- As there can be computers and switches that are not VLAN aware, the first VLAN-aware bridge to touch a frame adds VLAN fields and the last one removes them
  - the switch uses the VLAN identifier as an index into a table to find out which ports to send the frame
  - VLAN-aware bridges can autoconfigurate themselves based on observing the tags that come by



W9 Summary (1)

- LAN is a private network that operates within and nearby a single building
- Many link layer protocols rely on a broadcast communication medium to transmit data
- In any broadcast network, they key issue involves determining who gets to use the channel when there is "competition" for it
- The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called MAC
- Allocate a single broadcast channel among users: static vs. dynamic allocation
- Many solutions for allocating multiple access channels exist; CSMA/CD
- Classic vs. Switched Ethernet to deal with the increased load
- Switches only output frames to the ports for which those frames are destined: when a switch port receives an Ethernet frame from a station, the switch checks the Ethernet addresses to see which port the frame is destined for

W9 Summary (2)

- Fast, Gigabit, 10+ Gigabit Ethernet standards
- Many organizations have multiple LANs and connect them with bridges (switches)
- Different devices in different layers: repeater, hub, bridge, switch, router, transport gateway, application gateway
- The Ethernet header was changed to contain a VLAN tag, for logically configured LANs
- Which VLANs are accessible via which ports: configuration tables have to be set up in the bridges