COMP2001J Computer Networks

Lecture 6 – Data Link Layer
(Applications)

Dr. Shen WANG (王燊)

shen.wang@ucd.ie

About Quiz 2

- Consider a LAN that uses CSMA/CD for its medium access control. Its data transmission rate is 15Mb/s. The distance between host A and host B is 3km. The signal propagation speed is 300000km/s. If there is a collision occurs while host A and host B are transmitting data, what is the "gap" (in milliseconds) between the maximum and minimum time duration, which starts from when they begin to transmit, to the moment when BOTH hosts have detected the collision?

About Quiz 2

- The maximum time duration
  - When collision occurs very close to either side
  - 2 x propagation delay
- The minimum time duration
  - When collision occurs at the mid-point between A and B
  - 2 x ($\frac{1}{2}$ x propagation delay)
- Answer: one-way propagation delay
  - $3/3*10^5$= 0.01 ms

About Quiz 2

- Consider transmitting frames (1.5kbit length for each) over a satellite channel that has 60kb/s data rate. Assume that 3 bits are used for numbering frames, piggybacking ACK is used, and the end-to-end one directional propagation delay is 300ms. What is the maximum channel efficiency (in percentage point, 2 decimal places) under the following protocols?
  - Stop-and-Wait
  - Go-back-N
  - Selective Repeat (sending/receiving window are the same in length)

About Quiz 2

- "piggybacking ACK is used"
  - means ACK is sent with data frame;
  - also implies that transmission time for ACK frame should not be ignored;
  - Thus, a full period T = 2 x Transmission Time + 2 x Propagation Time
- $w_r + w_s \leq 2^n$, w_s:
  - Stop-and-wait: always 1, thus 1* Transmission Time / T
  - Go-back-N: $2^3 - 1 = 7$, thus 7* Transmission Time / T
  - Selective Repeat: $2^{3-1}=4$, thus 4* Transmission Time / T

Outline

- LAN
  - Ethernet
  - Wireless LAN
  - Switch
  - Virtual LAN
- WAN
  - PPP
  - HDLC

Local Area Network

- LAN refers to a type of computer network that has a relatively small geographic range (e.g. school, company) for sharing resources internally.
  - Owned by one entity logically with limited connected devices.
  - Sharing a high data rate.
  - Low latency and bit error rate
  - All connected devices are equally important.
  - Can do broadcast and multicast

Local Area Network

- Different LANs vary in
  - Topologies (e.g. Bus, Star, Ring)
  - Transmission mediums (e.g. Twisted Pairs, Fiber, Coaxial Cable)
  - MAC schemes (e.g. ALOHA, CSMA)
- Among all LANs, Ethernet dominates the market!

Ethernet

- Classic Ethernet (10Mbps)
- Switched / Fast Ethernet (100Mbps)
- Gigabit / 10 Gigabit Ethernet (1000Mbps / 10Gbps)

Ethernet

- In the mid 1970s Xerox PARC developed first Ethernet to connect 100 computers on a 1 km cable

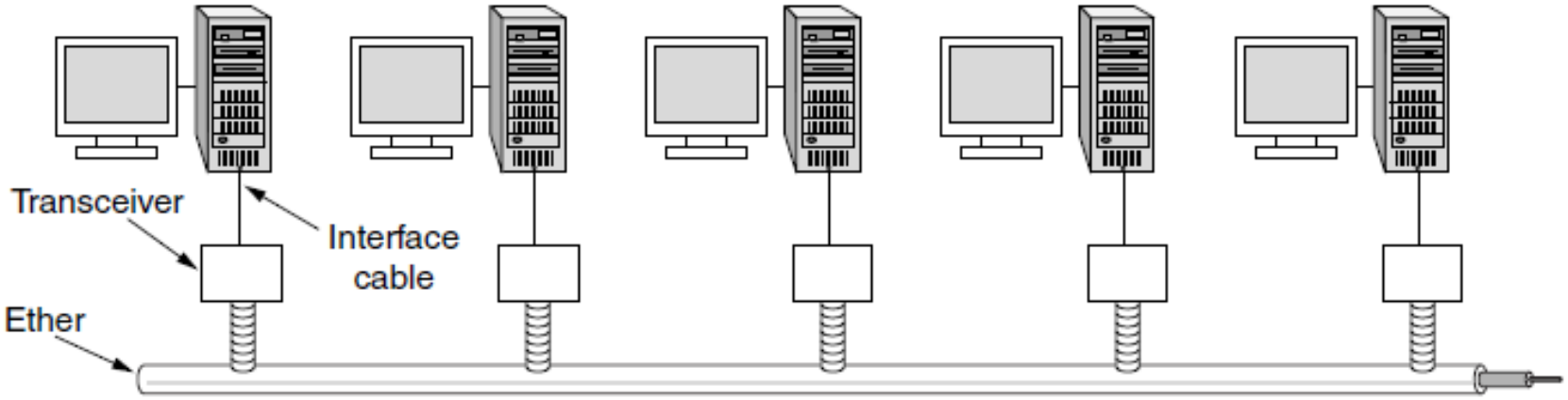
- It used the channel access method: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – to try to reduce the ***likelihood*** and ***effects*** of a collision

Ethernet Names

- Data rate + “BASE” + Cable Type
- Example 1: 10BASE-5
  - Maximum data rate: 10 Mbps
  - Cable Type: Category 5 Coaxial Cable
- Example 2: 100BASE-FX
  - Maximum data rate: 100 Mbps
  - Cable Type: Fiber
- Example 3: 1000BASE-T
  - Maximum data rate: 1000 Mbps
  - Cable Type: Unshielded Twisted Pairs

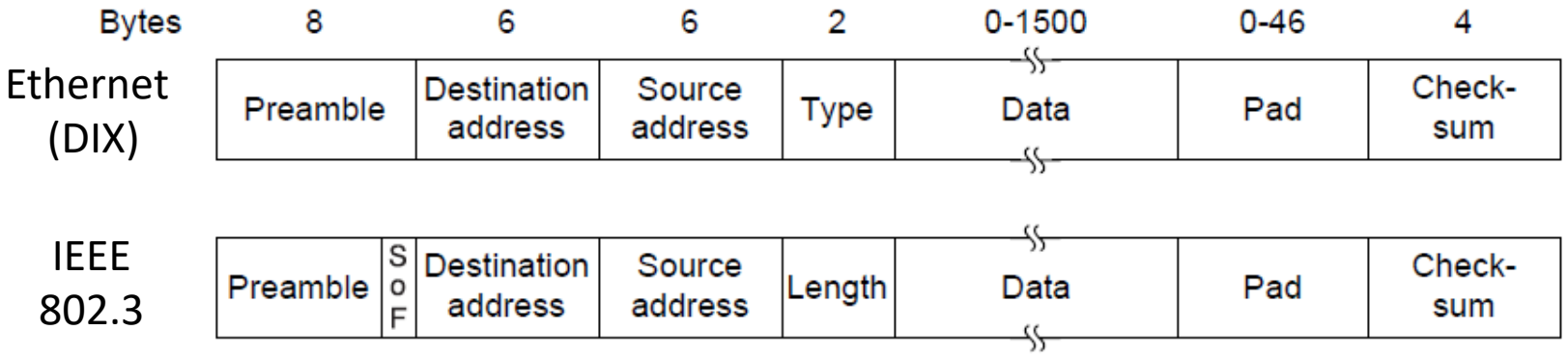
Classic Ethernet – Physical Layer

- One shared coaxial cable to which all hosts attached
  - Up to **10 Mbps**, with **Manchester encoding**
  - Hosts ran the classic Ethernet protocol for access



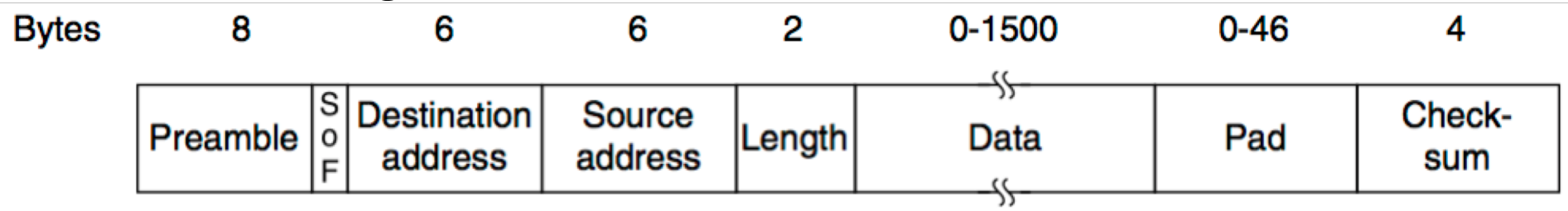
Classic Ethernet - MAC

- MAC protocol is 1-persistent CSMA/CD (earlier)
  - Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)
  - Frame format is still used with modern Ethernet.
- There are two standards for Ethernet (Ethernet DIX, IEEE 802.3), but their frames are almost the same.



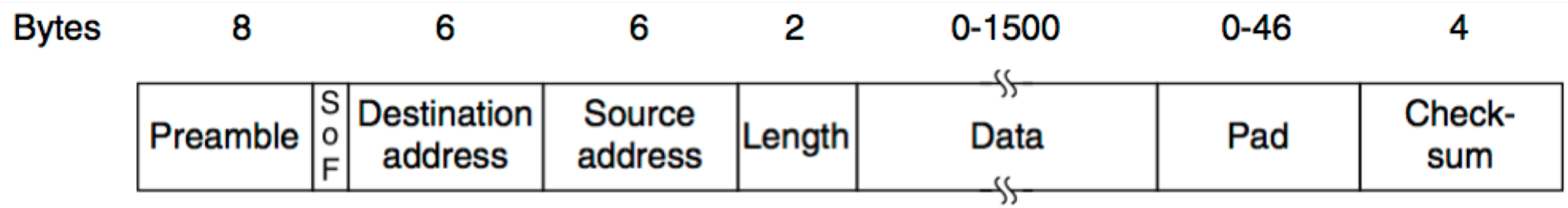
Ethernet Frame

- **Preamble** is to allow receiver to synchronize with incoming transmission
  - This is 56 alternating 1s and 0s (10101010…)
- SoF is the start flag in Ethernet (sometimes called SFD – Start Frame Delimiter)
  - This is a single byte that starts with alternating 1s and zeros but ends with two consecutive 1s (10101011)
  - This signals that the frame information is about to start



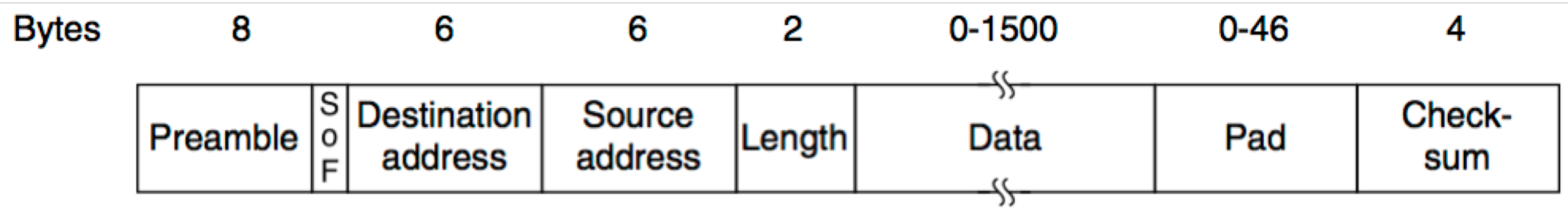
Ethernet Frame

- Destination and source addresses are **6-byte** numbers that uniquely identify the Network Interface Card (NIC) of the sender and receiver
  - Each NIC ever created has a **unique** address in the world!
  - This is called **MAC address**!
- The length field specifies how much data is in the Data section
  - There is a maximum of **1500 bytes** (**MTU**: Maximum Transmission Unit)



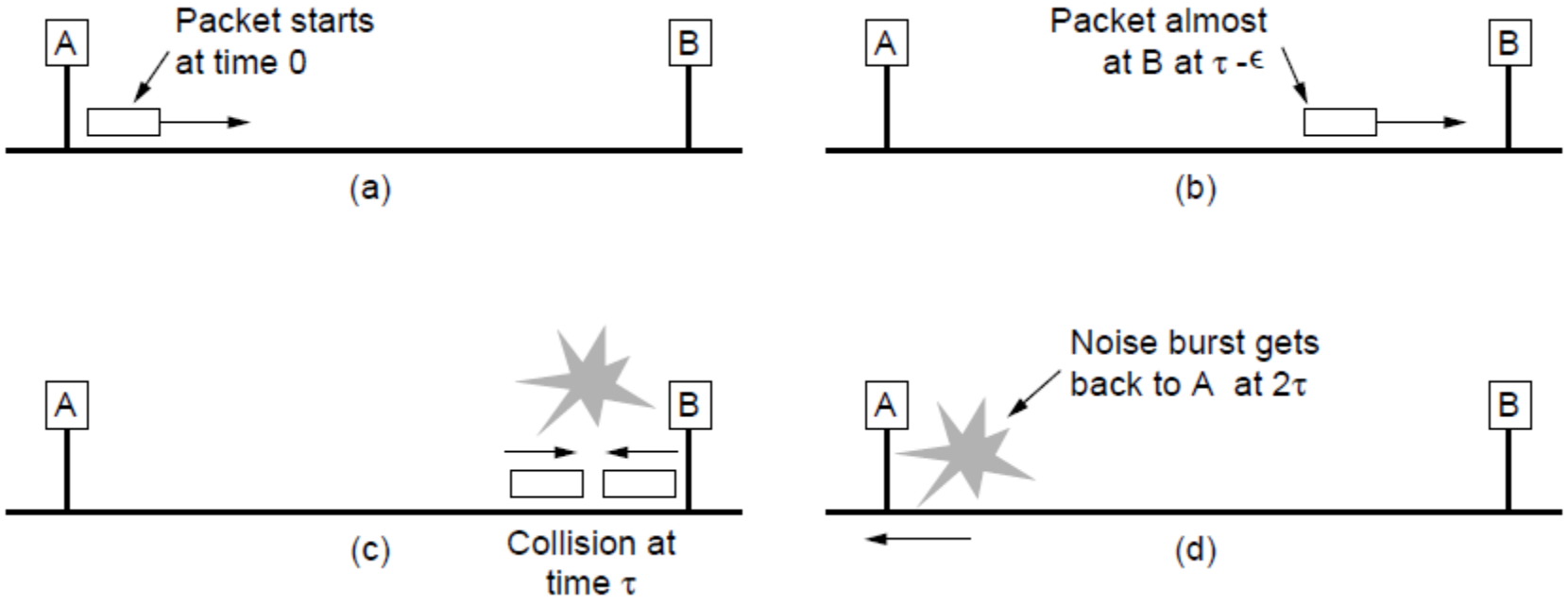
Ethernet Frame

- The minimum size of a valid frame is **64 bytes** not including the preamble
  - The control data at the start is only 14 bytes long
  - The CRC checksum at the end is only 4 bytes long
- Therefore if the data transmitted is less than 46 bytes we need increase the size of the frame so it is valid
  - We do this with the Pad field



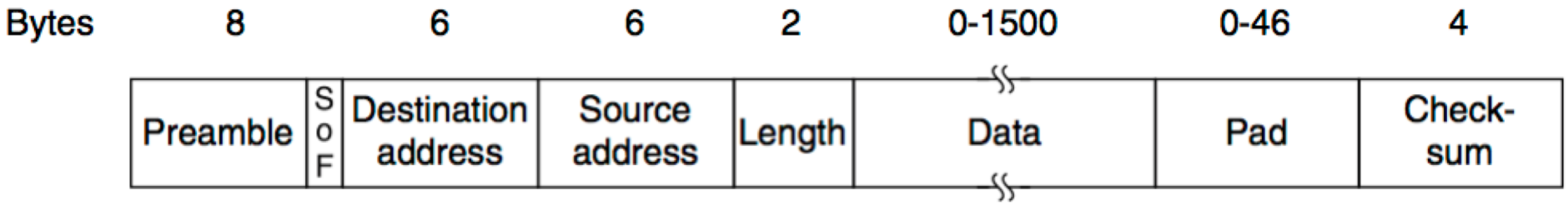
Classic Ethernet - MAC

- Collisions can occur and take as long as 2τ to detect
  - τ is the time it takes to propagate over the Ethernet
  - Leads to minimum frame size for reliable detection



Ethernet Frame

- The last field is the checksum
  - This is a 32-bit CRC algorithm
  - It is basically the same algorithm we have already studied but with a larger result

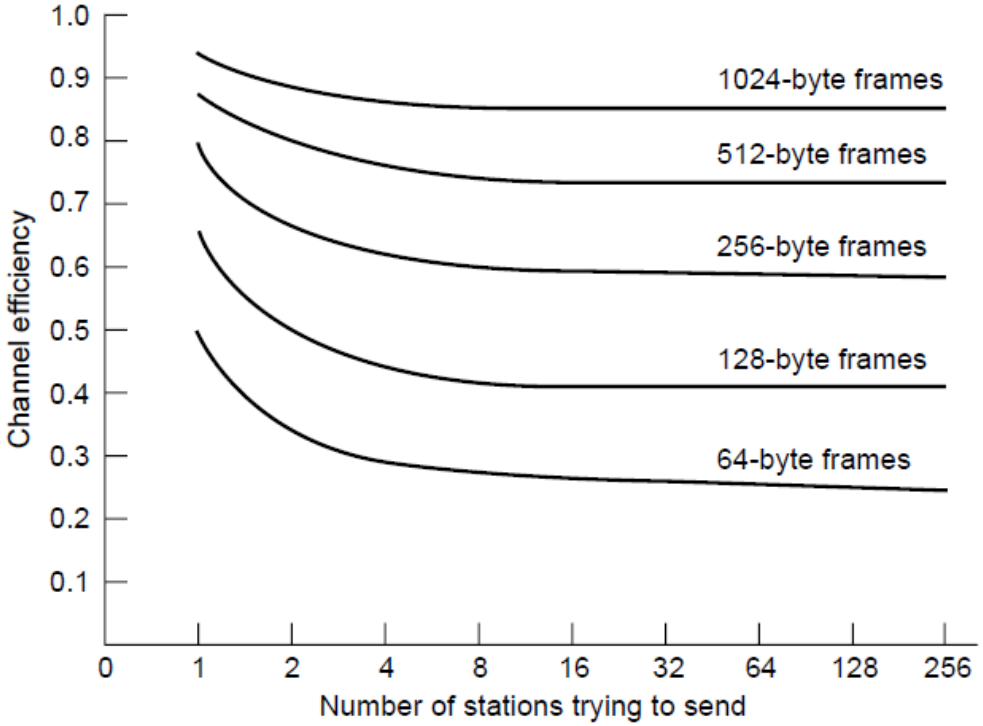


Classic Ethernet-Performance

- Recall the channel efficiency is:

$$\frac{1}{1 + 2BLe/c\boldsymbol{F}}$$

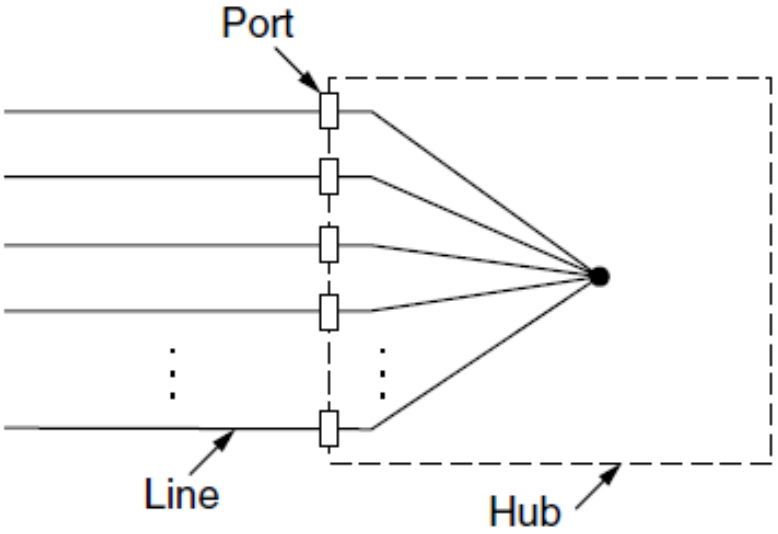
- Efficient for large frames, even with many senders
  - Degrades for small frames (and long LANs)
  - It can't be too large, as long frame size leads to high bit error rate.

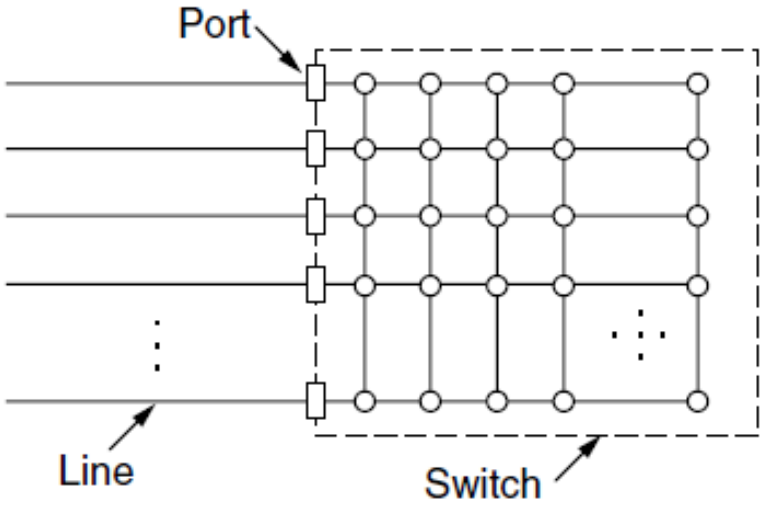


10 Mbps Ethernet, 64 byte min. frame

Switched / Fast Ethernet

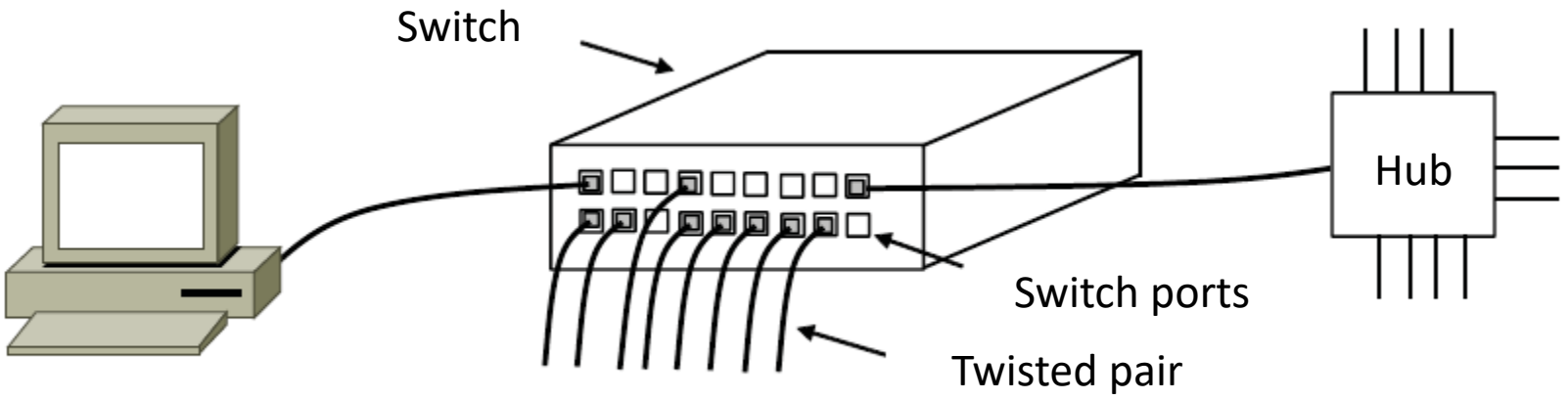
- Hubs wire all lines into a single CSMA/CD domain
- Switches isolate each port to a separate collision domain
  - Much greater throughput (100Mbps each) for multiple ports
  - No need for CSMA/CD with full-duplex lines





Switched / Fast Ethernet

- Switches can be wired to computers, hubs and switches
  - Hubs concentrate traffic from computers
  - More on how to switch frames later in this class



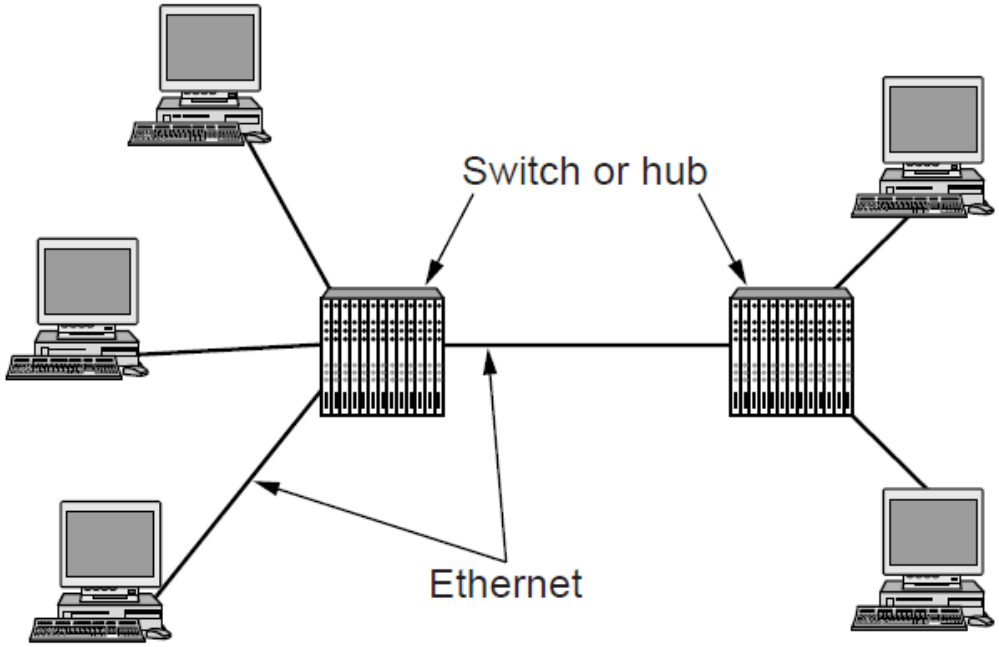
Switched / Fast Ethernet

- Fast Ethernet extended Ethernet from 10 to 100 Mbps
  - Twisted pair (with Cat 5) dominated the market

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 / 10 Gigabit Ethernet

- Switched Gigabit Ethernet is now the garden variety
  - With full-duplex lines between computers/switches



Gigabit / 10 Gigabit Ethernet

- Gigabit Ethernet is commonly run over twisted pair

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 Gigabit Ethernet is being deployed where needed

Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85μ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3μ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5μ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

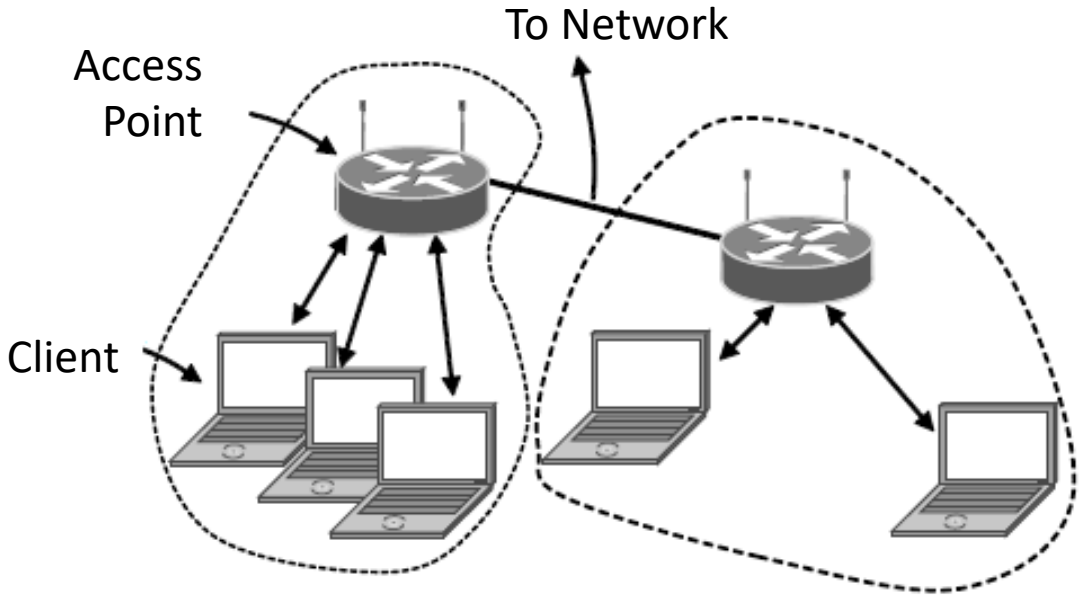
- 40/100 Gigabit Ethernet is under development

Wireless LANs

- 802.11 architecture / protocol stack
- 802.11 physical layer
- 802.11 MAC
- 802.11 frames

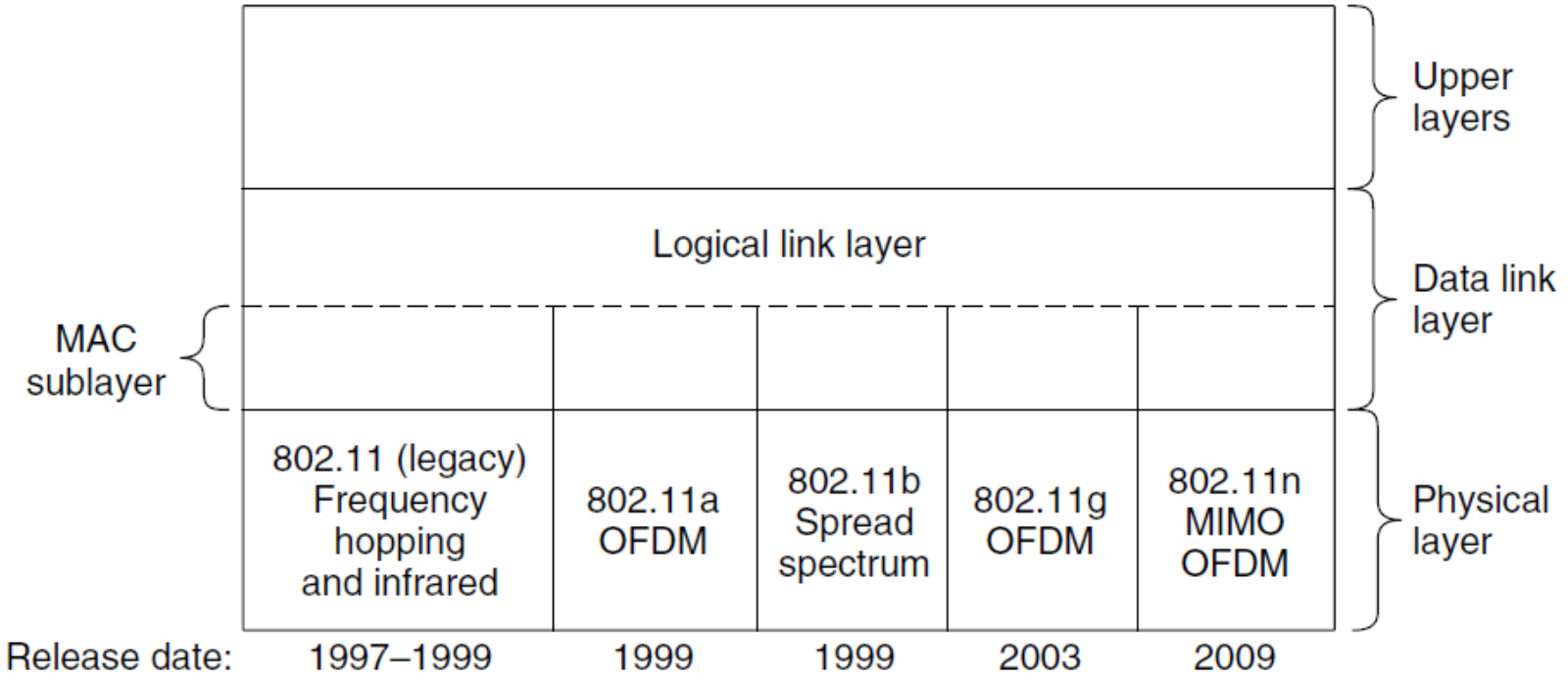
802.11 Architecture/Protocol Stack

- Wireless clients associate to a wired AP (Access Point)
  - Called infrastructure mode; there is also ad-hoc mode with no AP, but that is rare.



802.11 Architecture/Protocol Stack

- MAC is used across different physical layers



802.11 physical layer

- NICs are compatible with multiple physical layers
  - E.g., 802.11 a/b/g

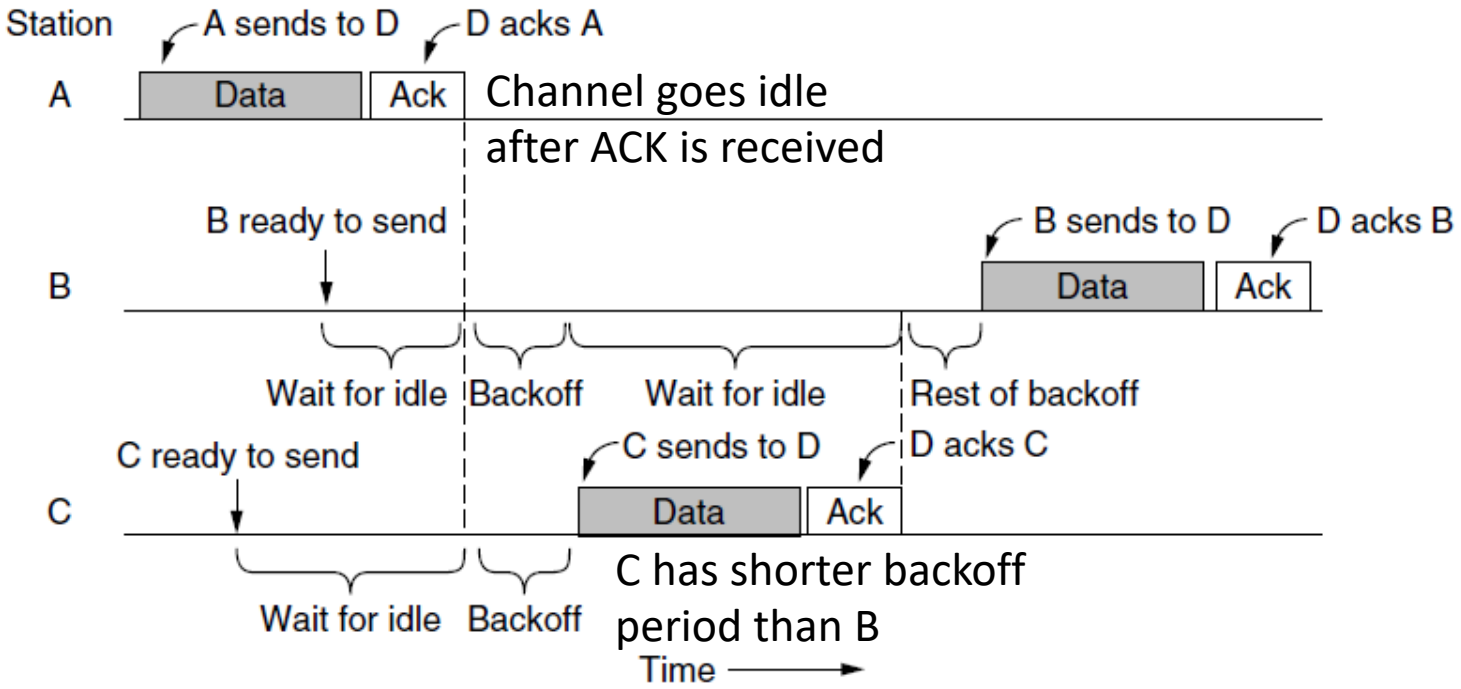
Name	Technique	Max. Bit Rate
802.11b	Spread spectrum, 2.4 GHz	11 Mbps
802.11g	OFDM, 2.4 GHz	54 Mbps
802.11a	OFDM, 5 GHz	54 Mbps
802.11n	OFDM with MIMO, 2.4/5 GHz	600 Mbps

Wireless Channel Problems

- Radios are nearly always half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency.
  - The received signal can easily be a million times weaker than the transmitted signal, so it cannot be heard at the same time.
- The transmission ranges of different stations may be different.
  - With a wire, the system is engineered so that all stations can hear each other.
  - With the complexities of RF propagation this situation does not hold for wireless stations. Consequently, situations such as the hidden/exposed terminal problem can arise.

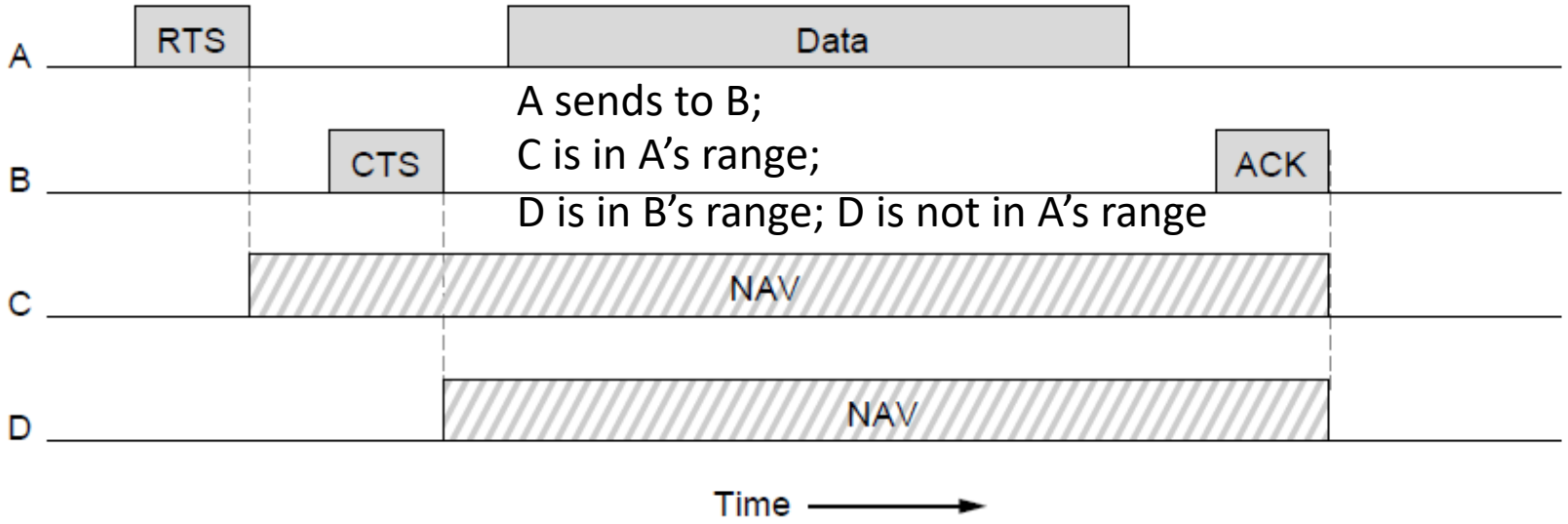
802.11 MAC

- CSMA/CA inserts backoff slots to avoid collisions
  - Once idle, a sender starts with a random backoff, rather than sending frames immediately (backoff occurs when collisions detected for CSMA/CD)
- MAC uses ACKs/retransmissions for wireless errors
  - As collisions can not be detected



802.11 MAC

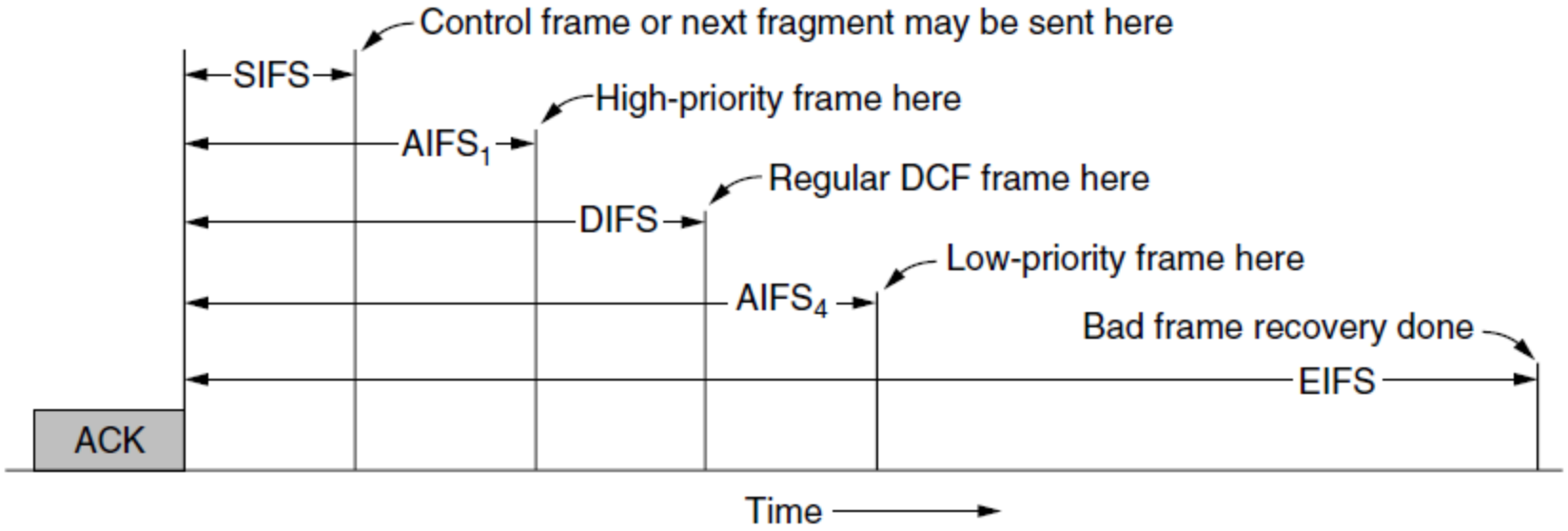
- Virtual channel sensing with the NAV and optional RTS/CTS (often used for long frames) avoids hidden terminals



D does not hear the RTS, but it does hear the CTS, so it also updates its NAV. Note that the NAV signals are not transmitted; they are just kept internally to remind to keep quiet for a certain period of time until other transmission is finished (ACK is received).

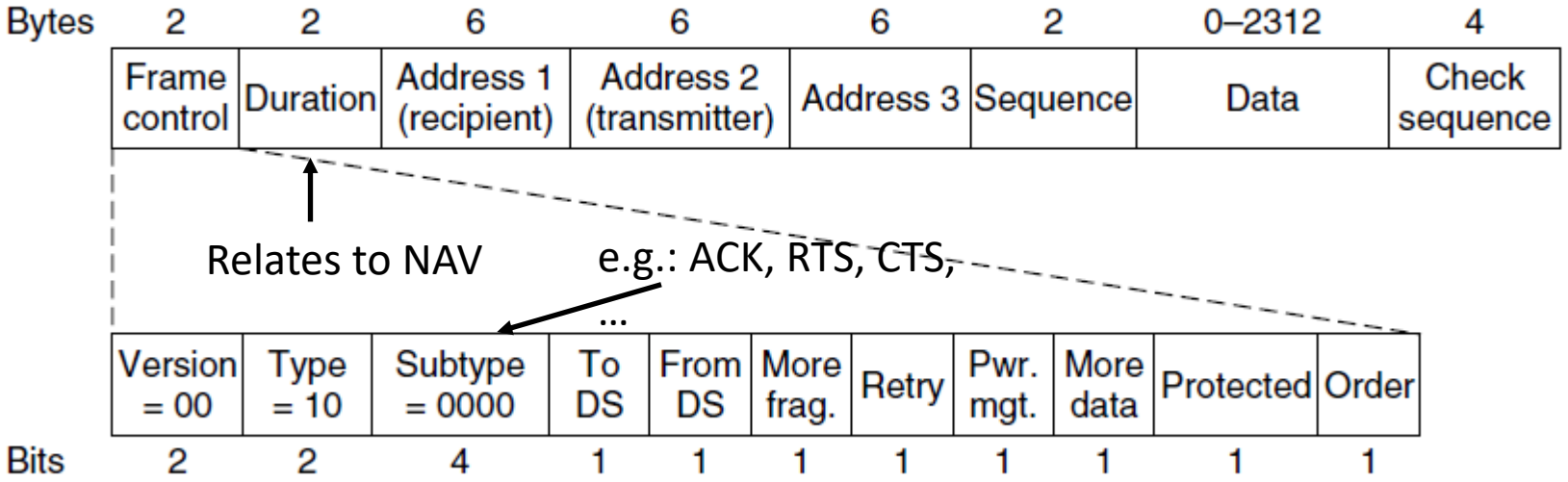
802.11 MAC

- Different backoff slot times add quality of service
  - Short intervals give preferred access, e.g., control, VoIP
- MAC has other mechanisms too, e.g., power save



802.11 Frames

- Frames vary depending on their type (Frame control)
- Data frames have 3 addresses to pass via APs
  - Address 1: Access Point (relay point)
  - Address 2: Sender
  - Address 3: Receiver, after being relayed by AP

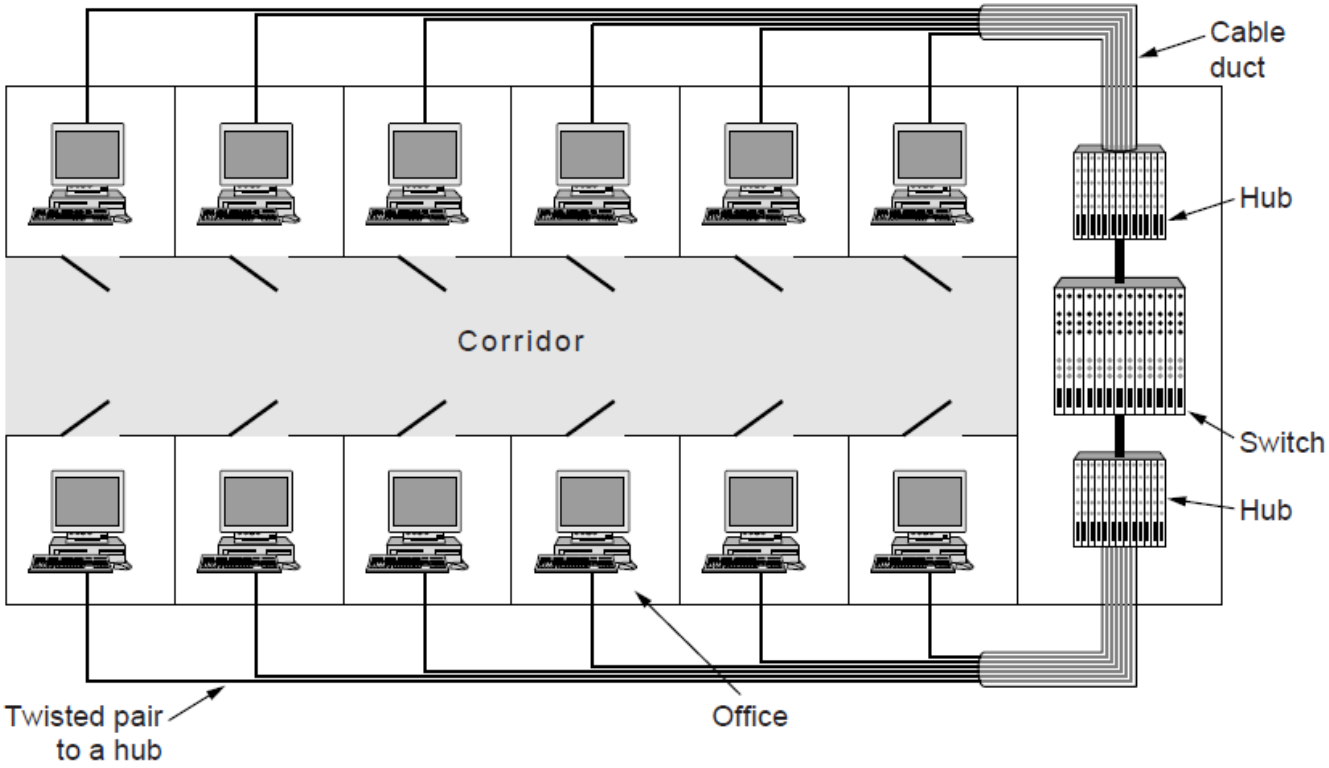


Switch

- Switch
  - “Switch” often used interchangeably with “Bridge”
- Virtual LAN

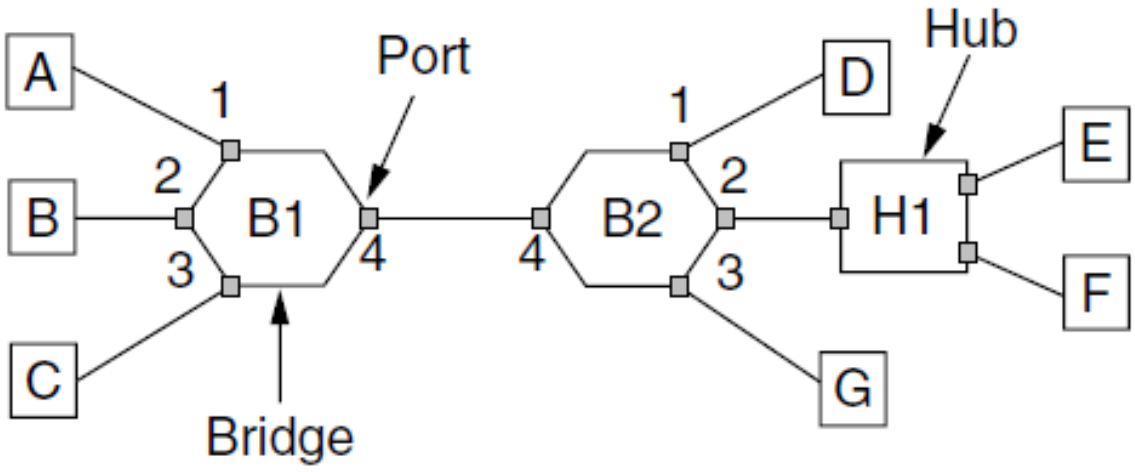
Uses of Bridges

- Common setup is a building with centralized wiring
  - Bridges (switches) are placed in or near wiring closets



Learning Bridges

- A bridge operates as a switched LAN (not a hub)
  - Computers, bridges, and hubs connect to its ports
  - Forwarding table is used for “store-and-forward”.

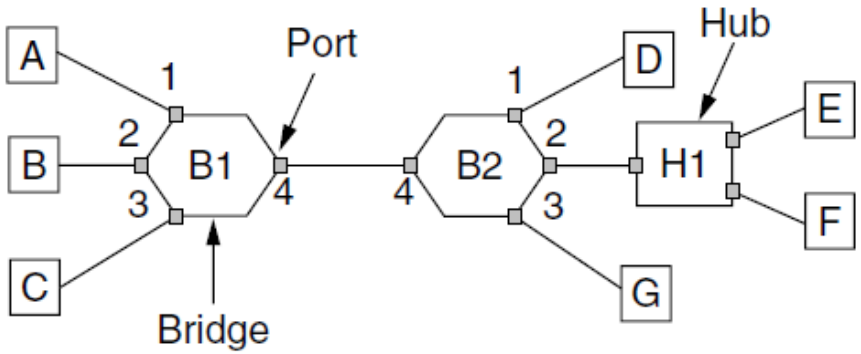


Forwarding Table (B1)	
Destination (MAC address)	Port
A	1
D, E, F, G	4
C	3
B	2

Learning Bridges

- Backward learning algorithm picks the output port:
  - If the port for the destination address is the same as the source port, discard the frame.
  - If the port for the destination address and the source port are different, forward the frame on to the destination port.
  - If the destination port is unknown, use flooding and send the frame on all ports except the source port.
- Needs no configuration
  - Forget unused addresses to allow changes
  - Bandwidth efficient for two-way traffic

Example



Forwarding Table (B1)	
Destination (MAC address)	Port
A	1
D, E, F, G	4
C	3
B	2

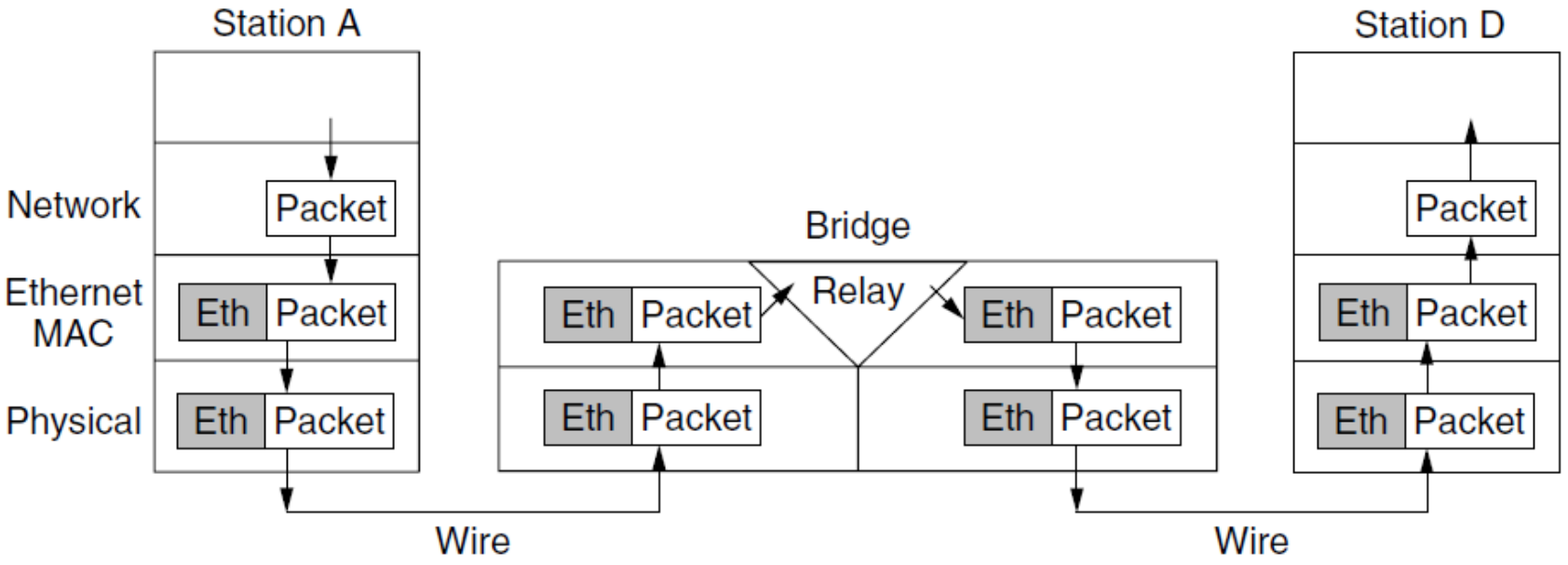
E.g.: A->B
Suppose the forwarding table of B1 is empty.
B1 knows A is sent from port 1, so it adds a new entry;
B1 does not know where is B, so it floods to all other ports (2, 3, 4);

If B1's forwarding table is fully learned, then B1 just forwards the frame from port 2

E.g.: E->F
B2 checks the destination port is the same as the source port, it discards.

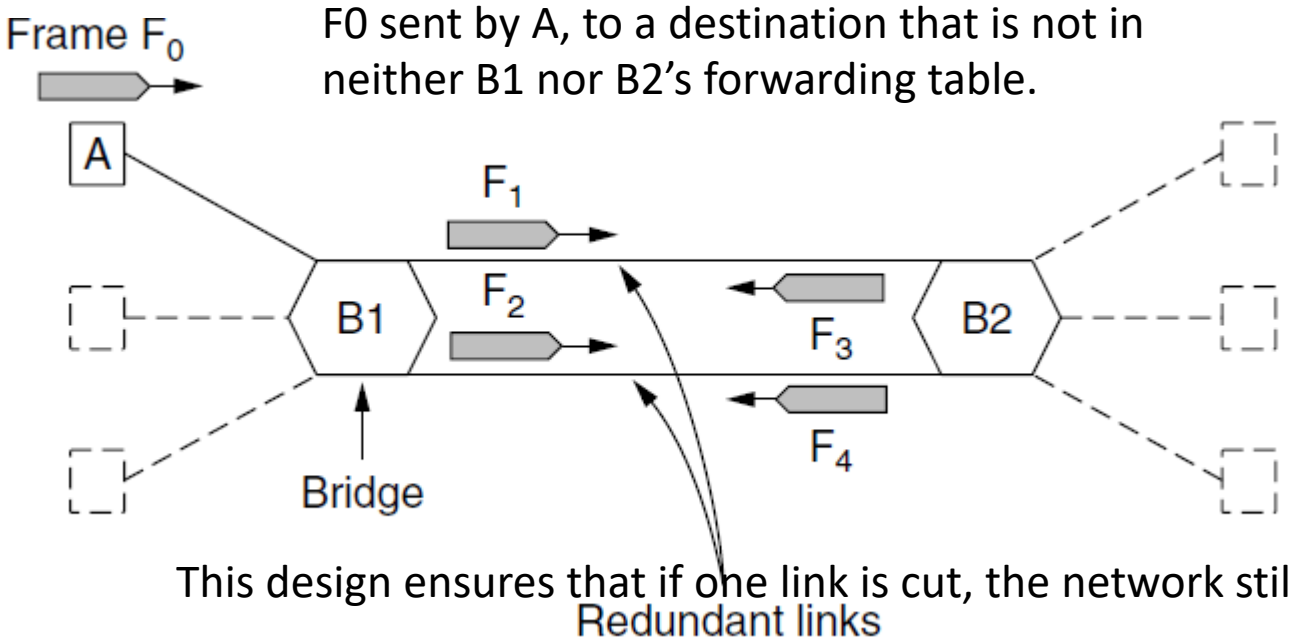
Learning Bridges

- Bridges extend the Link layer:
  - Use but don't remove Ethernet header/addresses
  - Do not inspect Network header



Spanning Tree – Problem

- Bridge topologies with loops and only backward learning will cause frames to circulate forever
  - Need spanning tree support to solve problem



Spanning Tree - Algorithm

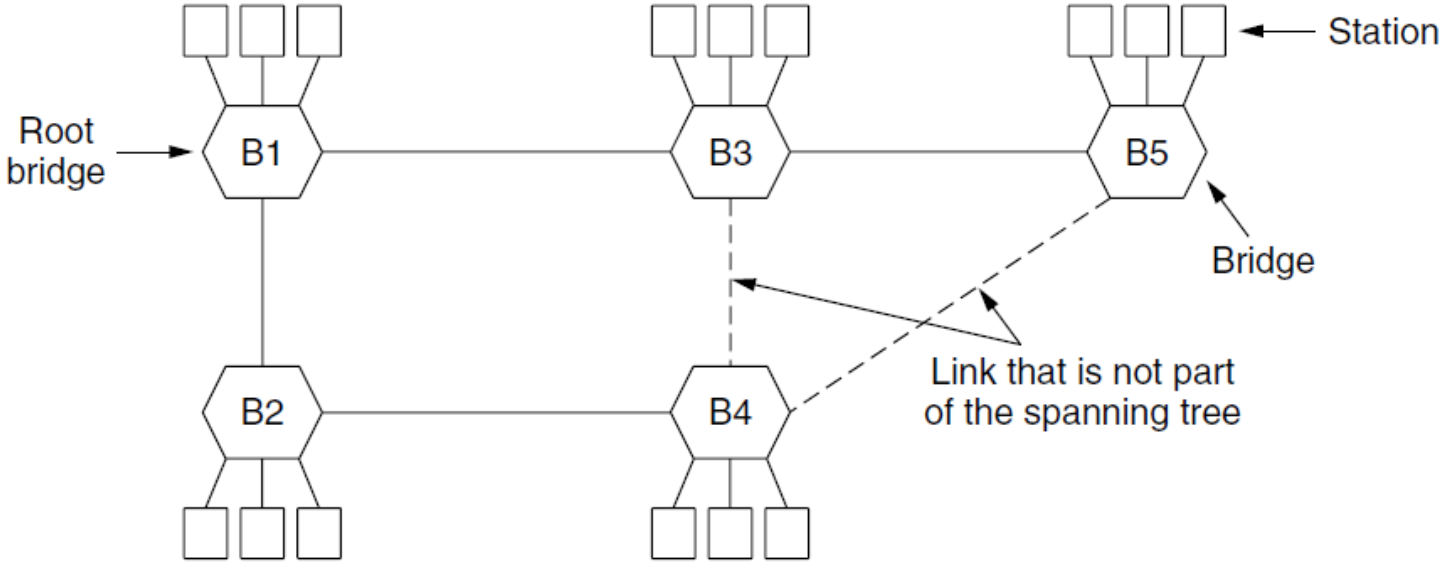
- Subset of forwarding ports for data is use to avoid loops
- Selected with the spanning tree distributed algorithm by Perlman

I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.

– Radia Perlman, 1985.

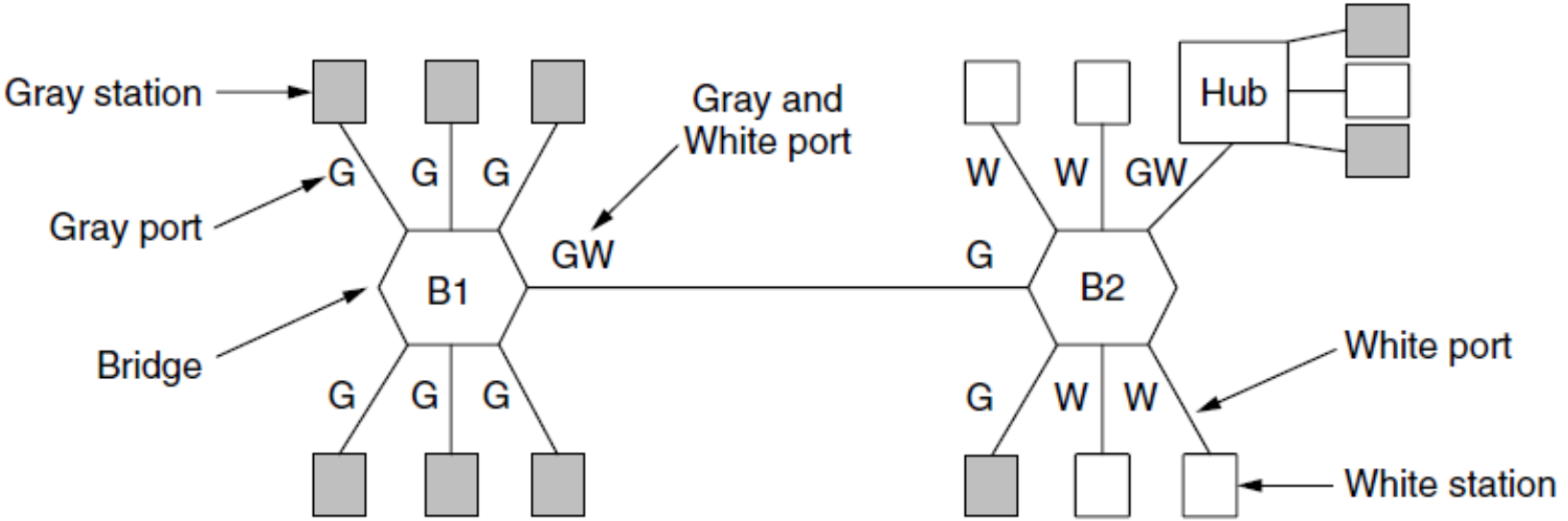
Spanning Tree – Example

- After the algorithm runs:
  - B1 is the root, two dashed links are turned off
  - B4 uses link to B2 (lower identifier than B3 also at distance 1)
  - B5 uses B3 (distance 1 versus B4 at distance 2)



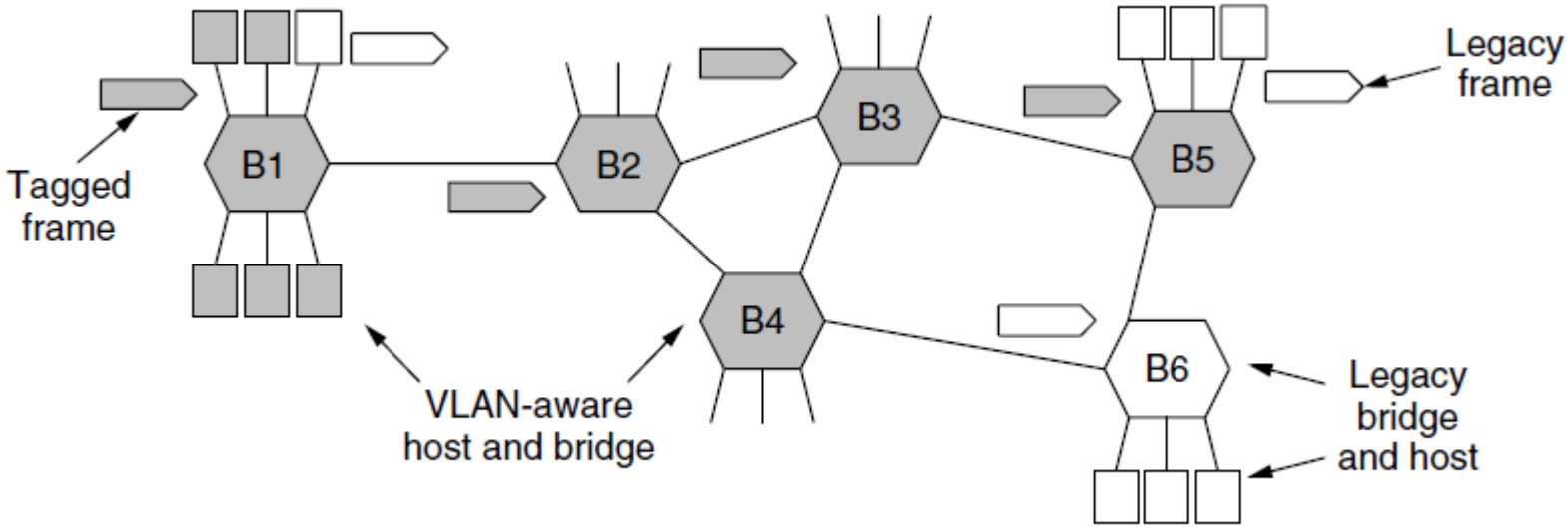
Virtual LANs

- VLANs (Virtual LANs) splits one physical LAN into multiple logical LANs to ease management tasks
  - E.g. Software development team are distributed in different floors in the same building.
  - Ports are “colored” according to their VLAN



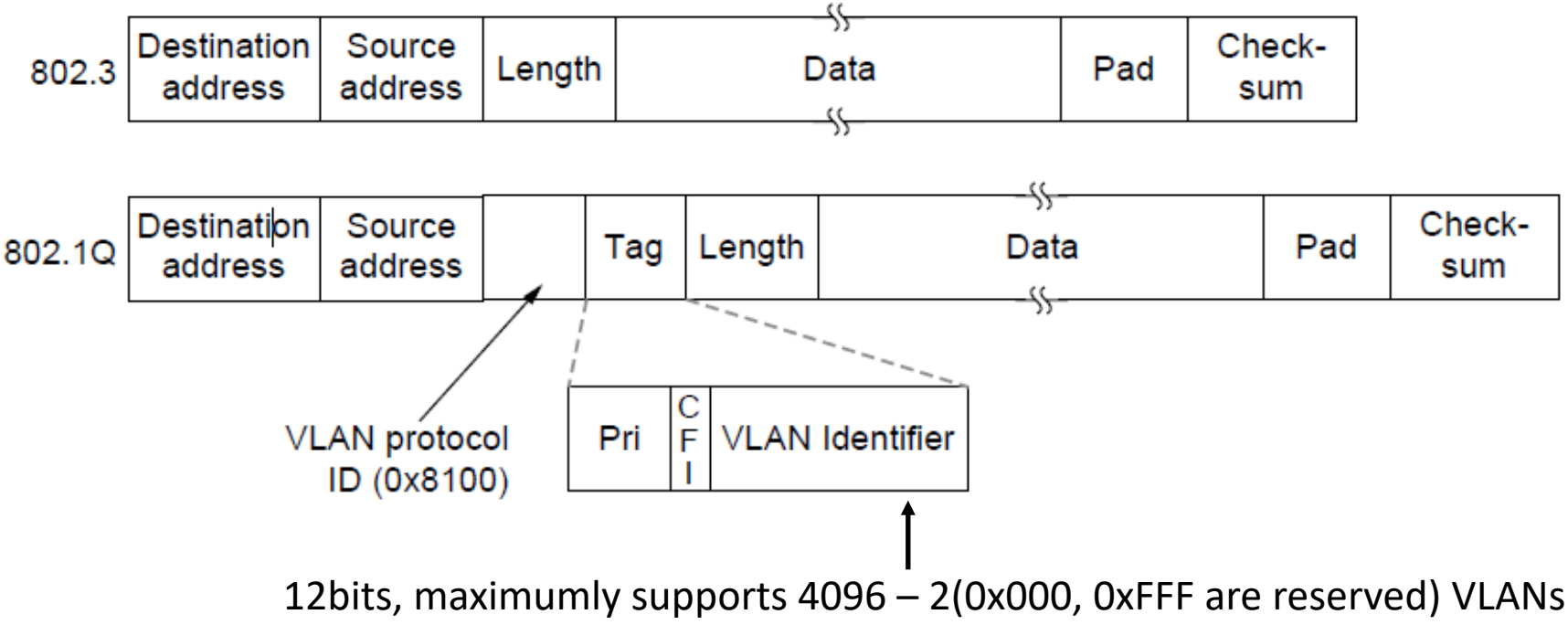
Virtual LANs – IEEE 802.1Q

- Bridges need to be aware of VLANs to support them
  - In 802.1Q, frames are tagged with their "color"
  - Legacy switches with no tags are supported



Virtual LANs – IEEE 802.1Q

- 802.1Q frames carry a color tag (VLAN identifier)
  - Length/Type value is 0x8100 for VLAN protocol

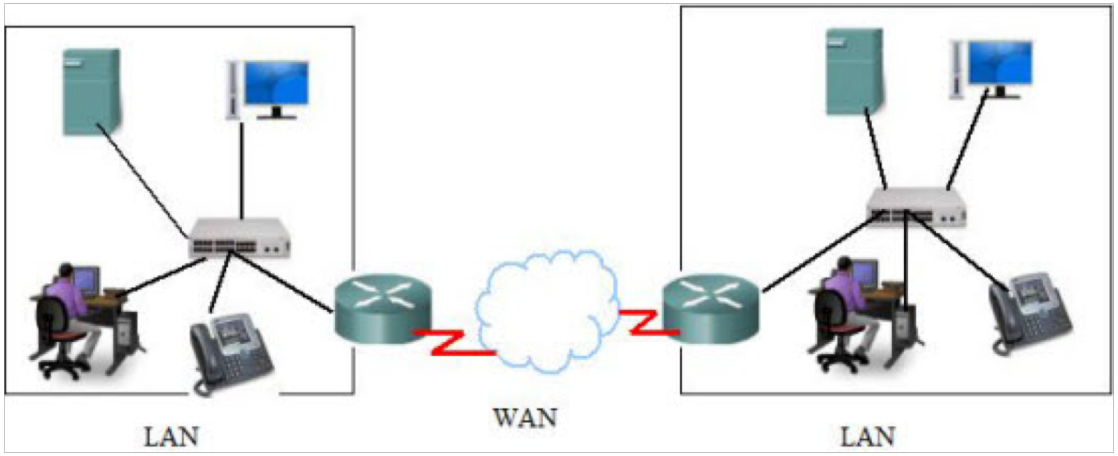


WAN

- Wide Area Network
- PPP
  - Frame Format
  - Compared to HDLC

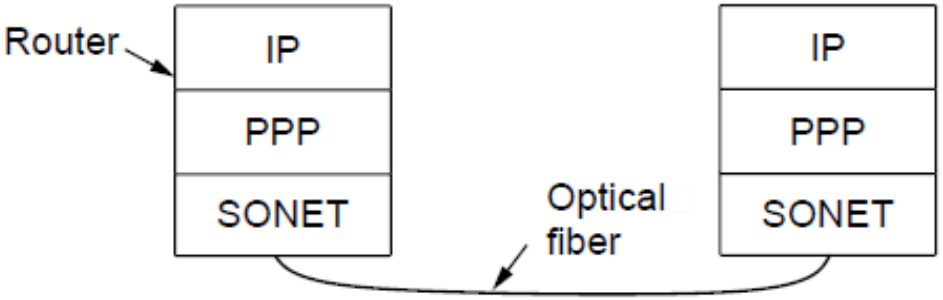
Wide Area Network (WAN)

- WAN and LAN are major components of Internet
- WAN usually uses many switches/routers to connect LANs that are geographically far away.
- WAN: up to layer 3; LAN: up to layer 2
- WAN: Point-to-Point; LAN: Multi-Point Access

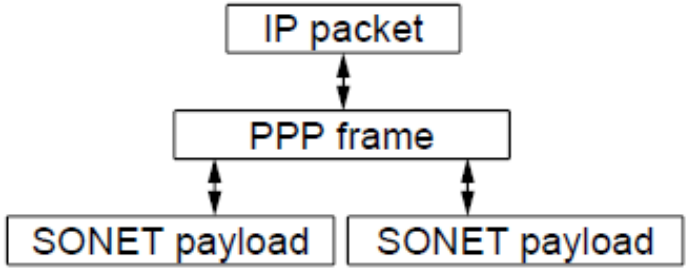


Packet over SONET

- Packet over SONET is the method used to carry IP packets over SONET optical fiber links
  - Uses **PPP** (Point-to-Point Protocol) for framing



Protocol stacks

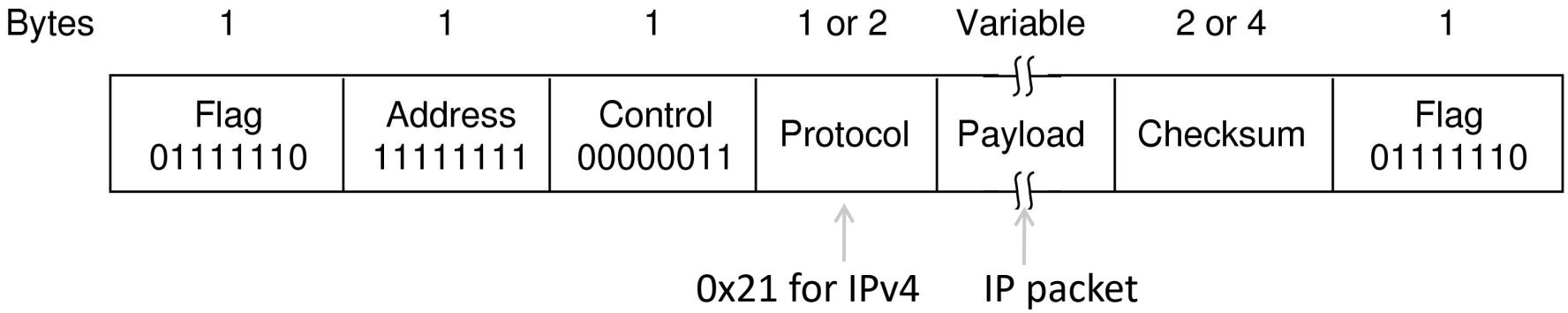


PPP frames may be split over SONET payloads

SONET is the physical layer protocol that is most commonly used over the wide-area optical fibre links that make up the backbone of communications networks, including the telephone system.

PPP

- PPP (Point-to-Point Protocol) is a general method for delivering packets across links
  - Framing uses a flag (0x7E) and byte stuffing
  - "Unnumbered mode" (connectionless unacknowledged service) is used to carry IP packets
  - Errors are detected with a checksum
  - Address field always "one" (all stations can receive)



Compared to HDLC

- High-level Data Link Control
  - widely used instance of an earlier family of protocols, the predecessor of PPP.

- The differences between PPP and HDLC:
  - PPP is byte oriented rather than bit oriented.
    - PPP uses byte stuffing and all frames are an integral number of bytes. HDLC uses bit stuffing and allows frames of, say, 30.25 bytes.
  - HDLC provides reliable transmission with a sliding window, acknowledgements, and timeouts in the manner we have studied.
    - PPP only ensures that the received frames are correct. As the current transmission links for WAN are more reliable than the old one that HDLC is designed for.