CHAPTER 4
THE MEDIUM ACCESS CONTROL (MAC) **SUBLAYER** (介质访问子层)

- The channel allocation problem
- Multiple access protocols
- 802.3: Ethernet
- 802.11: Wireless LANs
- Data link layer switching
- 802.15: Bluetooth*
- 802.16: Broadband wireless*
- RFID*

THE CHANNEL ALLOCATION PROBLEM

- Two types of networks:
  - Those using **point-to-point** connection.
  - Those using **broadcast** channels.
- In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it.
  - Consider a telephone conference call.
  - Broadcast channels are sometimes 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 the MAC (Medium Access Control). The MAC sublayer is the bottom part of the data link layer.

The Channel Allocation Problem: Introduction

- 信道分配问题: How to allocate a single broadcast channel among competing users
  - **Static channel allocation** in LANs and MANs
    - TDM
    - FDM
  - **Dynamic channel allocation** in LANs and MANs
    - ALOHA
    - CSMA
    - Collision free protocols
    - Limited-contention protocols
    - …

The Channel Allocation Problem: **Static** channel allocation in LANs and MANs

The traditional way of allocating a single channel among multiple competing users is Frequency Division Multiplexing (FDM, 频分多路复用).

- When there is only a small and fixed number of users, each of which has a heavy (buffered) load of traffic, FDM is a simple and efficient allocation.
- When the number of senders is large and continuously **varying** or the traffic is **bursty**, FDM has some problems.

The Channel Allocation Problem:
Static channel allocation in LANs and MANs

- Mathematical analysis

- Similar for other static channel allocation methods such as TDM (Time Division Multiplexing)

The Channel Allocation Problem:
Dynamic channel allocation in LANs and MANs

Five key assumptions for the channel allocation problem

1. Independent Traffic (独立传输). The model consists of *N* independent stations, each with a program or user that generates frames for transmission.
2. Single channel (单信道假设). A single channel is available for all communication.
3. Collision assumption (冲突假设).
4. Time assumption (时间假设): (a) Continuous Time.(b) Slotted Time.
5. Carrier assumption (载波假设): (a) Carrier Sense.(b) No Carrier Sense.

MULTIPLE ACCESS PROTOCOLS

- ALOHA
- Carrier Sense Multiple Access (CSMA) protocols
- Collision-free protocols
- Limited contention protocols

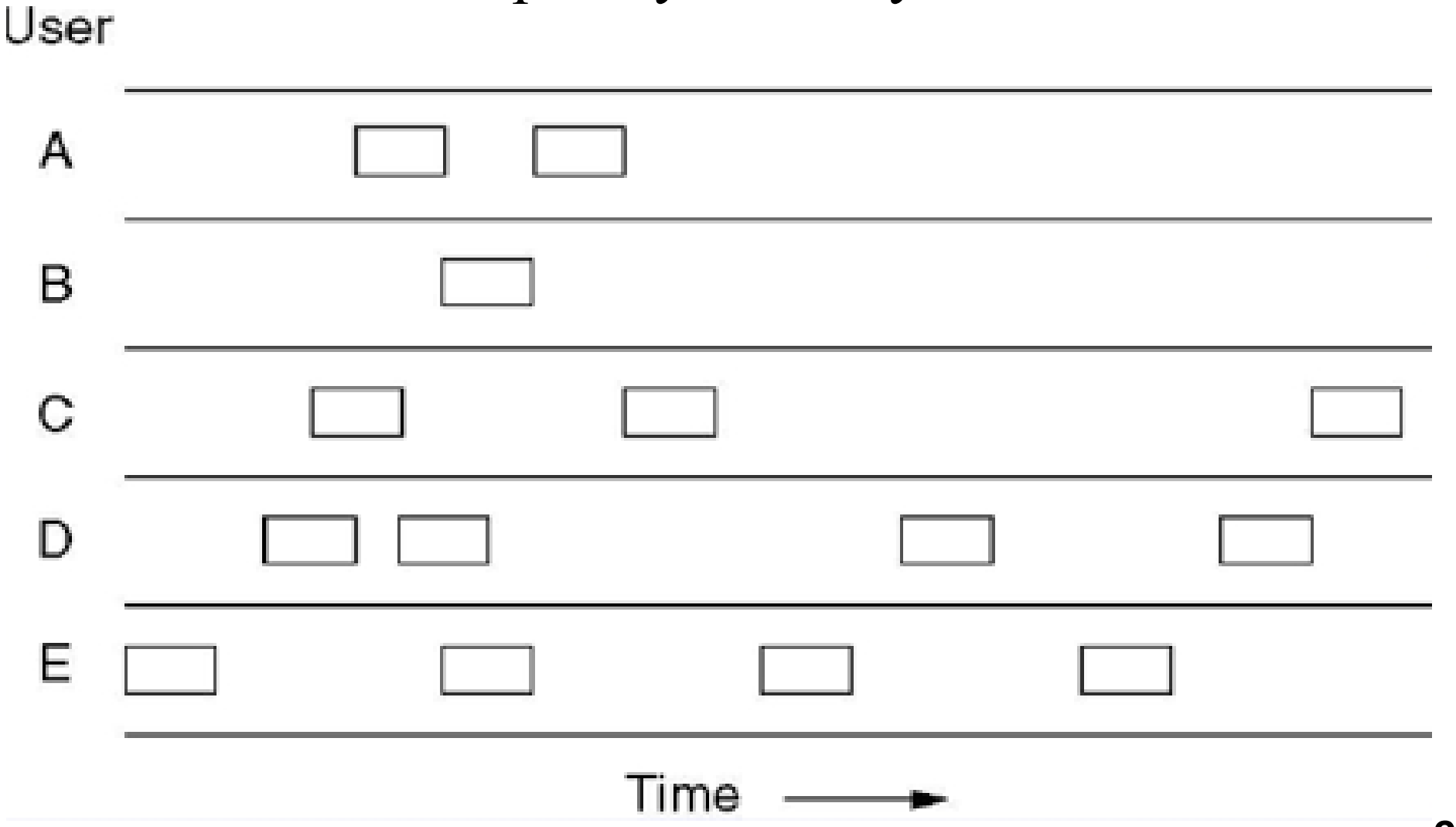
- Wireless LAN Protocols

Multiple Access Protocols: ALOHA

- Let users transmit whenever they have data to be sent.
  - There will be collisions and the colliding frames will be destroyed.
  - The sender just waits a random amount of time and sends it again if a frame is destroyed.
- Two types of ALOHA:
  - Pure ALOHA
  - Slotted ALOHA

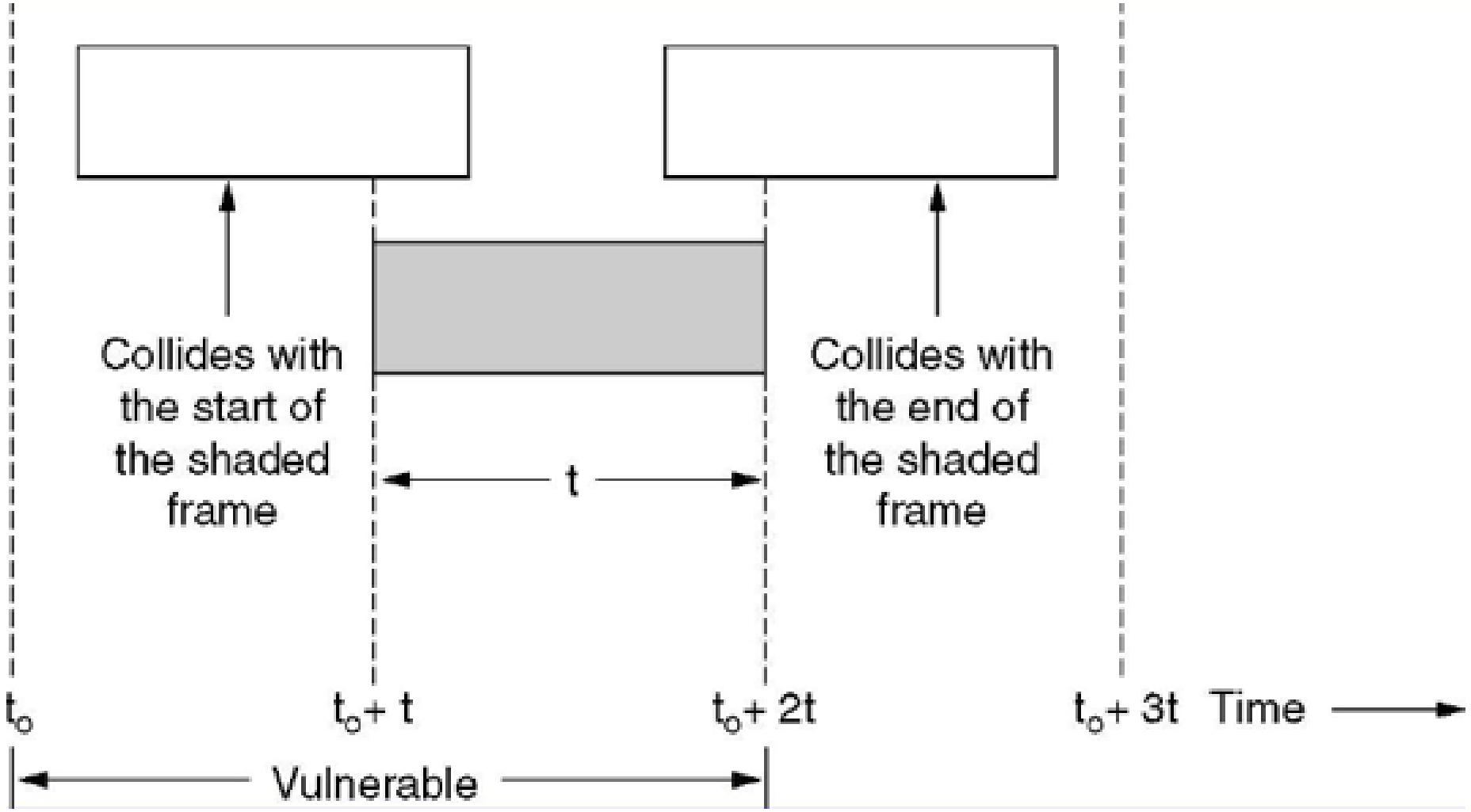
Multiple Access Protocols: ALOHA

In pure ALOHA, frames are transmitted at completely arbitrary times.



Multiple Access Protocols: ALOHA

Vulnerable period for the shaded frame.

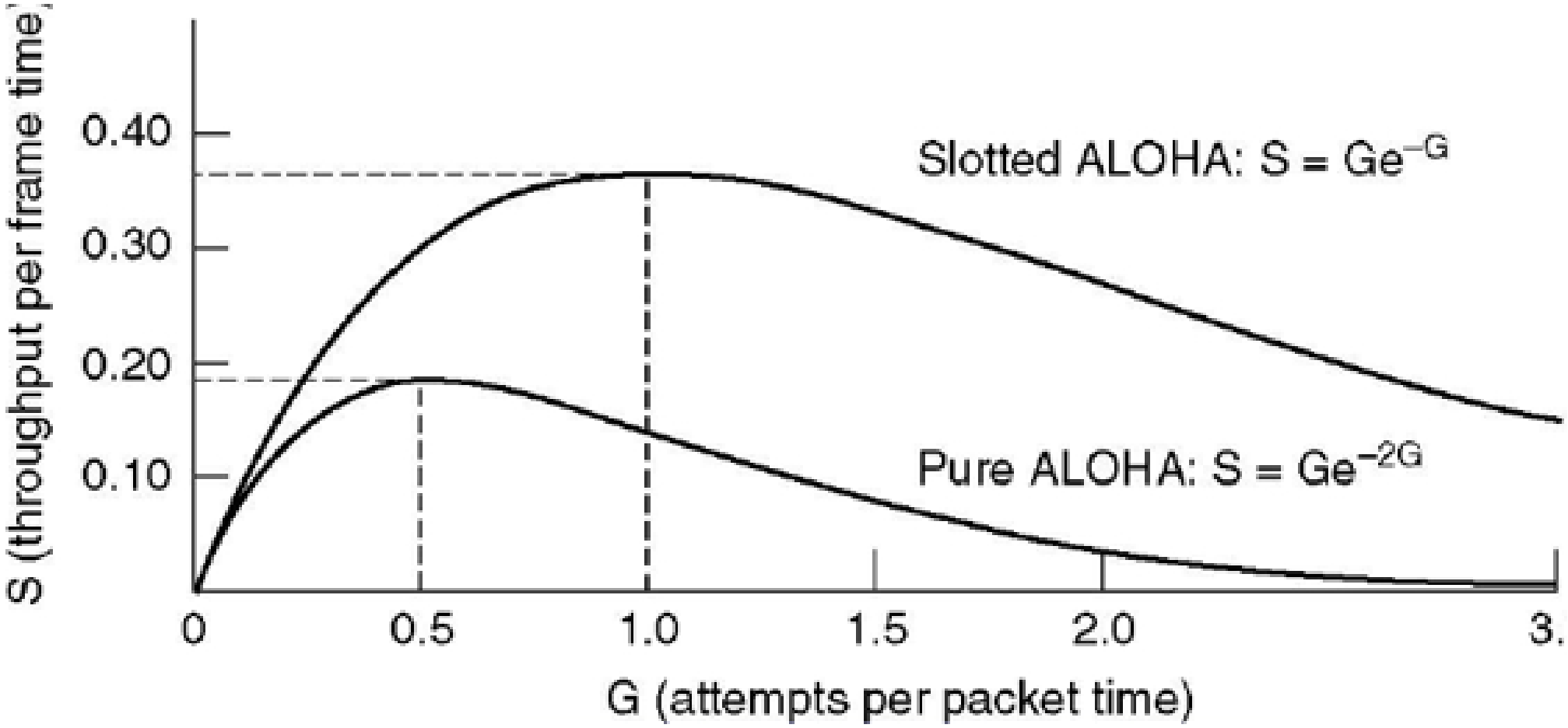


Multiple Access Protocols: Efficiency of ALOHA

- Concepts:
  - Frame time: frame length / bit rate
  - A station generates N (Poisson mean) new frames per frame time
  - Offered load: G (Poisson mean) transmission attempts per frame time. G includes old and new.
    - At low loads: $G \approx N$
    - At high loads: $G > N$
  - Throughput $S = GP_0$ where P_0 is the probability that a frame does not suffer a collision.

Multiple Access Protocols: ALOHA

Throughput versus offered traffic for ALOHA systems.



Multiple Access Protocols: Slotted ALOHA

- In 1972, Roberts published a method for doubling the capacity of an ALOHA system.
- **Time is slotted**. A computer is not permitted to send at any time. Instead it is required to wait for the beginning of the next slot.
- **The vulnerable period is halved for Slotted ALOHA**.
- **Note**: Protocols that are perfectly valid fall into disuse for political reasons, but years later some clever person realizes that a long-discarded protocol solves his current problem.

→ Study many protocols that are in current use.

→ Study a number of elegant protocols that are not currently in widespread use, but might easily be used in future applications.

Multiple Access Protocols: CSMA

- With stations transmitting at will, without paying attention to what the other stations are doing, there are bound to be many collisions,
  不听就说→ poor channel utilization.
- If stations can detect what other stations are doing and adjust their behavior accordingly,
  先听再说→ better channel utilization.
- Protocols in which stations listen for a carrier and act accordingly are called Carrier Sense Multiple Access Protocols (CSMA Protocols, 载波侦听多路访问协议).

Multiple Access Protocols: CSMA

- CSMA (Carrier Sense Multiple Access) without CD (Collision Detection)
  - Persistent CSMA
  - Non-persistent CSMA
  - p-persistent CSMA

- CSMA with CD

Multiple Access Protocols:
CSMA without CD: Persistent CSMA

Before sending, a station senses the channel.

- If the channel is **idle**, the station **transmits** a frame.
- If the channel is **busy**, the station **waits** until it becomes idle. Then the station transmits a frame.
- If a **collision occurs**, the station **waits a random amount of time** and starts all over again.

The protocol is called *1-persistent* because the station transmits with a probability of 1 whenever it finds the channel idle.

Multiple Access Protocols:
CSMA without CD: Persistent CSMA

Discussion

- This scheme seems to avoid collisions except for the rare case of simultaneous sends, but in fact it does not.
- If two stations become ready in the middle of a third station's transmission,
  - both will wait politely until the transmission ends,
  - both will then begin transmitting exactly simultaneously, resulting in a collision.
- If they were not so impatient, there would be fewer collisions.

Multiple Access Protocols:
CSMA without CD: Persistent CSMA

Discussion (Cont)

- propagation delay has an important effect on collisions
  - There is a chance that just after a station begins sending, another station will become ready to send and sense the channel.
  - If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision.
  - This chance depends on the number of frames that fit on the channel, or the bandwidth-delay (BD) product of the channel
    - Low BD product → small chance of collision
    - Large BD product → high chance of collision
- Better than ALOHA.

Multiple Access Protocols:
CSMA without CD: Non-persistent CSMA

- Before sending, a station senses the channel.
  - If the channel is **idle**, the station **transmits** a frame.
  - If the channel is **in use**, the station ***does not*** continually sense it. Instead, it **waits a random period of time** and then repeats the algorithm.
  - If a **collision occurs**, the station **waits a random amount of time** and starts all over again.
- Discussion
  - Better channel utilization than 1-persistent CSMA (less greedy)
  - Longer delays than 1-persistent CSMA

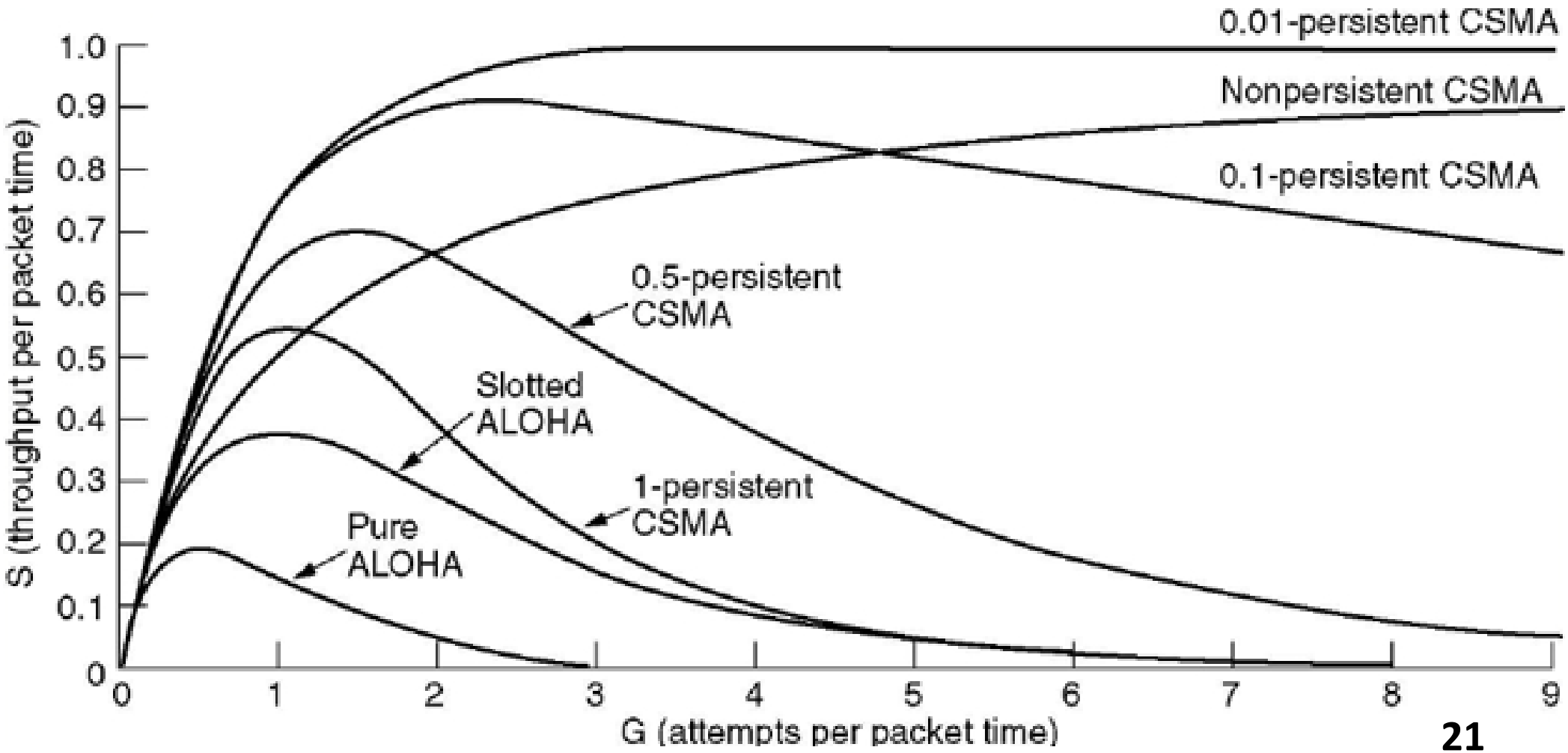
Multiple Access Protocols:
CSMA without CD: p-persistent CSMA

- Applied to slotted channels
- Before sending, a station senses the channel:
  - If the channel is **idle**, it **transmits with a probability *p***. With a probability $q=1-p$, it defers until the next slot.
  - If that slot is also idle, it either transmits or defers again, with probabilities p and q.
  - This process is repeated until either the frame has been transmitted or another station has begun transmitting.
  - If the channel is **busy**, it **waits until the next slot** and applies the above algorithm.

IEEE 802.11 uses a refinement of p-persistent CSMA

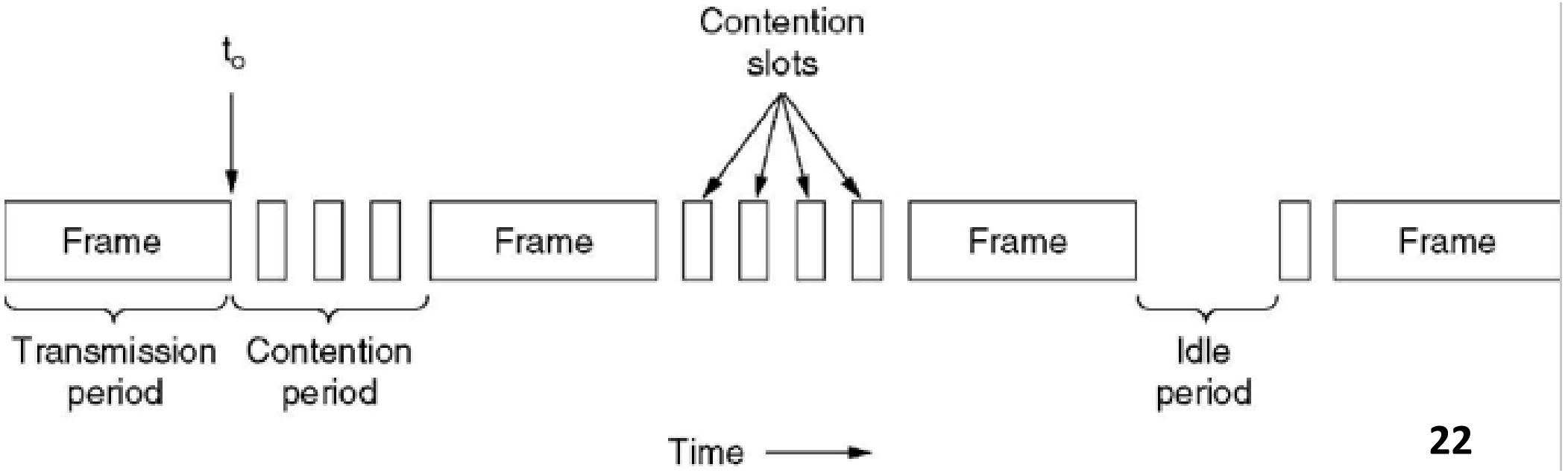
Multiple Access Protocols:
CSMA without CD: Comparison

Comparison of the channel utilization versus load for various random access protocols.



Multiple Access Protocols: CSMA with CD

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
  - is an improvement over CSMA without CD.
  - As soon as stations detect a collision, they stop their transmissions.
- CSMA/CD can be in one of three states: **contention**, **transmission**, or **idle**.

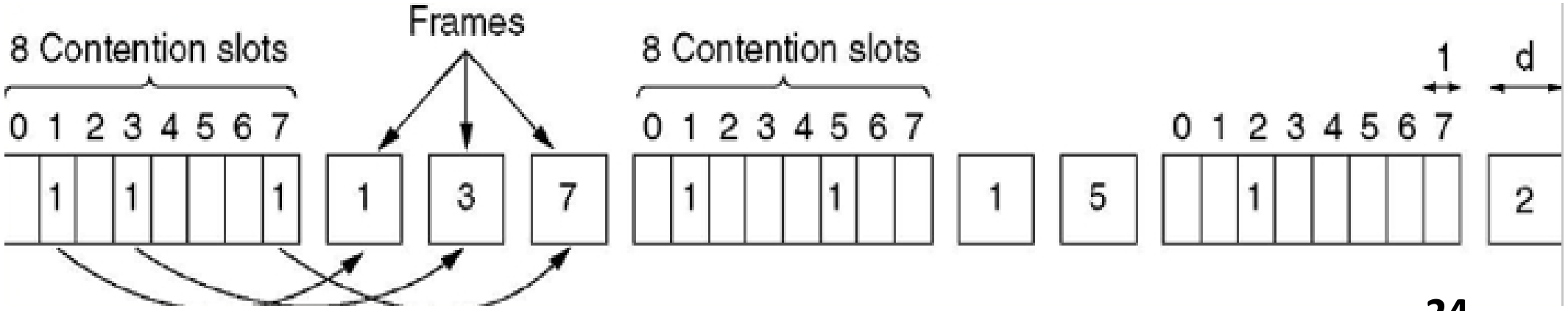


Multiple Access Protocols: CSMA with CD

- How long will it take to detect collisions?
  - The time for transmitting one full frame?
  - The time for transmitting from one end to the other end of the cable?
  - In the worst case, a station cannot be sure that it has seized the channel until it has transmitted for 2τ without hearing a collision. Here τ is the time for a signal to propagate between the two farthest stations. (See later)

Multiple Access Protocols:
Collision free protocols: A Bit-Map Protocol

- Each contention period consists of exactly N slots.
- In general, station i inserts 1 in time slot i in order to send data.
- After all N slots have passed by, each station has complete knowledge of which stations wish to transmit. Then they begin transmitting in numerical order. **Since everyone agrees on who goes next, there will never be any collisions**.
- After the last ready station has transmitted its frame, another N bit contention period is begun.



Multiple Access Protocols:
Collision free protocols: A Bit-Map Protocol

- Notations:
  - The time unit is one contention bit
  - N: contention period
  - d: data frame length
- At low load:
  - Delay for low-numbered stations: $0.5N + 1N = 1.5N$
  - Delay for high-numbered stations: $0.5N$

  → The mean delay for all stations is N.

  → The efficiency: $\mathrm{d}/(N + d)$.
- At high load:
  - the N bit contention period is distributed over N frames, yielding an overhead of only 1 bit per frame,

  → the efficiency: $d/(d + 1)$.

Multiple Access Protocols:
Collision free protocols: Token Passing

- Token passing
  - The token represents permission to send.
  - If a station has a queued frame when it receives the token, it can send that frame before it passes the token to the next station.
  - If a station has no queued frame, it simply passes the token
- Two kinds of token passing
  - Token ring
  - Token bus

Multiple Access Protocols:
Collision free protocols: Token Ring

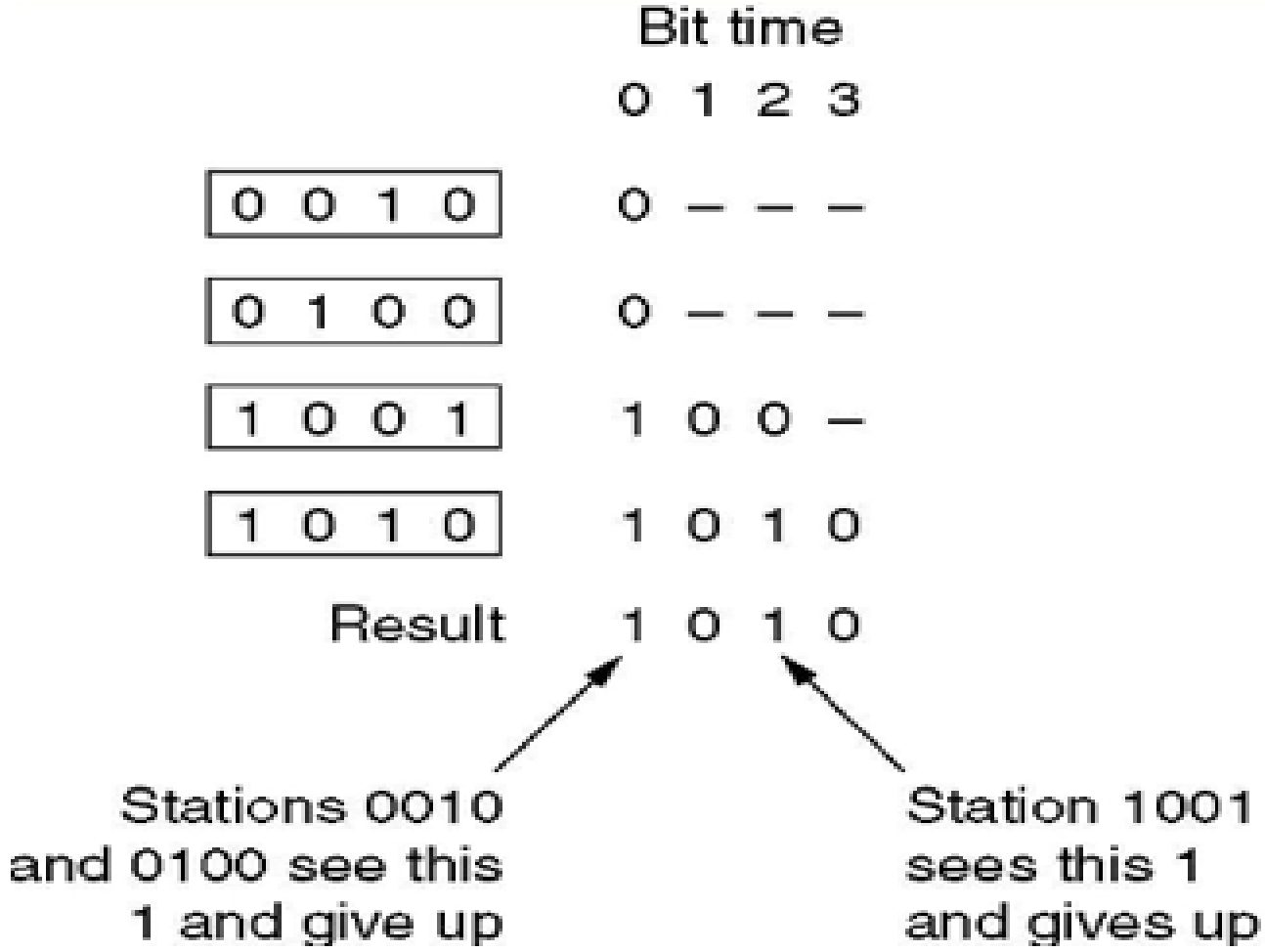
- For a ***token ring*** protocol, the stations are connected one to the next in a single ring.
- Passing the token to the next station then simply consists of receiving the token in from one direction and transmitting it out in the other direction.
- This way they will circulate around the ring and reach whichever station is the destination.
- Since all positions in the cycle are equivalent, there is no bias for low- or high-numbered stations.
- Examples: 802.5 (1980s), FDDI (1990s), RPR (Resilient Packet Ring, 802.17) (2000s), …

Multiple Access Protocols:
Collision free protocols: Binary Countdown

- A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high-order bit. All addresses are assumed to be the same length.
- The bits in each address position from different stations are BOOLEAN ORed together by the channel when they are sent at the same time.
- To avoid conflicts, an arbitration rule must be applied: as soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up.

Multiple Access Protocols:
Collision free protocols: Binary Countdown

The binary countdown protocol.
A dash indicates silence.



Multiple Access Protocols:
Limited-Contention protocols

- Methods with contention
  - ***Under low load***, the contention method (i.e., pure or slotted ALOHA, CSMA) is preferable due to its low delay.
  - ***Under high load***, the contention method becomes increasingly less efficient.
- Methods without contention
  - Under low load, the collision-free method has high delay.
  - Under high load, the collision-free method becomes increasingly more efficient.

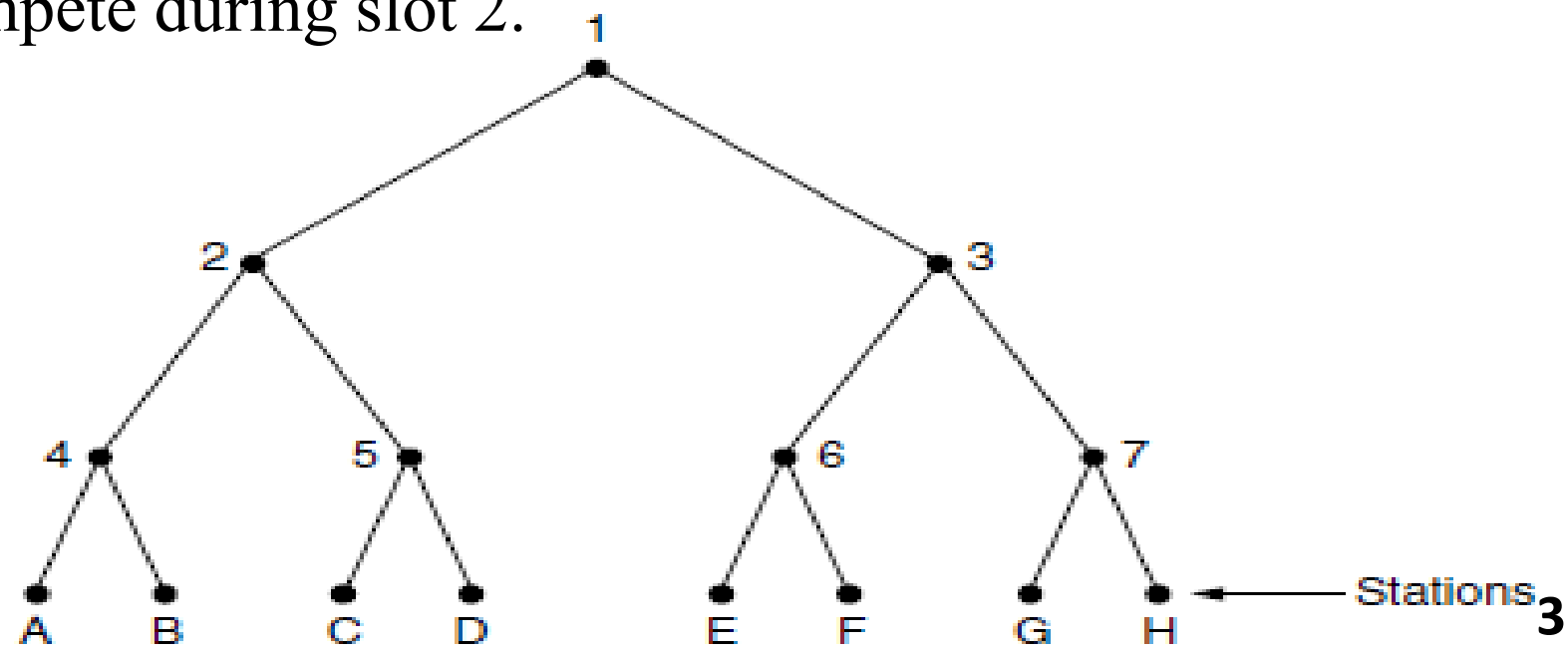
→ Limited-Contention Protocols

Multiple Access Protocols: Limited-Contention protocols

- What we need is a way to assign stations to slots dynamically
  - With many stations per slot when the load is low
  - With a few stations per slot when the load is high.
- Adaptive Tree Walk Protocol (自适应树搜索协议)

Multiple Access Protocols: Adaptive Tree Walk

- the stations as the leaves of a binary tree
- In **slot 0**, all stations are permitted to try to acquire the channel.
- If one of them does so, fine.
- If there is a **collision**, then during slot 1 only those **stations falling under node 2** in the tree may **compete**.
- If one of them acquires the channel, the slot following the frame is **reserved for stations under node 3**.
- If there is **collision** under node 2 for slot 1, **stations under node 4** may compete during slot 2.

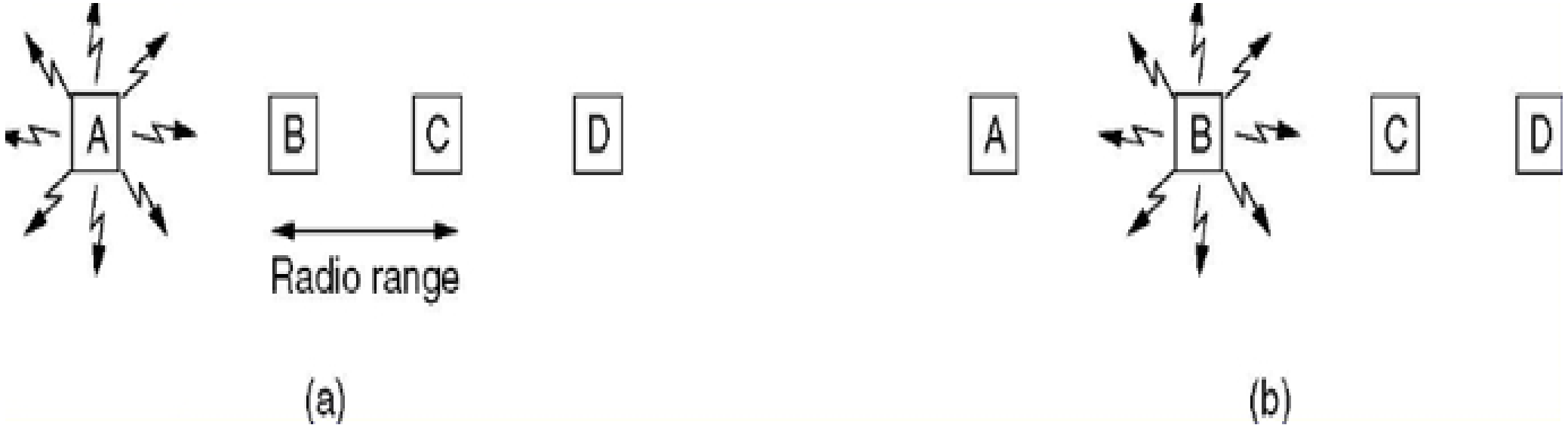


Multiple Access Protocols: Adaptive Tree Walk

- Adaptive Tree Walk Protocol
  - At what level in the tree should the search begin?
  - The heavier the load, the farther down the tree the search should begin.
  - Begin at $i = \log_2 q$ where q is the estimate of the number of ready stations.
  - Numerous improvements to the basic algorithm have been discovered (Bersekas and Gallager, 1992)

Multiple Access Protocols: Wireless LAN Protocols

- Hidden station problem (隐藏终端问题)
- Exposed station problem (暴露终端问题)



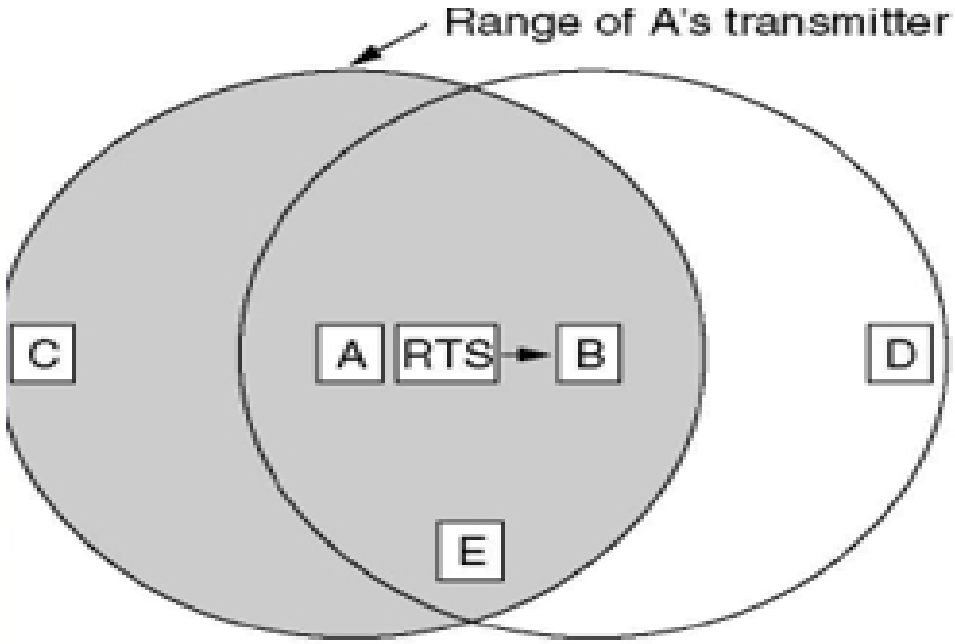
- The problem is that **before starting a transmission, a station really wants to know whether or not there is activity around the receiver not the sender.**

Multiple Access Protocols: Wireless LAN Protocols

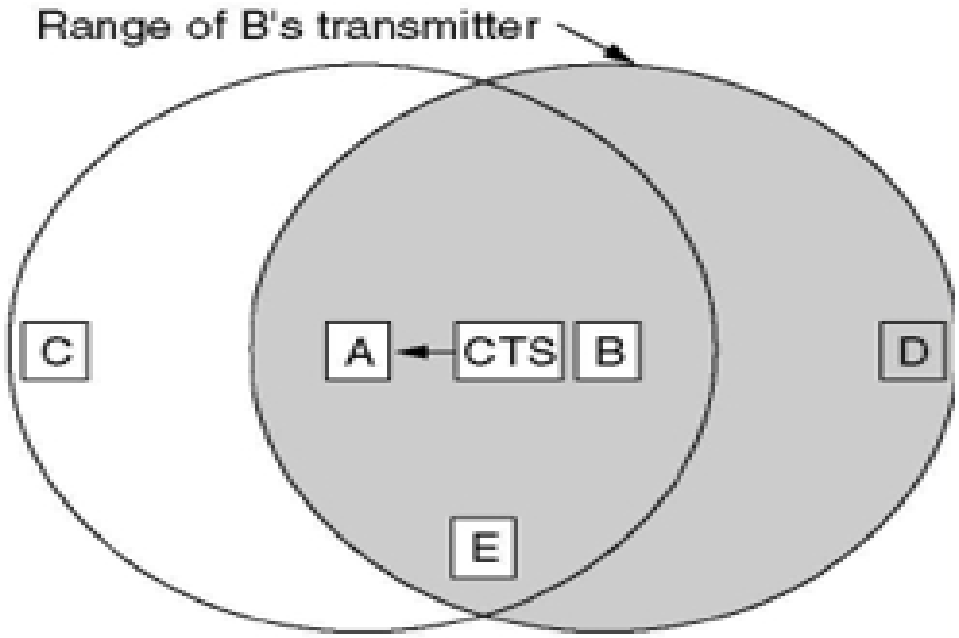
The MACA (Multiple Access with Collision Avoidance) protocol. A sending an RTS to B, B responding with a CTS to A.

1. D: A's hidden terminal, hear CTS and stop data
2. E: hear RTS and CTS, stop data
3. C: A's exposed terminal, hear RTS, wait until CTS, can transmit data

Collision can still occur, e.g. RTS



(a)



(b)

IEEE 802.3 (Ethernet)

- Classic Ethernet Physical Layer
- Classic Ethernet MAC Sublayer Protocol
- Ethernet Performance

- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10-Gigabit Ethernet

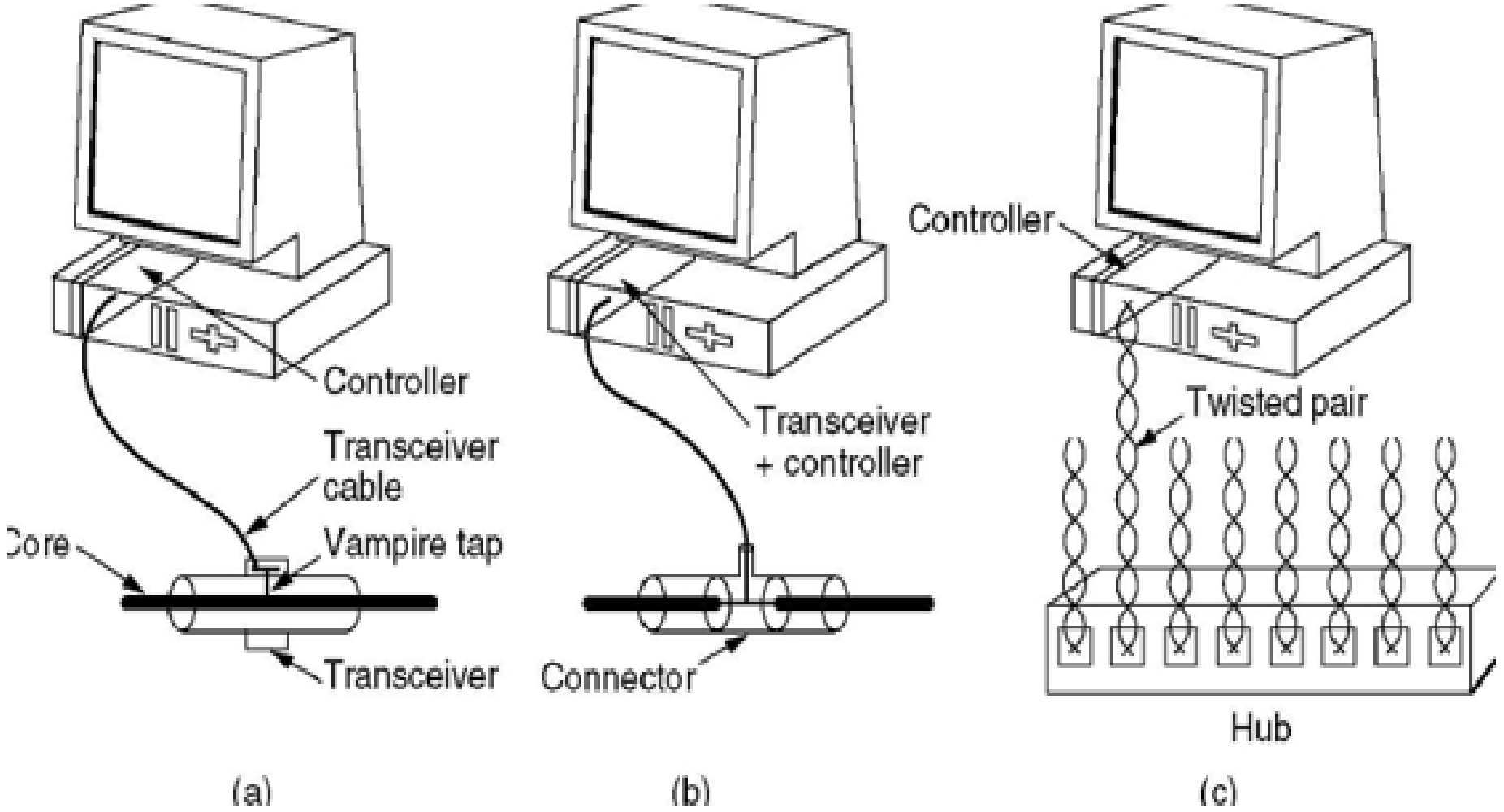
- Retrospective on Ethernet

802.3: Classic Ethernet Physical Layer

- 197x: the real beginning was the ALOHA system constructed to allow radio communication between machines scattered over the Hawaiian Islands.
- Bob Metcalf is interested in Norman Abramson's work → after PhD graduation, Bob spend the summer in Hawaii working with Abramson (before work at Xerox PARC) → first local area network (Ethernet)
- The Ethernet was so successful. **Xerox**, **DEC**, and **Intel** drew up a standard for 10-Mbps Ethernet. (DIX standard)
- 802.3 standard describes a whole family of 1-persistent CSMA/CD system, running at speeds from 1 to 10-Mbps over various media. (802.3 standard)

802.3: Classic Ethernet Physical Layer

Three kinds of Ethernet cabling. (a)10Base5 (thick Ethernet), (b) 10Base2 (thin Ethernet), (c) 10Base-T.



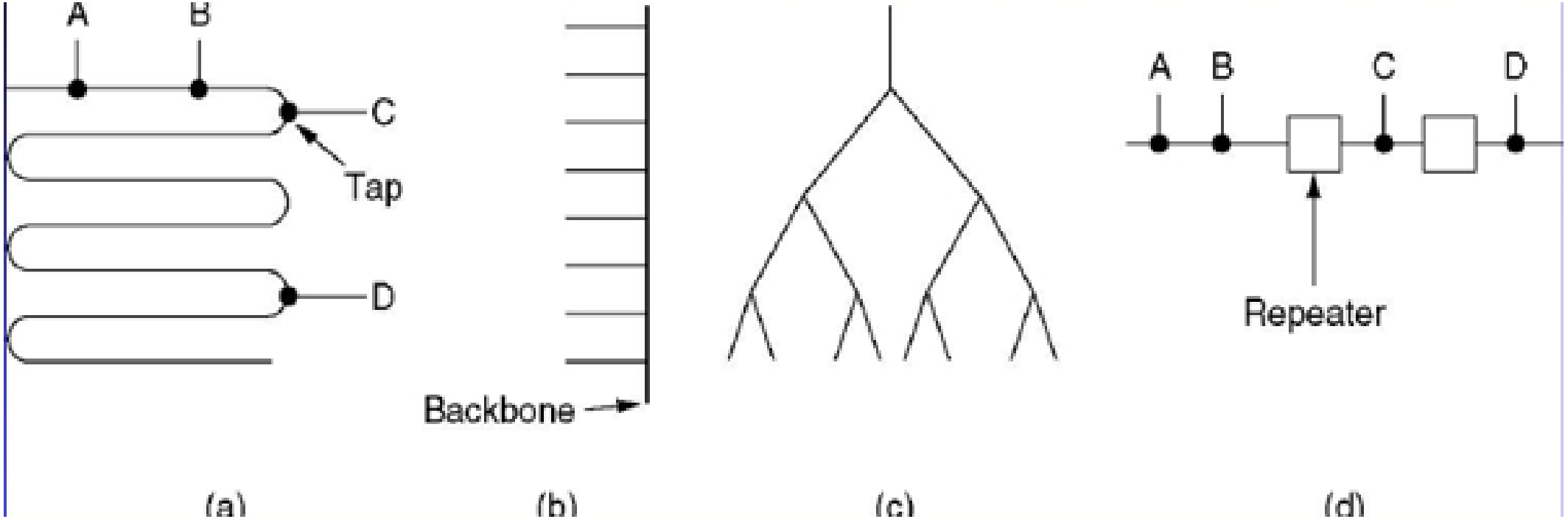
802.3: Classic Ethernet Physical Layer

The most common kinds of
Classic Ethernet cabling.

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

802.3: Classic Ethernet Physical Layer

Cable topologies.
(a) Linear, (b) Spine, (c) Tree, (d) Segmented.



802.3: Classic Ethernet Physical Layer

- With 0 volts for a 0 bit, with 5 volts for a 1 bit.
  - Difficult to tell the difference between an idle sender (0 volts) and a 0 bit (0 volts).

  → If one station sends the bit string 0001000, others might falsely interpret it as 1000000 or 01000000.
- With –1 volts for a 0 bit, with 1 volts for a 1 bit
  - A receiver may sample the signal at a slightly different frequency than the sender used to generate it

  → can be out of synchronization.
- To unambiguously determine the start, end, or middle of each bit without reference to an external clock.
  - **Manchester** encoding
  - **Differential Manchester** encoding

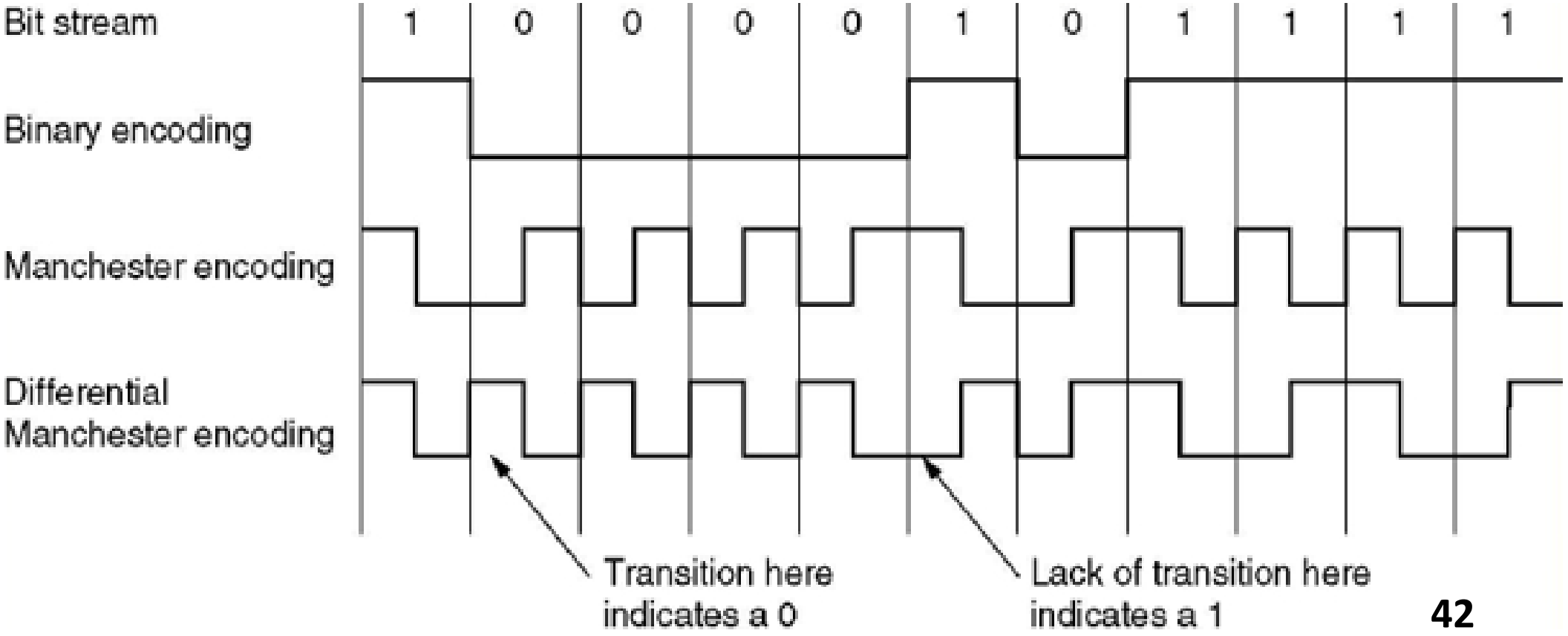
802.3: Classic Ethernet Physical Layer

Manchester encoding (used by Ethernet):

0: low-high; 1: high-low;

Differential Manchester encoding (used by Token Ring):

0: presence of transition; 1: absence of transition



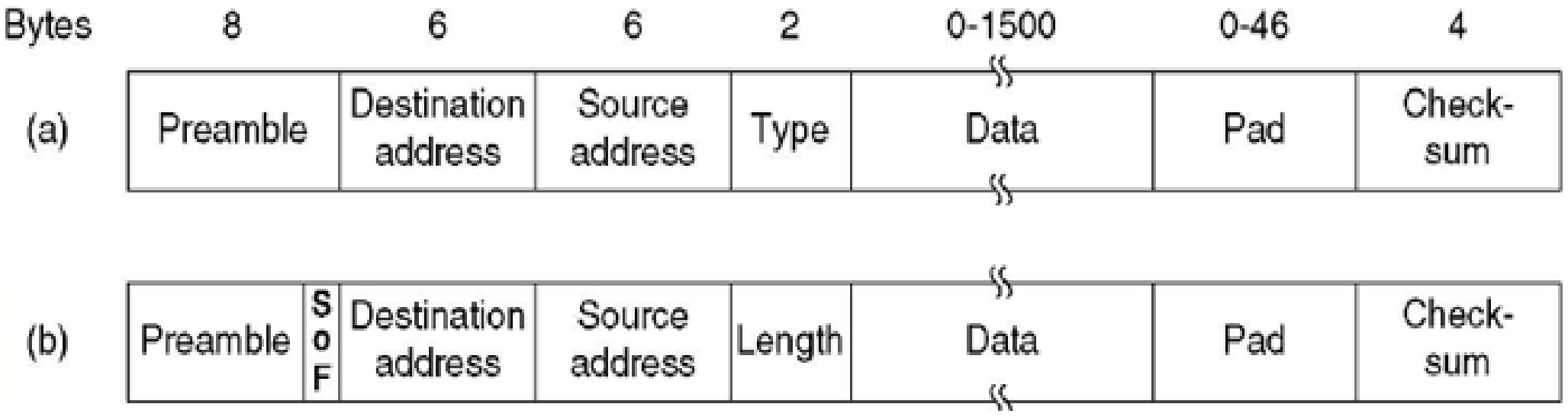
802.3: MAC Sublayer Protocol

Frame formats.

a) DIX Ethernet,

b) IEEE 802.3.

T/L <= 0x600 (1536): length; otherwise, type

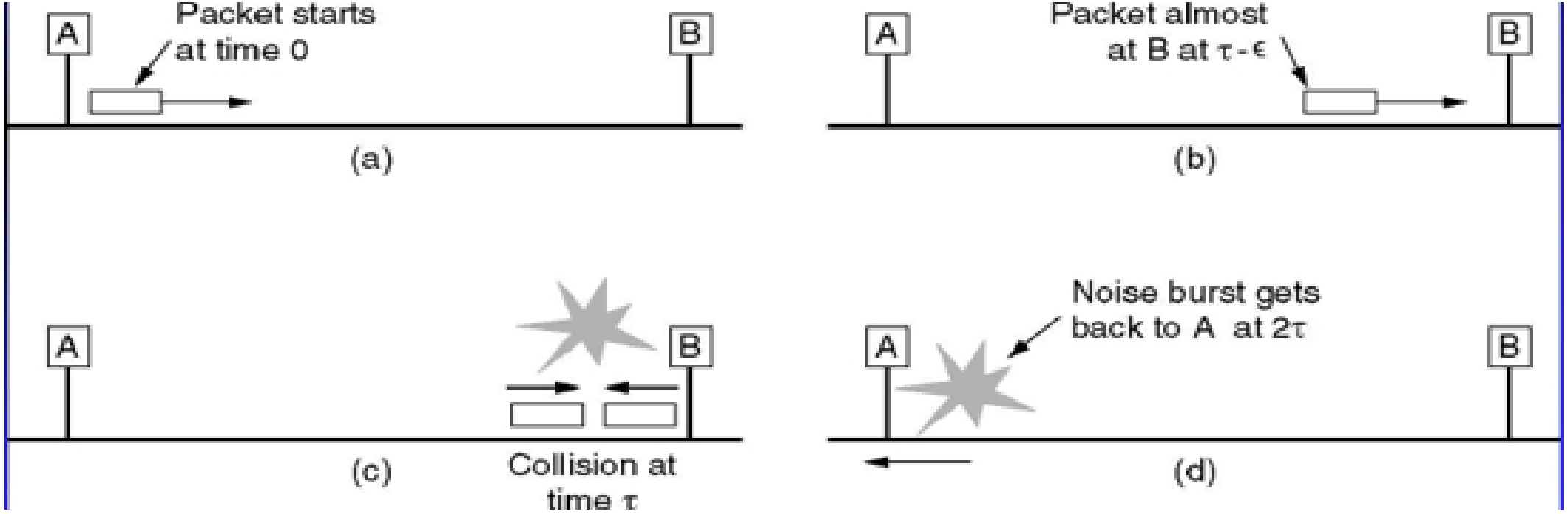


802.3: MAC Sublayer Protocol

- Preamble: 8 bytes, containing the bit pattern 10101010, used for synchronization
- Destination address and source address: 6 bytes each
  - Unicast address
  - Broadcast address
  - Multicast address
- Type field or length field
- Data: 1500 bytes (maximum), 46 bytes (minimum)
- Checksum: 32 bits, CRC

802.3: MAC Sublayer Protocol

How long does it take to find out whether there is a collision or not?



Collision detection can take as long as **2τ**.

802.3: MAC Sublayer Protocol

- All frames must take more than 2τ to send.
  - Too quick (to miss the collision)
  - Longer than 2τ to be sure of success.
- For a 10-Mbps LAN with a maximum length of 2500 meters and four repeaters, the maximum RTT is about 50us.

  Min frame length = 50us * 10 Mbps
  $=50*10^{-6}$ s $* 10*10^{6}$ bits/s = 500 bits $\approx$ 64 B

  Min payload length = 64–18 (src:6,dest:6,type:2,crc:4)
  = 46 B (→ Why min payload = 46)

802.3: MAC Sublayer Protocol:

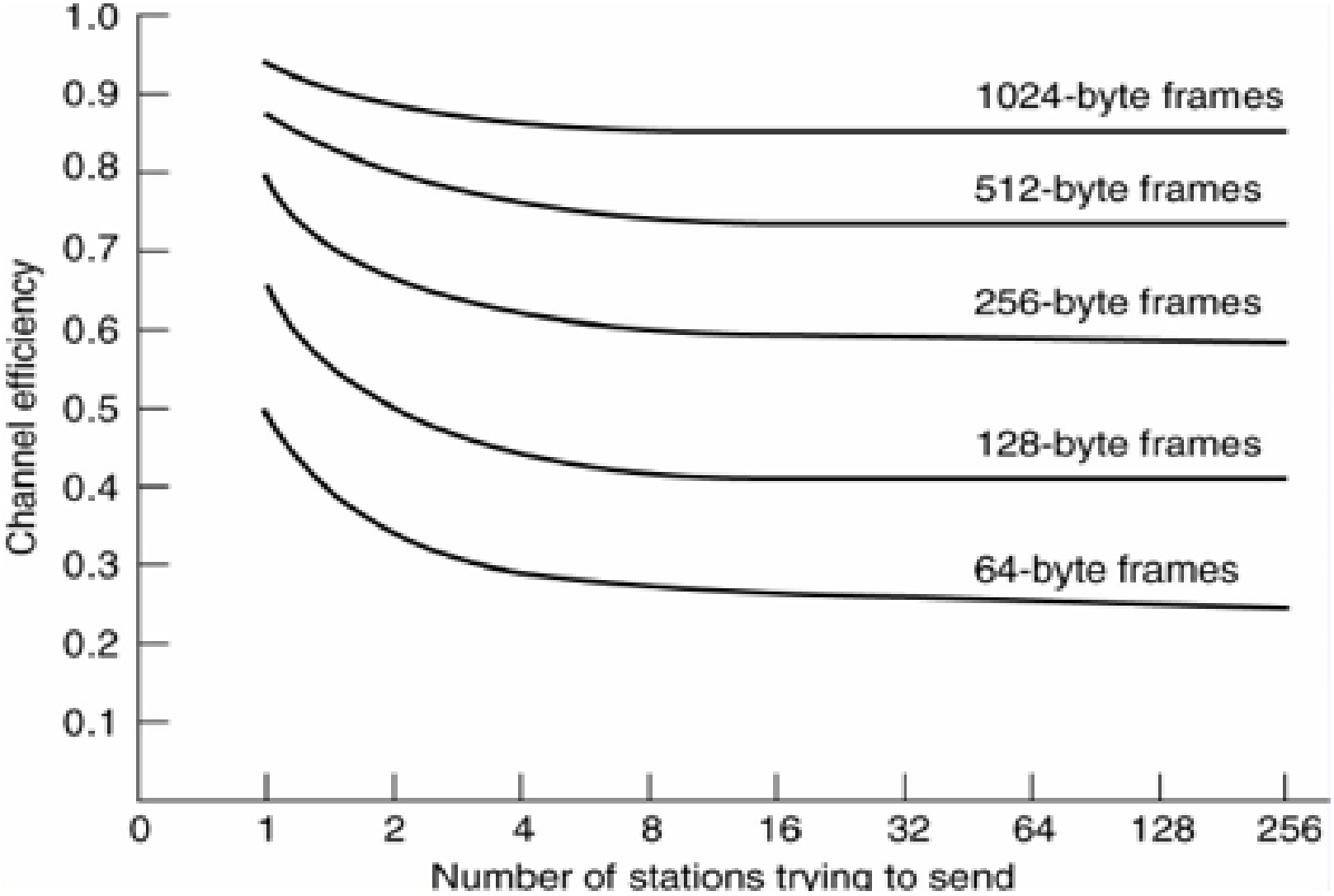
The **Binary Exponential Backoff Algorithm**

- Time is divided into discrete slots (51.2us).
- After the *1st* collision, each station waits either 0 or 1 (k in 0~2^1-1) slot times before trying again.
- After the *2nd* collision, each station picks either 0,1,2,3 (k in 0~2^2-1) at random and waits that number of slot times.
- After i-th collisions, each station picks either 0,1,2,…, $2^i - 1$ at random and waits that number of slot times.
- After 10th collisions, the randomization interval is frozen at a maximum of 1023 slots.
- After 16 consecutive collisions, the controller reports failure back to the computer.

→limited contention.

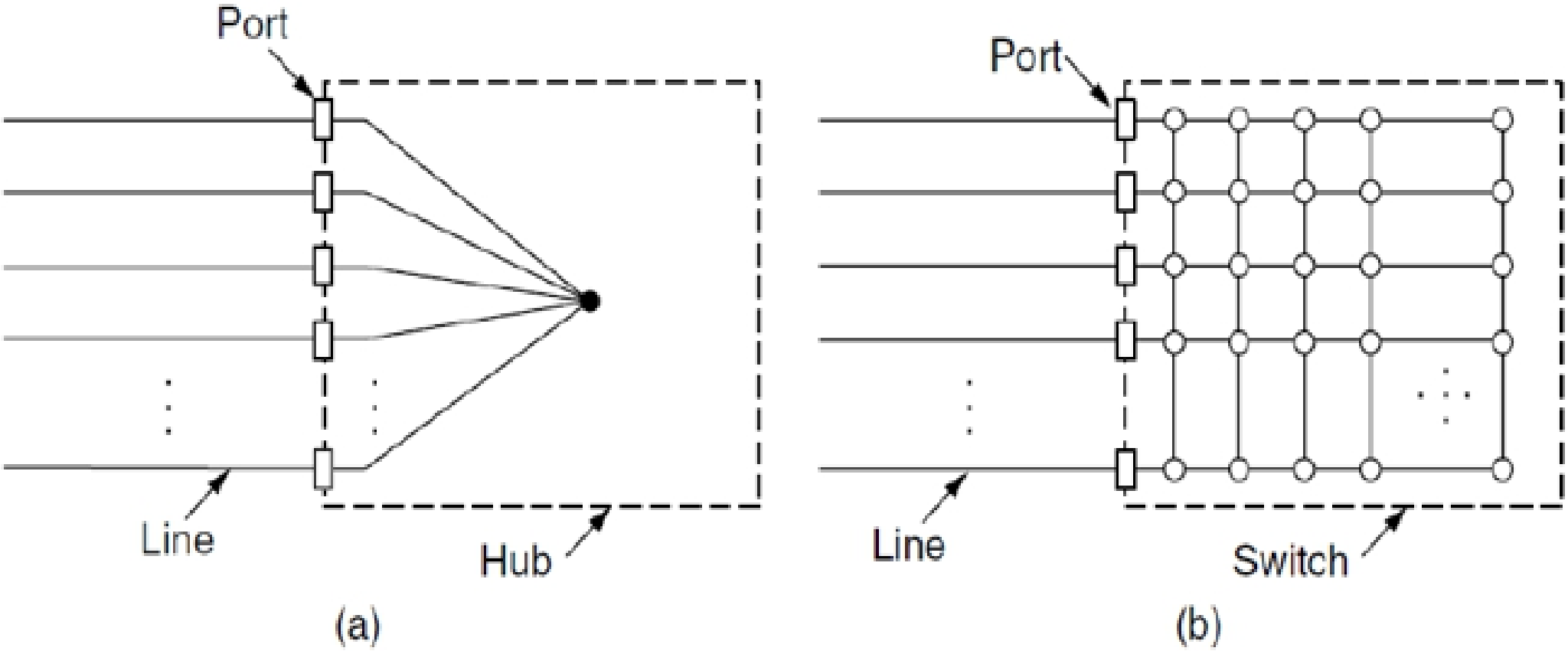
802.3: Performance

Efficiency of Ethernet at 10 Mbps with 512-bit slot times.



802.3: Switched Ethernet

Hub → Switch



802.3: Switched Ethernet

- Switch: The heart of this system is a **switch** containing a **high-speed backplane** that connects all of the ports
- Switch outputs frames to the ports for which those frames are destined. None of the other ports even knows the frame exists.
- What happens if more than one of the ports wants to send a frame at the same time?
  - Can send a frame on the cable at the same time
  - Why? Each port → one **collision domain** whereas all stations attached to a hub → one collision domain

802.3: Fast Ethernet (100-Mbps)

- Two high speed Ethernet: FDDI and Fiber Channel
  - Haven't done KISS (Keep It Simple, Stupid)
- IEEE 802
  - → IEEE 802.3u or Fast Ethernet (1992~1995)
  - → IEEE 802.3z or gigabit Ethernet (1995~1998)

The original fast Ethernet cabling.

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
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

802.3: Gigabit Ethernet (1-Gbps)

Gigabit Ethernet cabling.

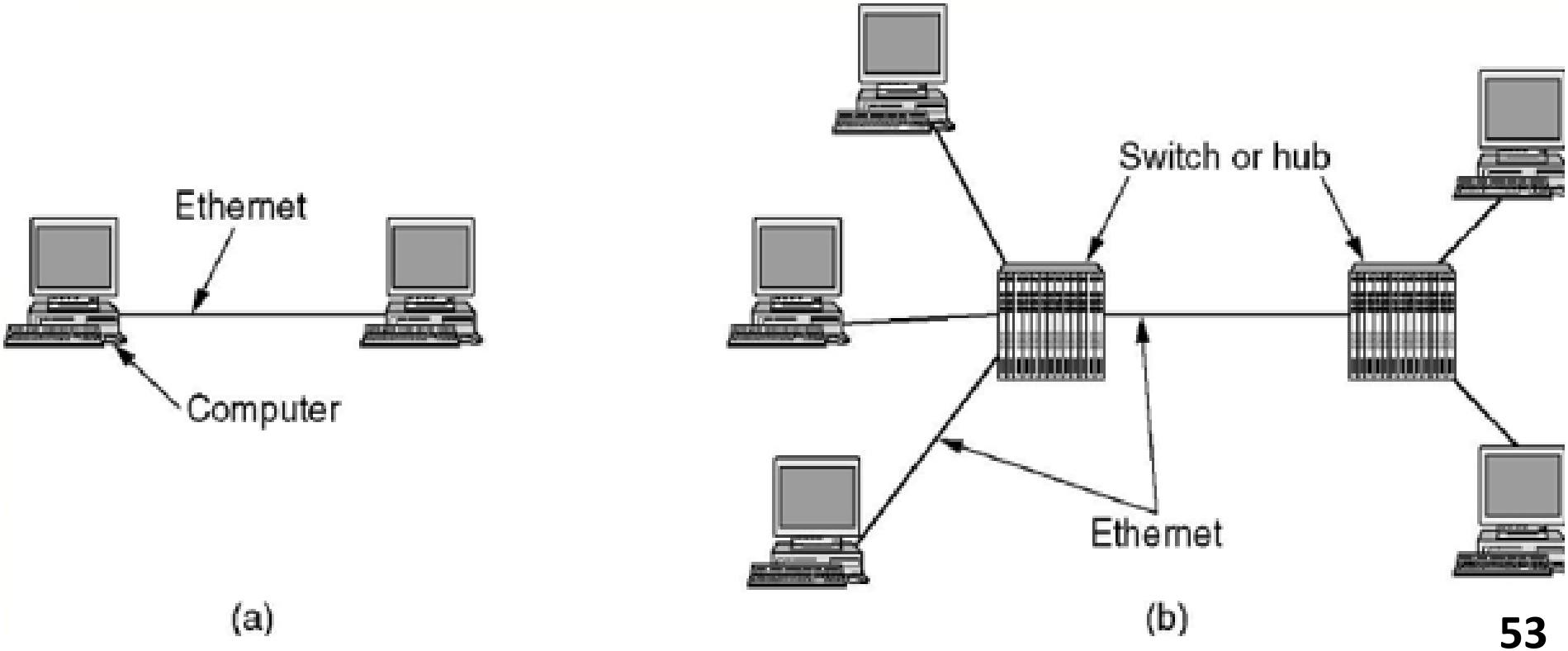
Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

802.3: Gigabit Ethernet (1-Gbps)

Possible connections:

a. A two-station Ethernet.

b. A multistation Ethernet.



802.3: 10-Gigabit Ethernet

10-Gigabit Ethernet cabling.

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

802.3: Comments

- Ethernet has been around for over 20 years
- Simple and flexible
  - Cheap
  - Easy to maintain
  - Ethernet works easily with TCP/IP
- There are 3 LAN standards:
  - 802.3 (Ethernet),
  - 802.4 (Token bus),
  - 802.5 (Token ring).
- They use roughly similar technology and get roughly similar performance.

802.3: Comments

802.3 (Ethernet):

- most widely used, simple, easy installation, low delay at low load.
- nondeterministic, no priorities, 64 byte minimum frame, collision problem

802.4 (Token bus(令牌总线))

- more deterministic, short minimum frames, priorities, real-time, multiple channels.
- a lot of analog engineering and including modems and wideband amplifiers, extremely complex protocol, substantial delay at low load, poorly suited for fiber optic implementations and a small installed base of users.

802.5 (Token Ring(令牌环))

- Easy engineering, fully digital, priorities, excellent throughput and efficiency at high load.
- centralized monitor, delay at low load.

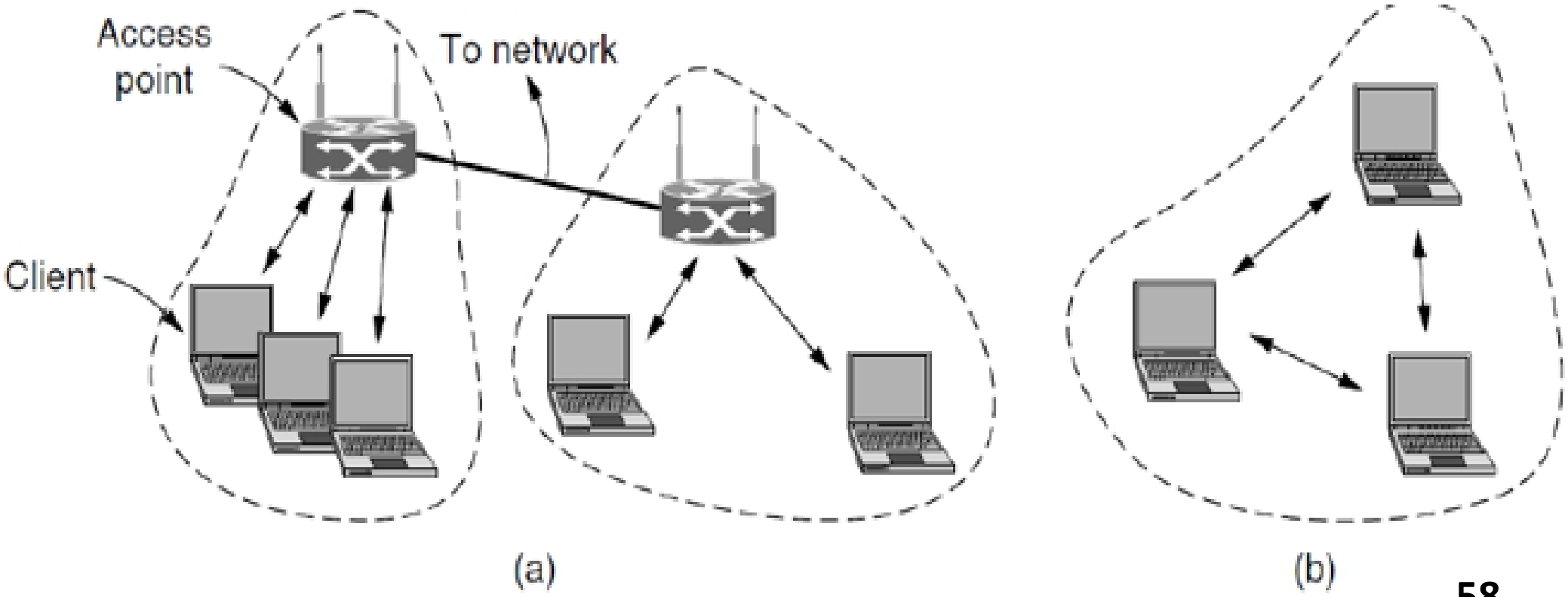
→ **the winner is 802.3.**

IEEE 802.11 (WIRELESS LANS)

- The 802.11 Architecture and Protocol Stack
- The 802.11 Physical Layer
- The 802.11 MAC Sublayer Protocol
- The 802.11 Frame Structure
- Services

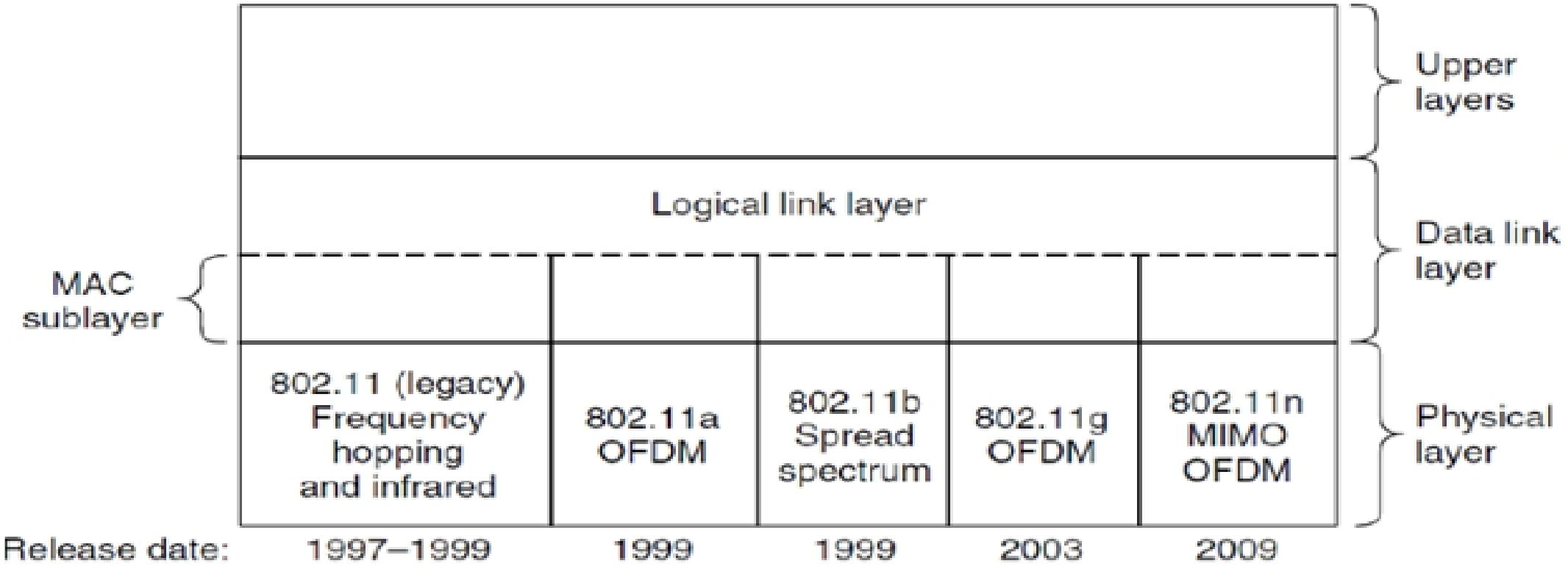
The 802.11: Architecture and Protocol Stack

802.11 architecture.
(a) Infrastructure mode.
(b) Ad-hoc mode.



The 802.11:
Architecture and Protocol Stack

Part of the 802.11 protocol stack.



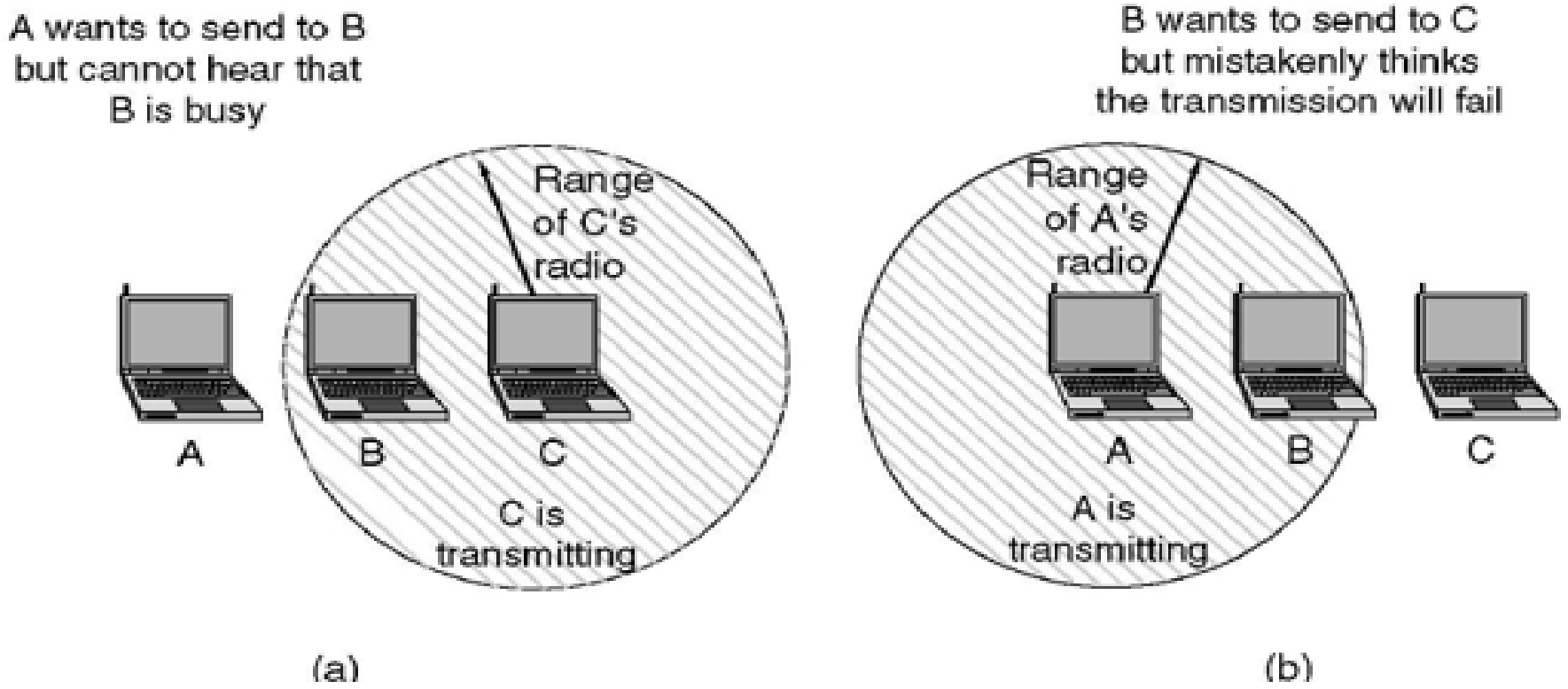
The 802.11: Physical Protocol

- **802.11**: **FHSS** (Frequency Hopping Spread Spectrum) and Infrared (**2.4Mbps**)
- **802.11a**: **OFDM** (Orthogonal Frequency Division Multiplexing) at 5GHz (**54Mbps**)
- **802.11b**: **HR-DSSS** (High Rate Direct Sequence Spread Spectrum) (**11Mbps**)
- **802.11g**: **OFDM** (Orthogonal Frequency Division Multiplexing) at 2.4 GHz (**54Mbps**)
- **802.11n**: **MIMO OFDM** (Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing) at multiple frequencies. (**600Mbps**)

The 802.11: Sublayer Protocol

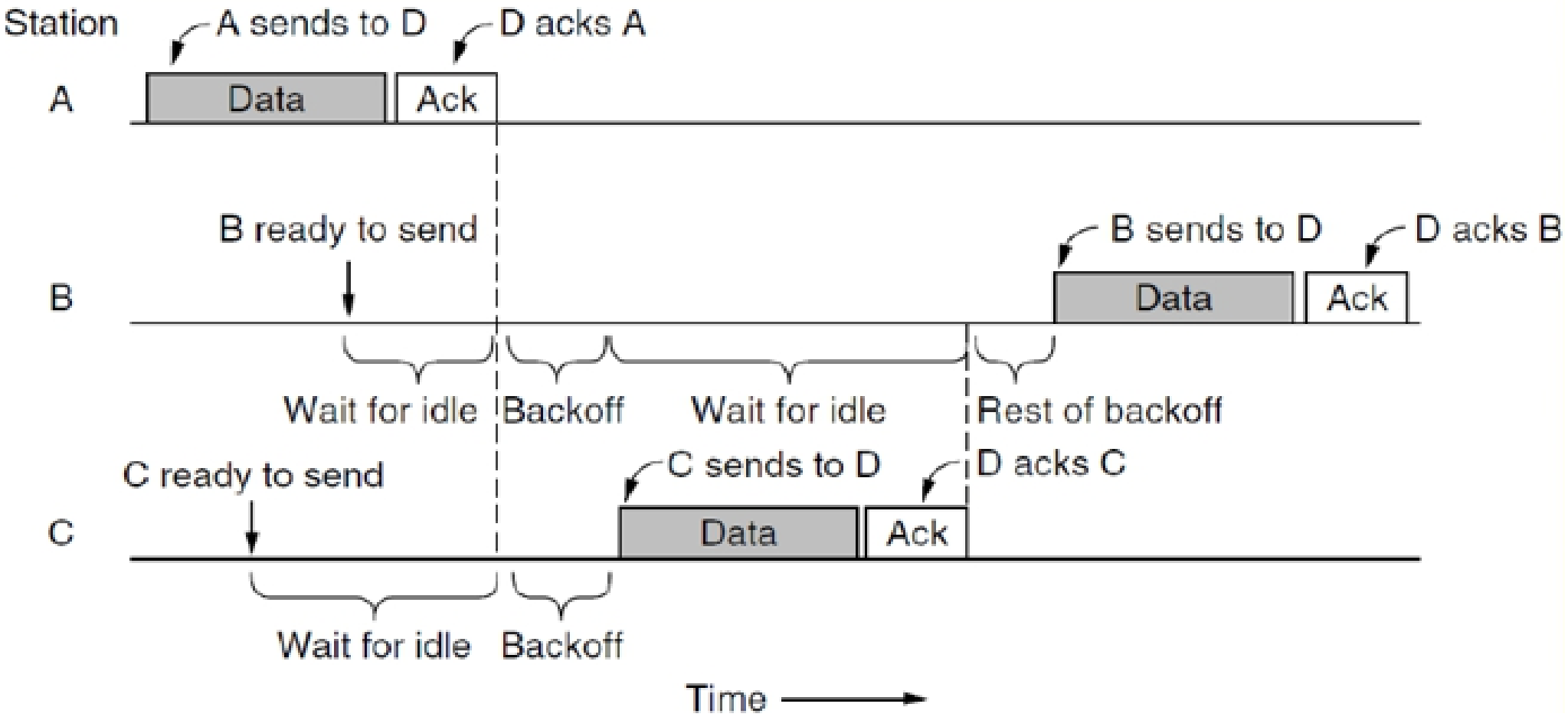
(a) The hidden station problem.

(b) The exposed station problem.



The 802.11: Sublayer Protocol

Sending a frame with CSMA/CA



The 802.11: Sublayer Protocol

- DCF (Distributed Coordination Function, 分布协调功能): CSMA/CA (CSMA with Collision Avoidance)

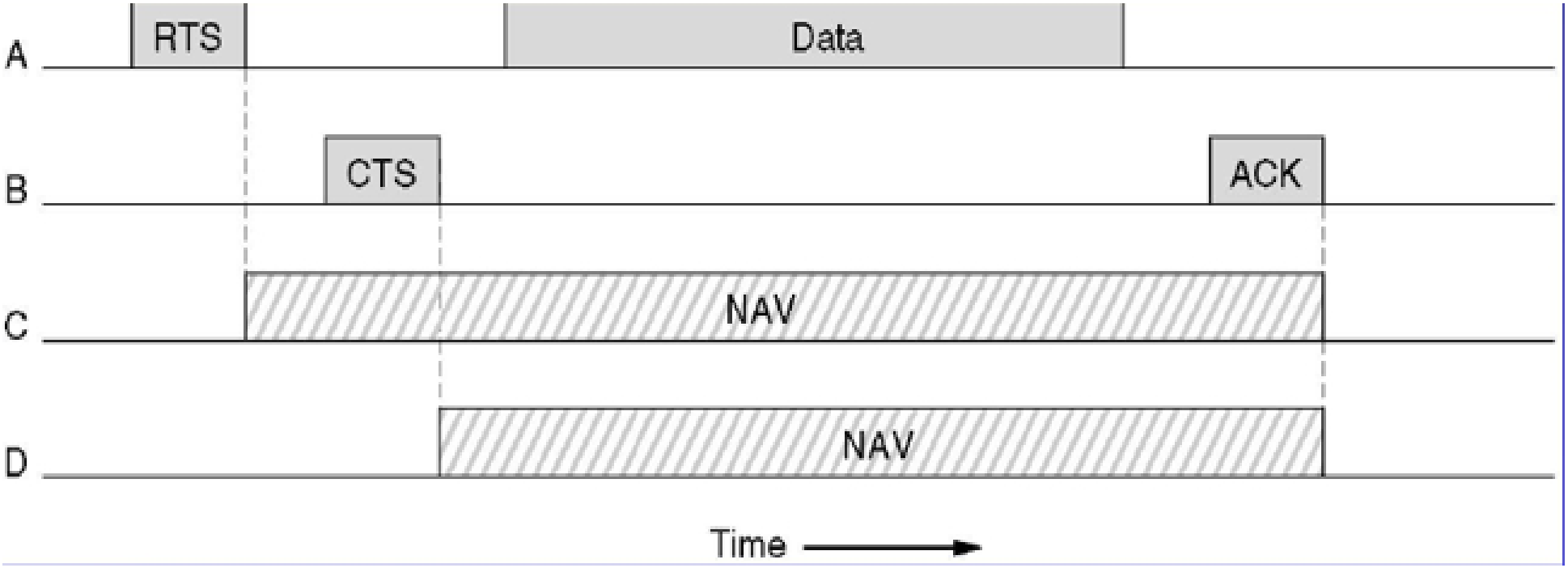
- PCF (Point Coordination Function, 集中协调功能): the access point controls all activity in its cell, just like a cellular base station (not used in practice)

The 802.11: Sublayer Protocol: PCF

- PCF (Point Coordination Function)
  - The base station broadcasts a beacon frame periodically. The beacon frame contains system parameters, such as hopping sequences and dwell times (for FHSS), clock synchronization, etc.
  - The base station also invites new stations to sign up for polling service. Once a station has signed up for polling service at a certain rate, it is effectively guaranteed a certain fraction of the bandwidth, thus making it possible to give quality-of-service guarantees.
  - 802.11 pays attention to the issue of power management.

The 802.11: Sublayer Protocol: DCF

The use of virtual channel sensing using CSMA/CA.

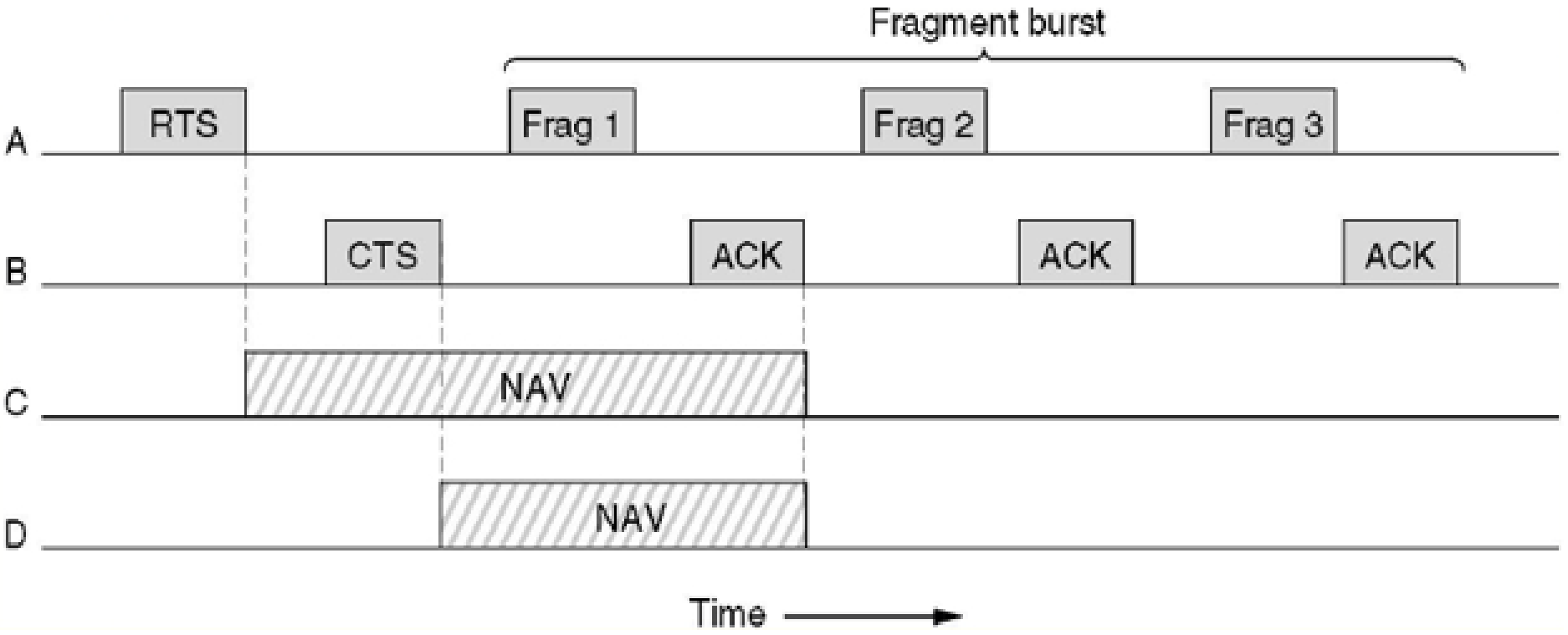


802.11 takes a conservative approach:

Stations hearing RTS cannot send data during NAV, i.e. exposed terminals of A cannot concurrently send data with A (as opposed to MACA)

The 802.11: Sublayer Protocol: DCF

A fragment burst.



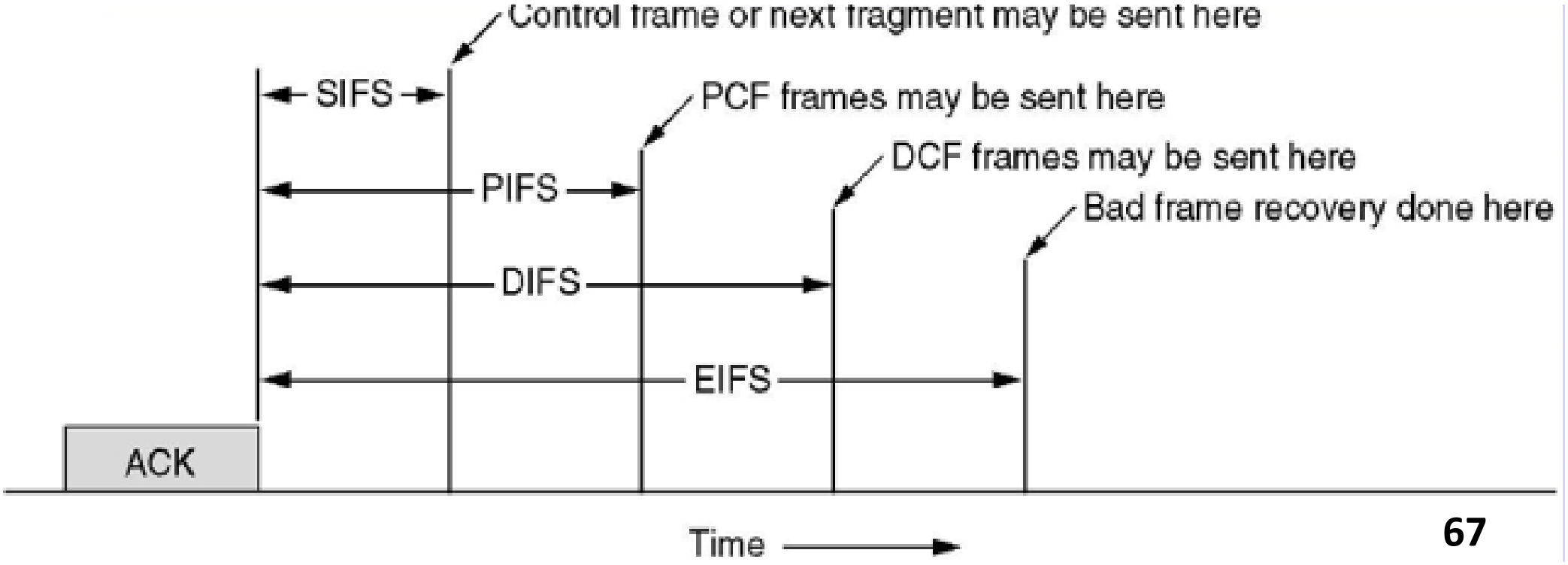
Why fragment?

How to ensure continuous transmission?

The 802.11: Sublayer Protocol

SIFS: Short InterFrame Spacing
PIFS: PCF InterFrame Spacing
DIFS: DCF InterFrame Spacing
EIFS: Extended InterFrame Spacing

Interframe spacing in 802.11.



The 802.11: Frame Structure

- The 802.11 standard defines three different classes of frames:
  - Data
  - Control
  - Management
- The 802.11 data frame

The 802.11: Services

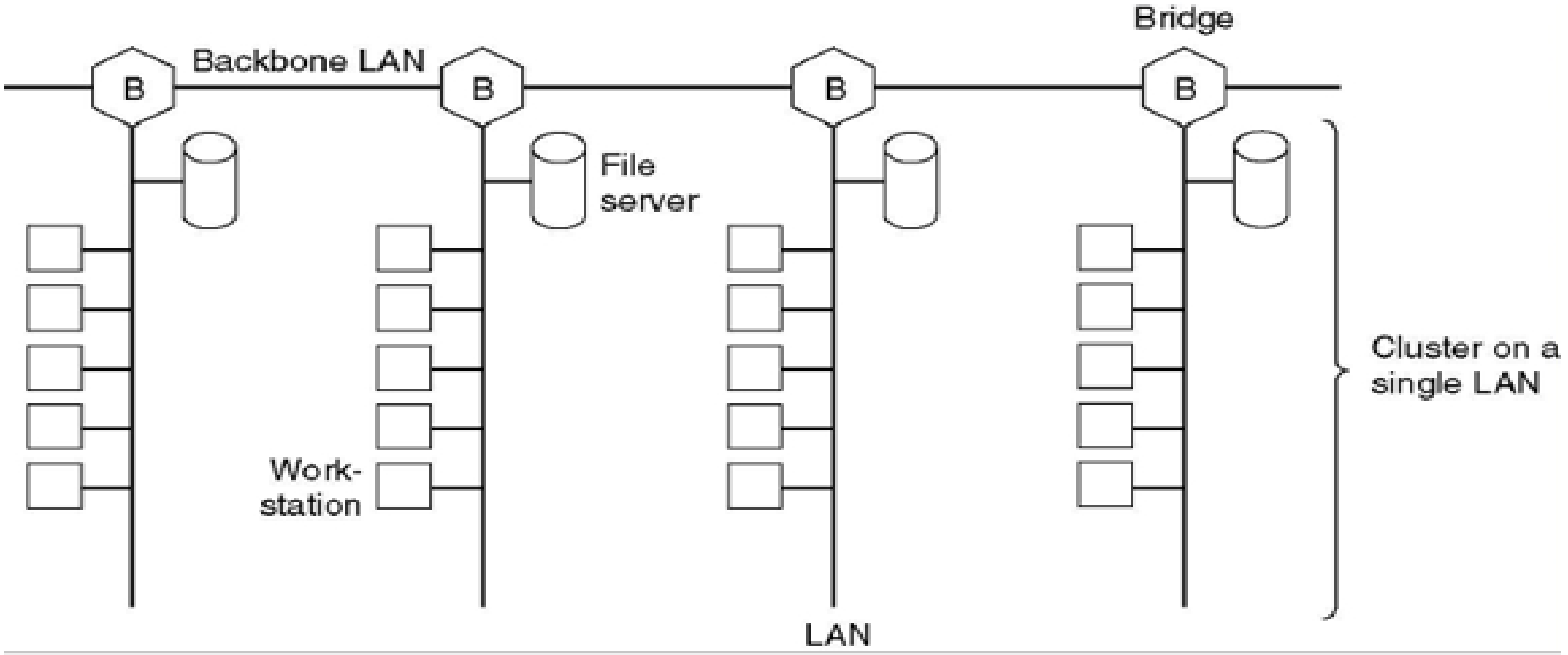
- Intracell Services
  - Authentication
  - Deauthentication
  - Privacy
  - Data Delivery
- Intercell Services
  - Association
  - Disassociation
  - Reassociation
  - Distribution
  - Integration

Data Link Layer Switching

- Uses of Bridges
- Learning Bridges
- Spanning Tree Bridges
- Virtual LANs
- Hubs, Repeaters, Bridges, Switches, Routers, Gateways

Data Link Layer Switching:
Uses of Bridges

Multiple LANs connected by a backbone to handle a total load higher than the capacity of a single LAN.



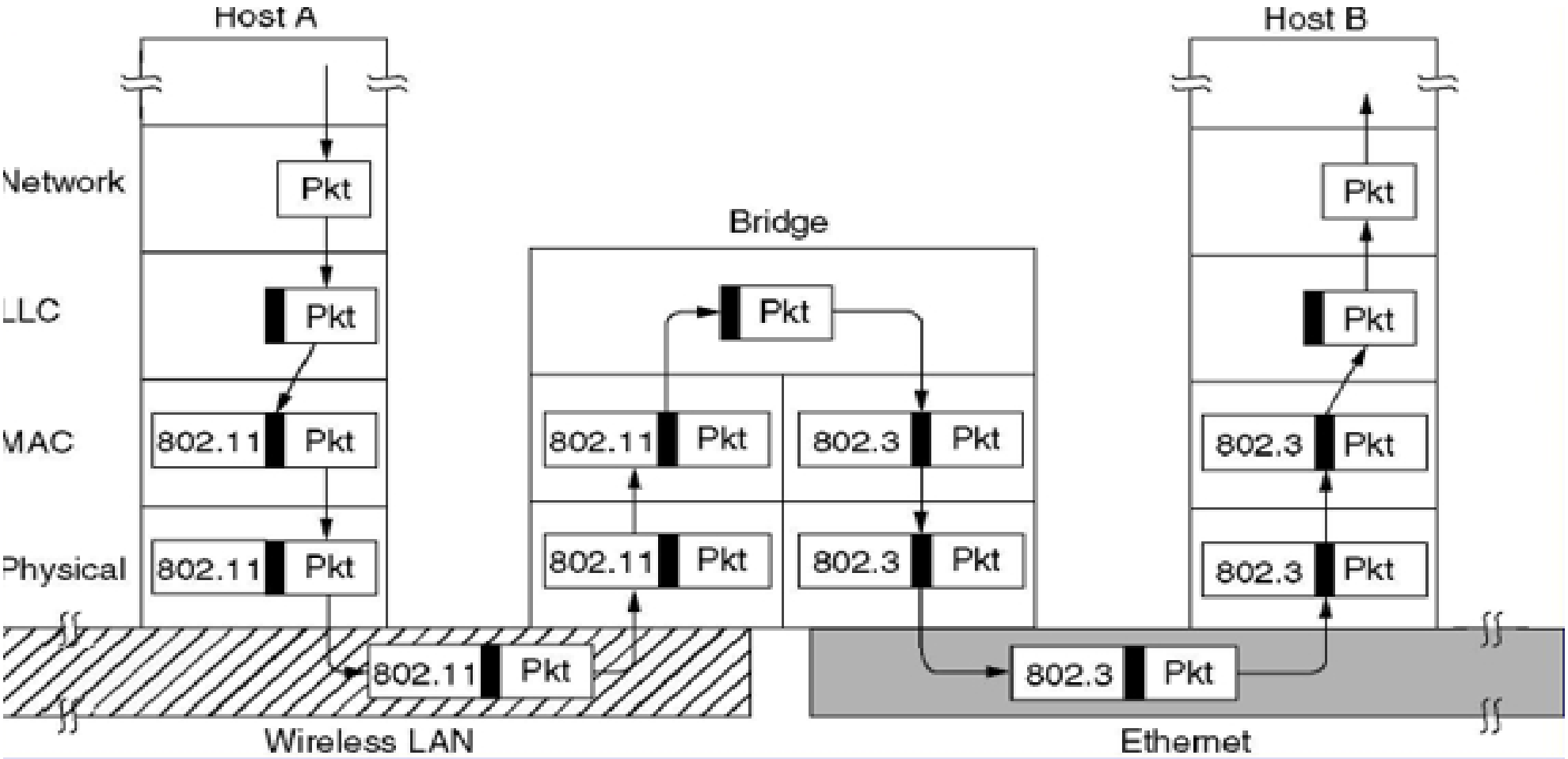
Data Link Layer Switching:
Uses of Bridges

- Why bridges are used?
  - Different organizations have different LANs, but need communicate.
  - Different locations have different LANs. Using bridges are cost effective than using a centralized switch.
  - Multiple LANs are used to accommodate the load.
  - ...

Data Link Layer Switching:

Uses of Bridges

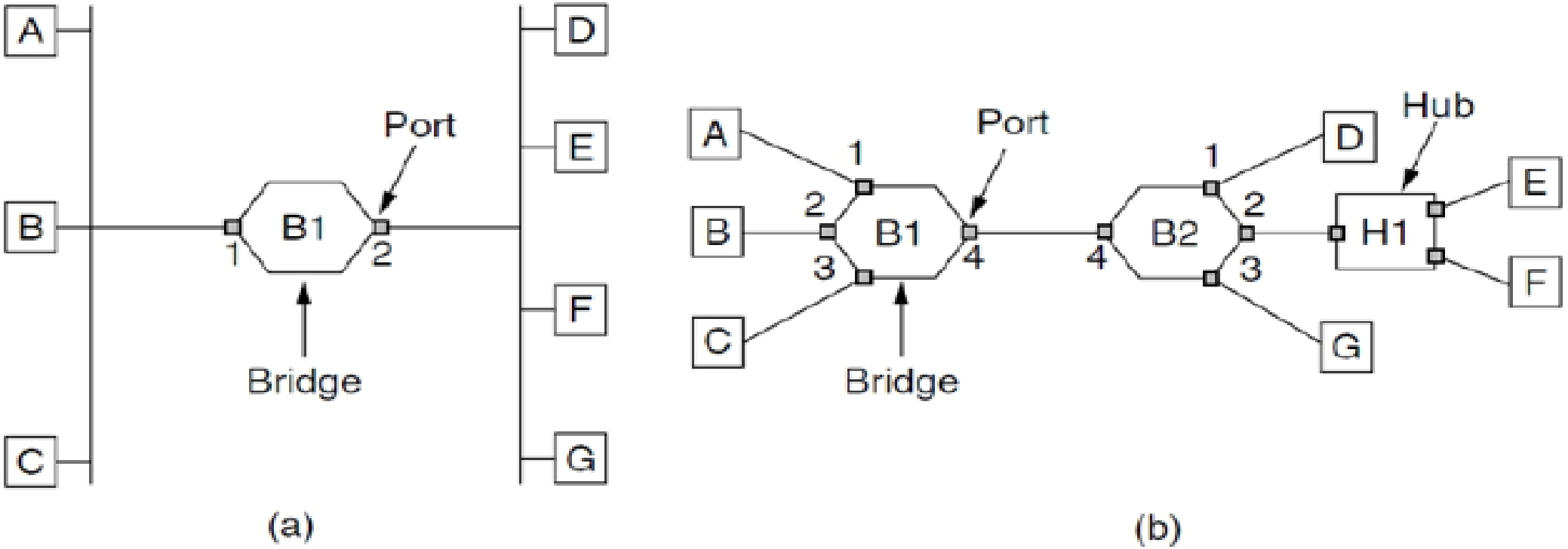
Operation of a LAN bridge from 802.11 to 802.3.



Data Link Layer Switching:
Learning Bridges

a) Bridge connecting two LANs.

b) Bridges (and a hub) connecting seven point-to-point stations.



Data Link Layer Switching:
Learning Bridges

- The first 802 bridge is a learning bridge or transparent bidge (透明网桥).
- The bridge has a big (hash) table inside it. The table can list each possible destination and tell which output line (LAN) it belongs on.
- When a frame arrives, a bridge must decide whether to discard or forward it and if the latter, on which LAN to put the frame.

Data Link Layer Switching:
Learning Bridges

- The hash table for the bridge
  - When the first bridges are first plugged in, all the hash tables are empty. None of the bridges know where any of the destinations are, so they use the flooding algorithm.
  - As time goes on, the bridges learn where destinations are. (**backward learning**)
  - Whenever a frame whose source is already in the table arrives, its entry is updated with the current time. (time updating)
  - Periodically, a process in the bridge scans the hash table and purges all entries more than a few minutes old. (Aging)

Data Link Layer Switching:
Learning Bridges

- The routing procedure for an incoming frame depends on the LAN it arrives and the LAN its destination is on.
  - If destination and source LANs are the same,
    →Discard the frame.
  - If the destination and source LANs are different,
    →Forward the frame.
  - If the destination LAN is unknown,
    →Use flooding.

Data Link Layer Switching:

Spanning Tree Bridges

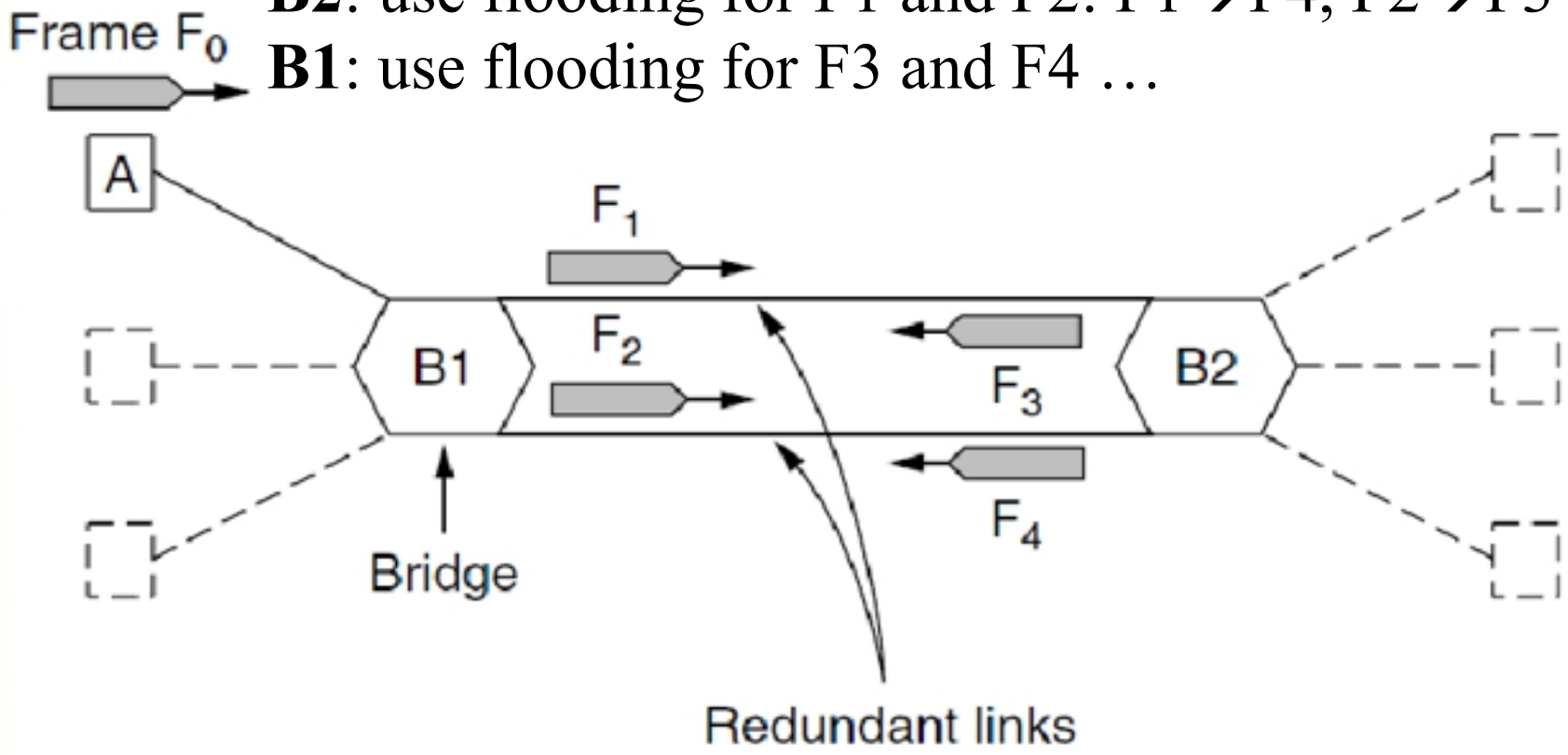
To increase reliability, redundant link may used. → **loop**

Ex: A → unknown station

B1: use flooding for F0, →F1 and F2 and others

B2: use flooding for F1 and F2: F1→F4, F2→F3

B1: use flooding for F3 and F4 …



Bridges with two parallel links

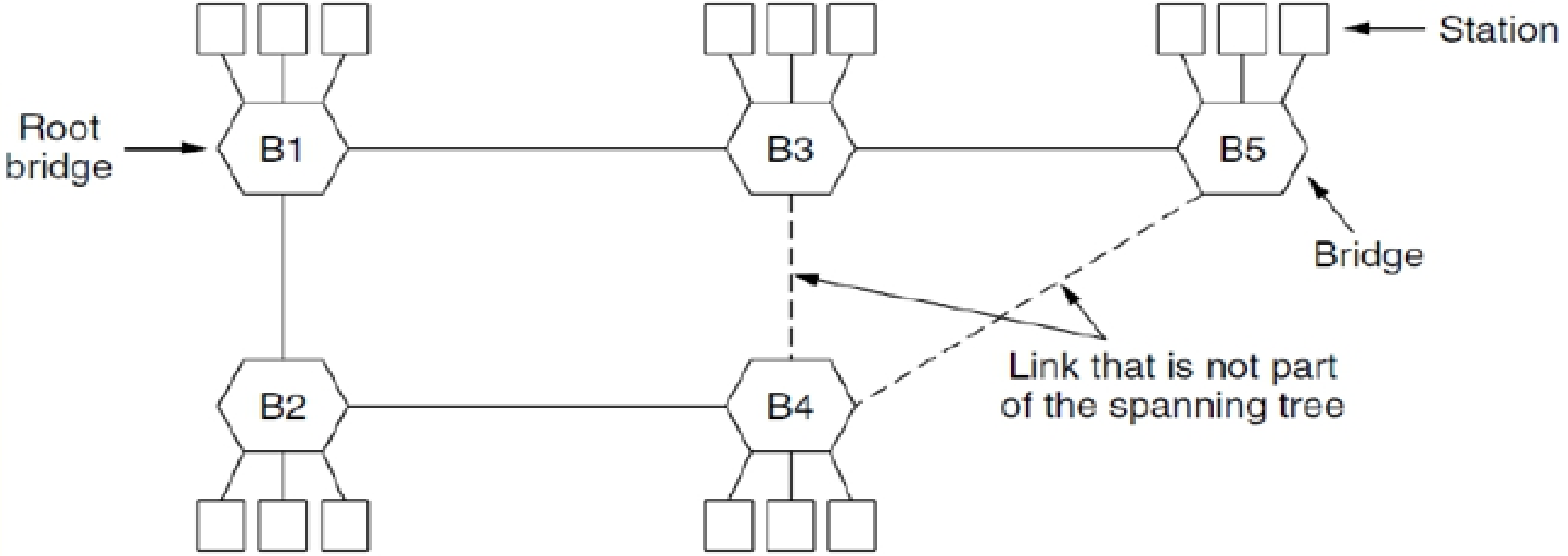
Data Link Layer Switching:
Spanning Tree Bridges

- The problem occurs if the topology contains loops!
- The solution to this difficulty is for the bridges to communicate with each other and overlay the actual topology with a spanning tree that reaches every LAN.

Data Link Layer Switching:

Spanning Tree Bridges

A spanning tree connecting five bridges.
The dashed lines are links that are not part of the spanning tree.



Data Link Layer Switching:

Spanning Tree Bridges

- How to build the spanning tree
  - The bridges have to choose one bridge to be the root of the tree. They make this choice by having each one broadcast its serial number, installed by the manufacturer and guaranteed to be unique worldwide. The bridge with the lowest serial number becomes the root.
  - A tree of shortest paths from the root to every bridge and LAN is constructed. This tree is the spanning tree.
  - If a bridge or LAN fails, a new one is computed.

Data Link Layer Switching:
Spanning Tree Bridges: Radia 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.

Data Link Layer Switching:
Virtual LANs

- Why want multiple LANs with restricted scope?
  - Security. (Promiscuous mode, 混杂模式)
  - Load.
  - Broadcasting.

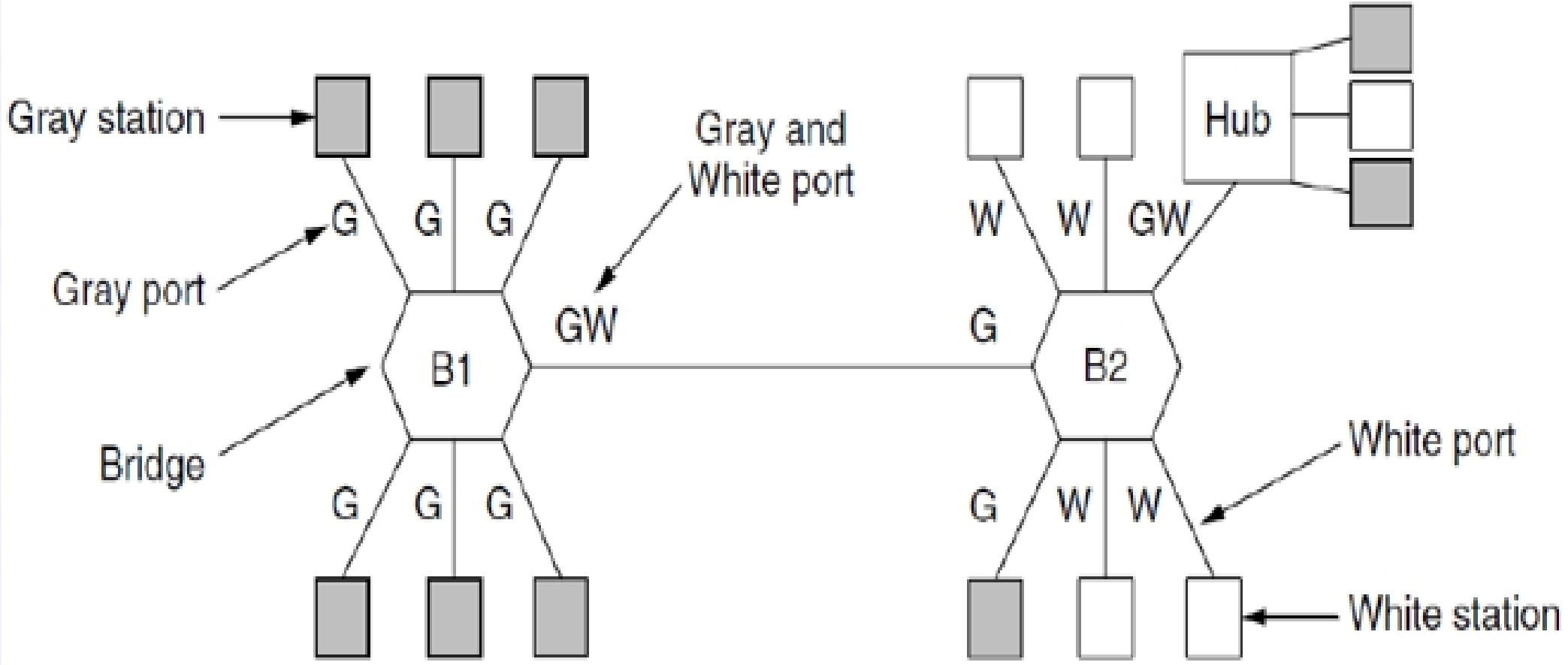
- How to dynamically move the user from one LAN to another LAN?
  - Pulling out plugs and pushing them back in somewhere else
  - VLAN (Virtual LAN), IEEE 802.1Q standard

Data Link Layer Switching:
Virtual LANs

- To setup a VLAN-based network
- The network administrator decides how many VLANs there will be, which computers will be on which VLAN, and what the VLANs will be called.
- The VLANs are marked/named by colors since it is then possible to print color diagrams showing the physical layout of the machines.
- To make the VLANs function correctly, configuration tables have to set up in the bridges or switches. These tables tell which VLANs are accessible via which ports (lines).
- A port may be labeled with multiple VLAN colors.

Data Link Layer Switching:
Virtual LANs

Two VLANs, gray and white, on a bridged LAN.



Data Link Layer Switching:
Virtual LANs

- How do bridges and switches know what color an incoming frame is:
  - Every port is assigned a VLAN color.
  - Every MAC address is assigned a VLAN color.
  - Every layer 3 protocol or IP address is assigned a VLAN color.

- IEEE 802.1Q: add a VLAN tag in Ethernet header

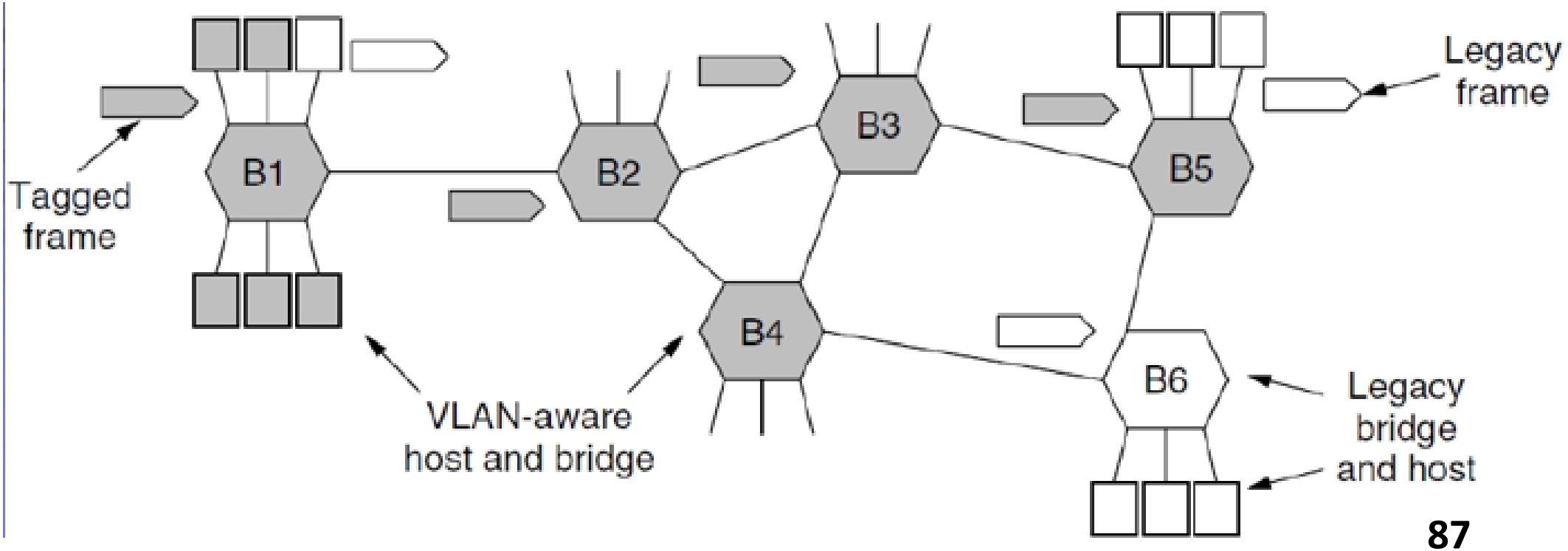
Data Link Layer Switching:

Virtual LANs:

The IEEE 802.1Q Standard

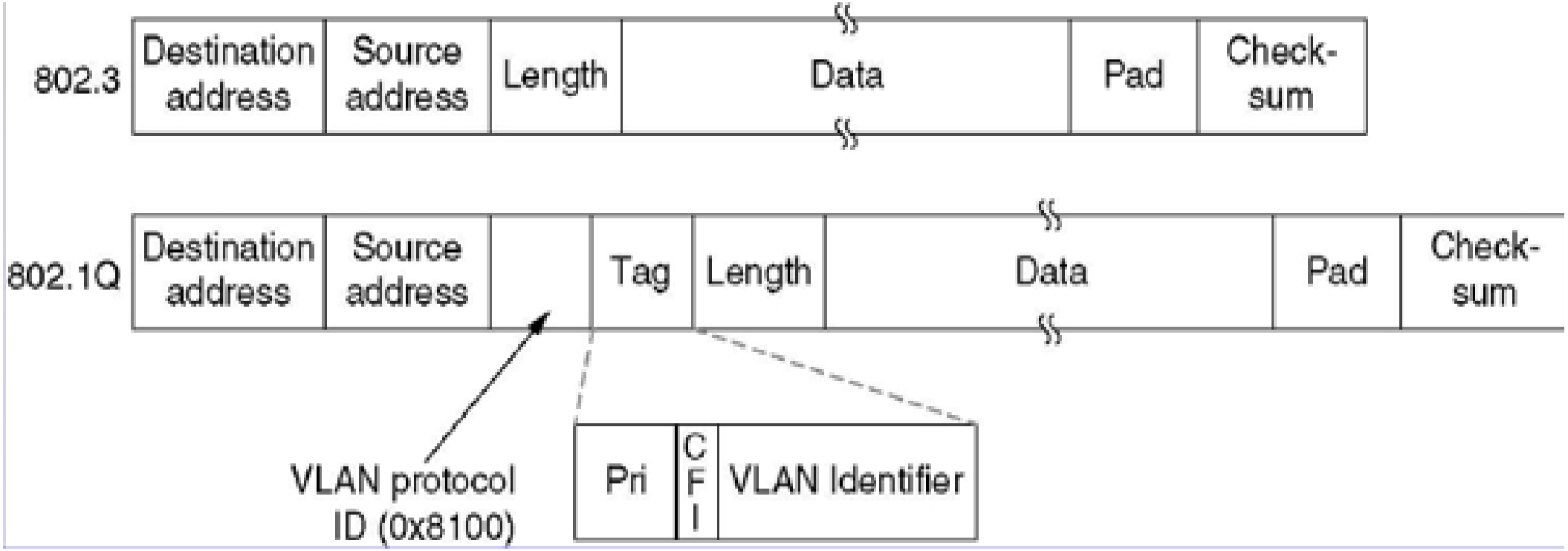
Bridged LAN that is only partly VLAN aware.

- The shaded symbols are VLAN aware.
- The empty ones are not.



Data Link Layer Switching: The IEEE 802.1Q Standard

The 802.3 (legacy) and 802.1Q Ethernet frame formats.

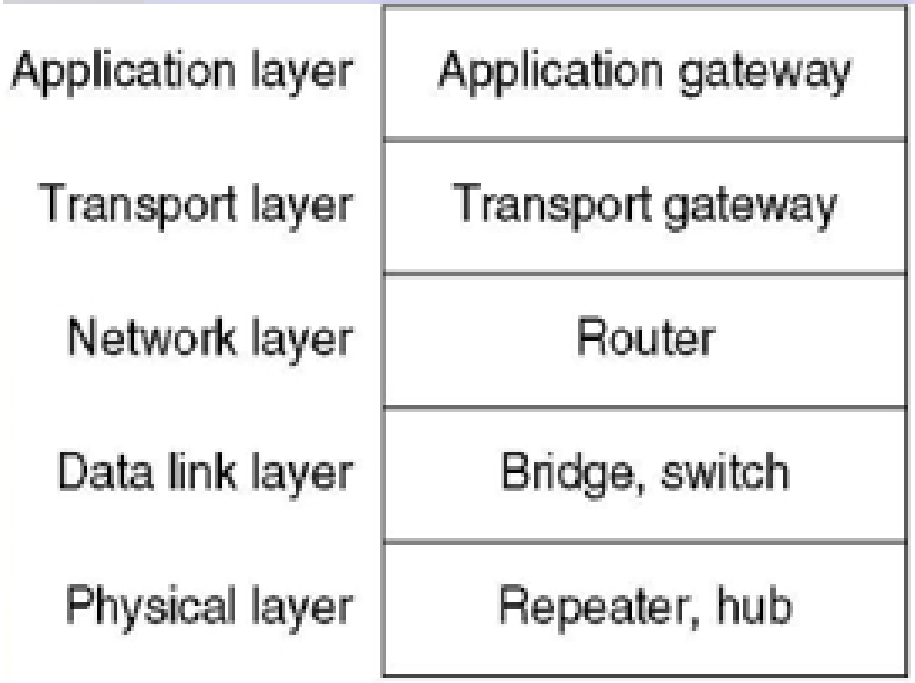


Data Link Layer Switching:

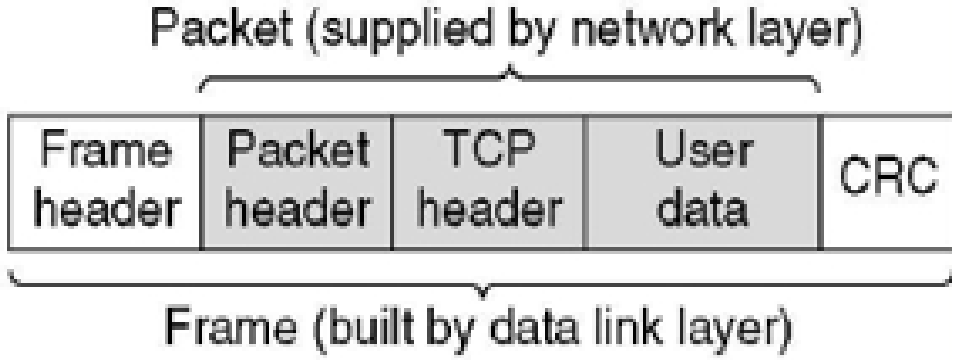
Hubs, Repeaters, Bridges, Switches, Routers and Gateways

(a) Which device is in which layer.

(b) Frames, packets, and headers.



(a)



(b)

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

- Repeaters (中继器)
  - Repeaters are analog devices that connected to two cable segments.
  - A signal appearing on one of them is amplified and put out on the other.
  - Repeaters don not understand packets, frames, or headers.
  - They understand volts.

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

- Hubs (网络集线器)
  - 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.
  - If two frames arrive at the same time, they will collide, just as on a coaxial cable.
  - Hubs do not examine the 802 addresses or use them in any way.
  - They do not amplify the incoming signals.

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

- Bridges (网桥)
  - A bridge connects two or more LANs.
  - When a frame arrives, software in the bridge extracts the destination address from the frame header and looks it up in a table to see where to send the frame.
  - A bridge may have line cards for different network types and different speeds.
  - With a bridge, each line is its own collision domain, in contrast to a hub.

Data Link Layer Switching:

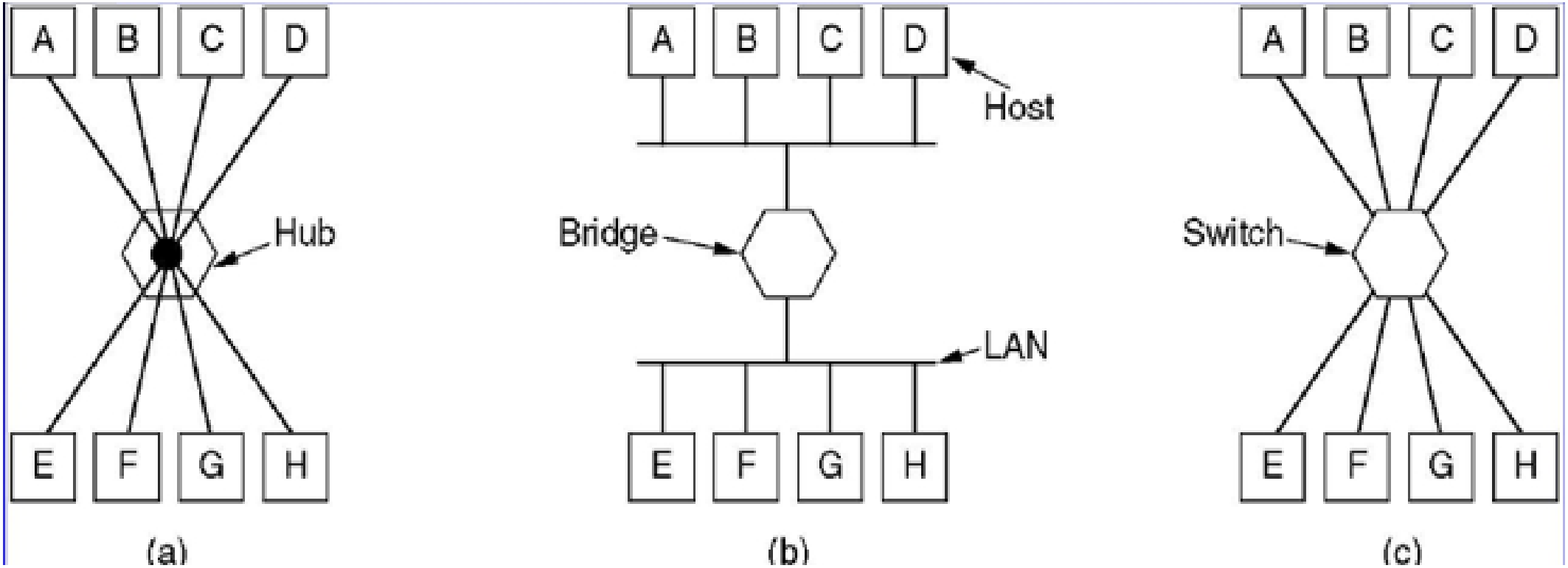
Hubs, Repeaters, Bridges, Switches, Routers and Gateways

- Switches (交换机)
  - Switches are similar to bridges in that both route on frame addresses.
  - Each port is its own collision domain, switches never lose frames to collisions.
  - If frames come in faster than they can be retransmitted, the switch may run out of buffer space and have to start discarding frames.
  - Modern switches (**cut-through switch**) start forwarding frames as soon as the destination header field has come in, but before the rest of the frame has arrived.

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

(a) A hub. (b) A bridge. (c) a switch.



More on bridges and switches

- **Bridges** were originally intended to be able to join different kinds of LANs. Never worked well.
- **Switches** are modern bridges by another name. a few points
  - Switches have more ports
  - Switches are more general, e.g. telephone switch

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

- Routers (路由器)
  - Routers use the packet header to choose an output line.
  - Routing algorithm: RIP, OSPF, …
  - QoS

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

- Gateways (网关)
  - Transport gateway
    - Transport gateways connects two computer that use different connection-oriented transport protocols.
    - For example, suppose a computer using the connection-oriented TCP/IP protocol needs to talk to a computer using the connection-oriented ATM transport protocol. The transport gateway can copy the packets from one connection to the other, reformatting them as need be.

Data Link Layer Switching:

Hubs, Repeaters, Bridges, Switches, Routers and Gateways

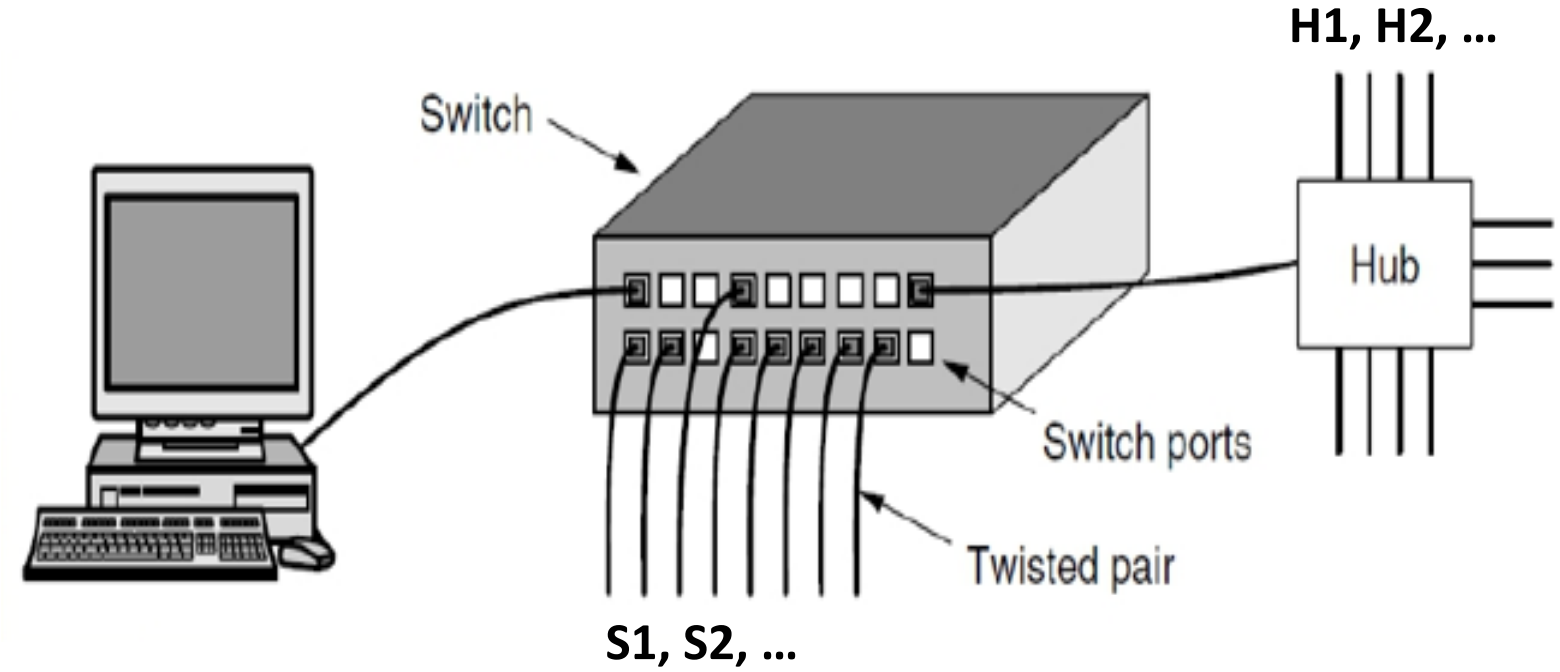
- Gateways (网关)
  - Application gateways
    - Application gateways understand the format and contents of the data and translate messages from one format to another.
    - An email gateway could translate Internet messages into SMS messages for mobile phones, for example

Some Clarifications: Collision domain v.s. broadcast domain

- A **collision domain** is a section of a network where data packets can collide with one another when being sent on a shared medium or through repeaters, particularly when using early versions of Ethernet. A network collision occurs when more than one device attempts to send a packet on a network segment at the same time.
- A **broadcast domain** is a logical division of a computer network, in which all nodes can reach each other by broadcast *at the data link layer*. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments.

An Ethernet Switch

All stations are in the same broadcast domain
H1, H2, … are in the same collision domain



Some Clarifications

- The host connected to a single hub belong to
  - Same collision domain and same broadcast domain
- Bridges can
  - Reduce the collision domain
  - Increase the broadcast domain
- Routers can
  - Increase the number of broadcast domains

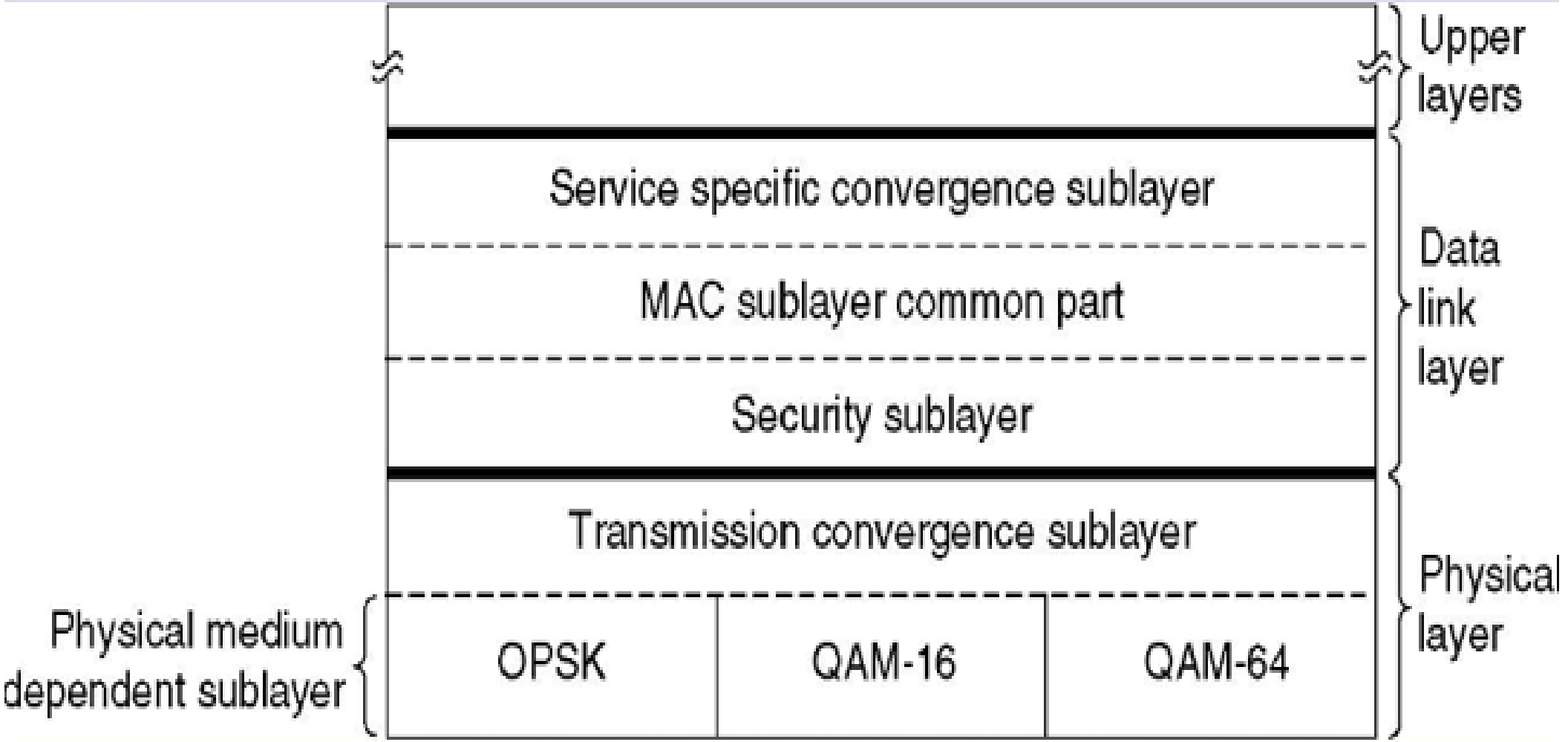
THE 802.16 BROADBAND WIRELESS

- Comparison of 802.11 and 802.16
- The 802.16 Protocol Stack
- The 802.16 Physical Layer
- The 802.16 MAC Sublayer Protocol
- The 802.16 Frame Structure

The 802.16: Comparison

- 802.16 (Wireless MAN) vs 802.11 (Wireless LAN)
  - 802.16 provides services to fixed buildings (fixed wireless), while 802.11 provides mobility service to mobile users (mobile wireless)
  - 802.16 can use full-duplex communication, while 802.11 avoids to keep the cost of the radios low.
  - 802.16 operates in the much higher 10-to-66 GHz frequency range while 802.11 uses the ISM band.
  - QoS
  - →In short, 802.11 was designed to be mobile Ethernet, whereas 802.16 was designed to be wireless, but stationary, cable television.

The 802.16: Protocol Stack

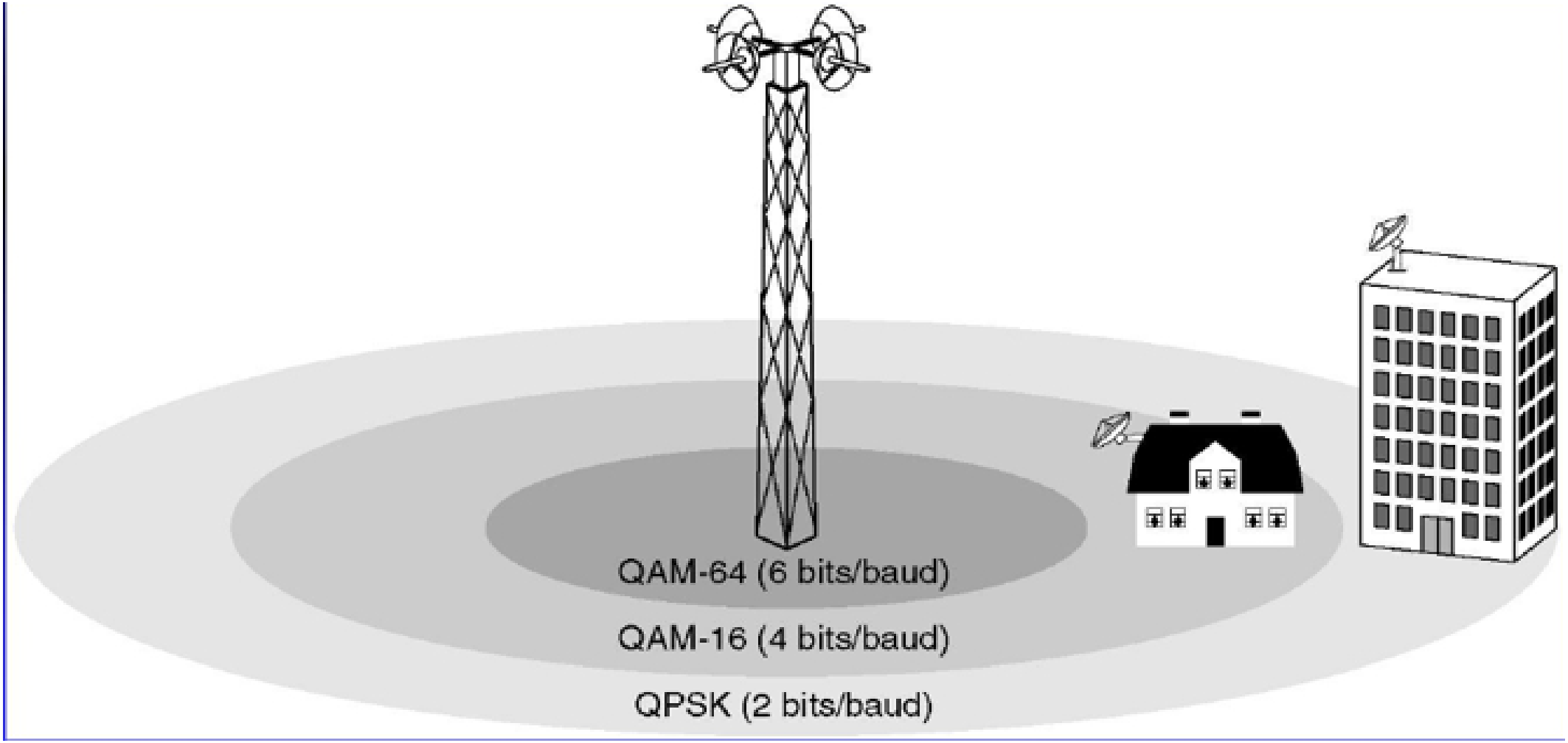


The 802.16: Physical Layer

- Broadband wireless needs a lot of spectrum.
  - (10 to 66 GHz)
- 3 Modulation frequencies (in fact more)
  - For close-in subscribers, QAM-64 (6 bits/baud)
  - For medium-distance subscribers, QAM-16 (with 4 bits/baud)
  - For distant subscribers, QPSK is used (2 bits/baund)
- Downstream > Upstream
- To use Hamming codes to do forward error correction in the physical layer.

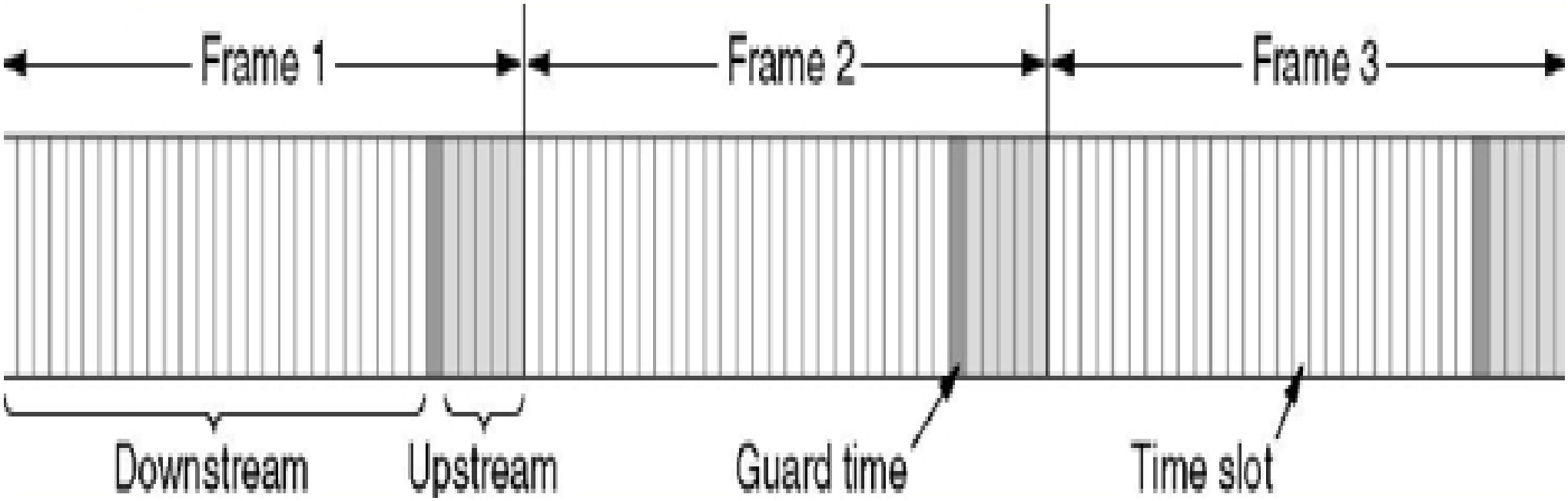
The 802.16: Physical Layer

The 802.16 transmission environment.



The 802.16: Physical Layer

Frames and time slots for time division duplexing.



The 802.16: MAC Sublayer Protocol

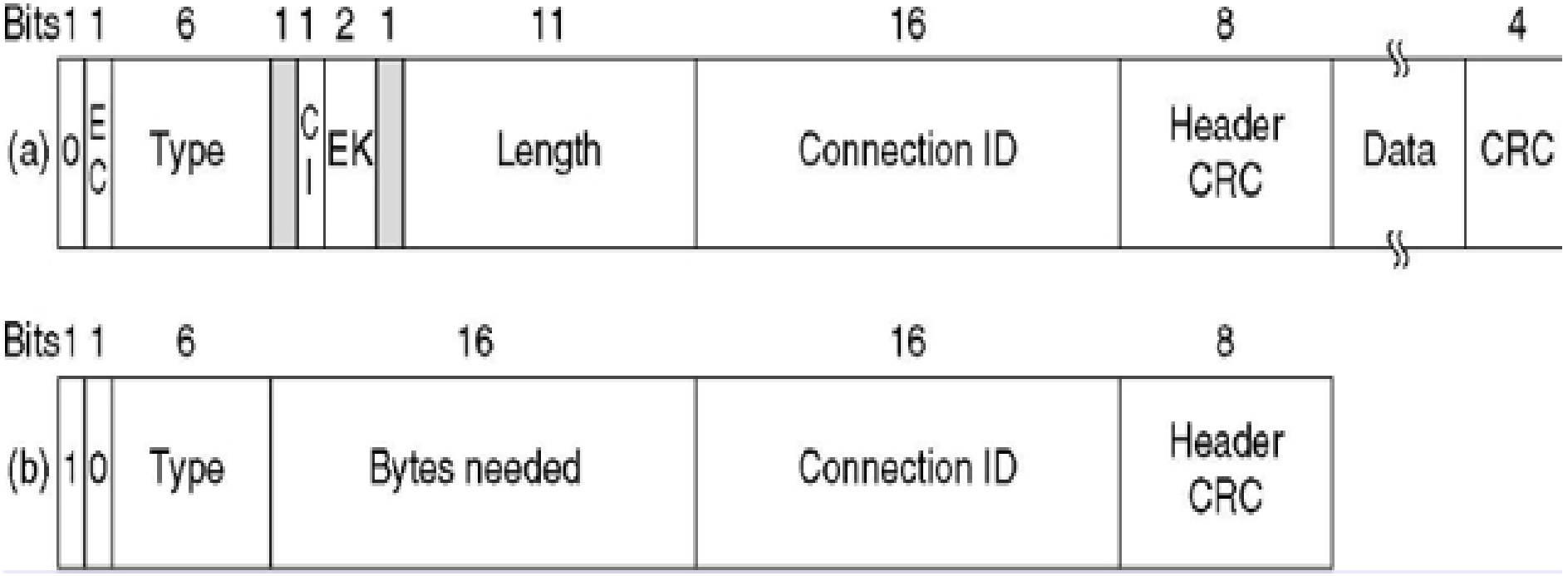
- Security
  - A subscriber connects to a base station, they perform mutual authentication with RSA public-key cryptography using X.509 certificates.
  - The payloads themselves are encrypted using a symmetric-key system, either DES with cipher block chaining or triple DES with two keys. AES (Rijndae1) is likely to be added soon.
  - Integrity checking uses SHA-1.

The 802.16: MAC Sublayer Protocol

- Service Classes
  - Constant bit rate service
  - Real-time variable bit rate service
  - Non-real-time variable bit rate service
  - Best efforts service

The 802.16: Frame Structure

(a) A generic frame. (b) A bandwidth request frame.



The 802.15 or Bluetooth

- In 1994, the L.M. Ericsson company → connecting its mobile phones to other devices without cables.
  - Ericsson, IBM, Intel, Nokia, and Toshiba
  - SIG (Special Interested Group)
- SIG → develop a wireless standard for interconnecting computing and communication devices and accessories using short-range, low power, inexpensive wireless radios
- In 1999 → a 1500 page specification of V1.0.
- In 2002 → V1.1, (3 Com, Agere, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia and Toshiba, and …).

Bluetooth

- Bluetooth Architecture
- Bluetooth Applications
- The Bluetooth Protocol Stack
- The Bluetooth Radio Layer
- The Bluetooth Baseband Layer
- The Bluetooth L2CAP Layer
- The Bluetooth Frame Structure

The 802.15

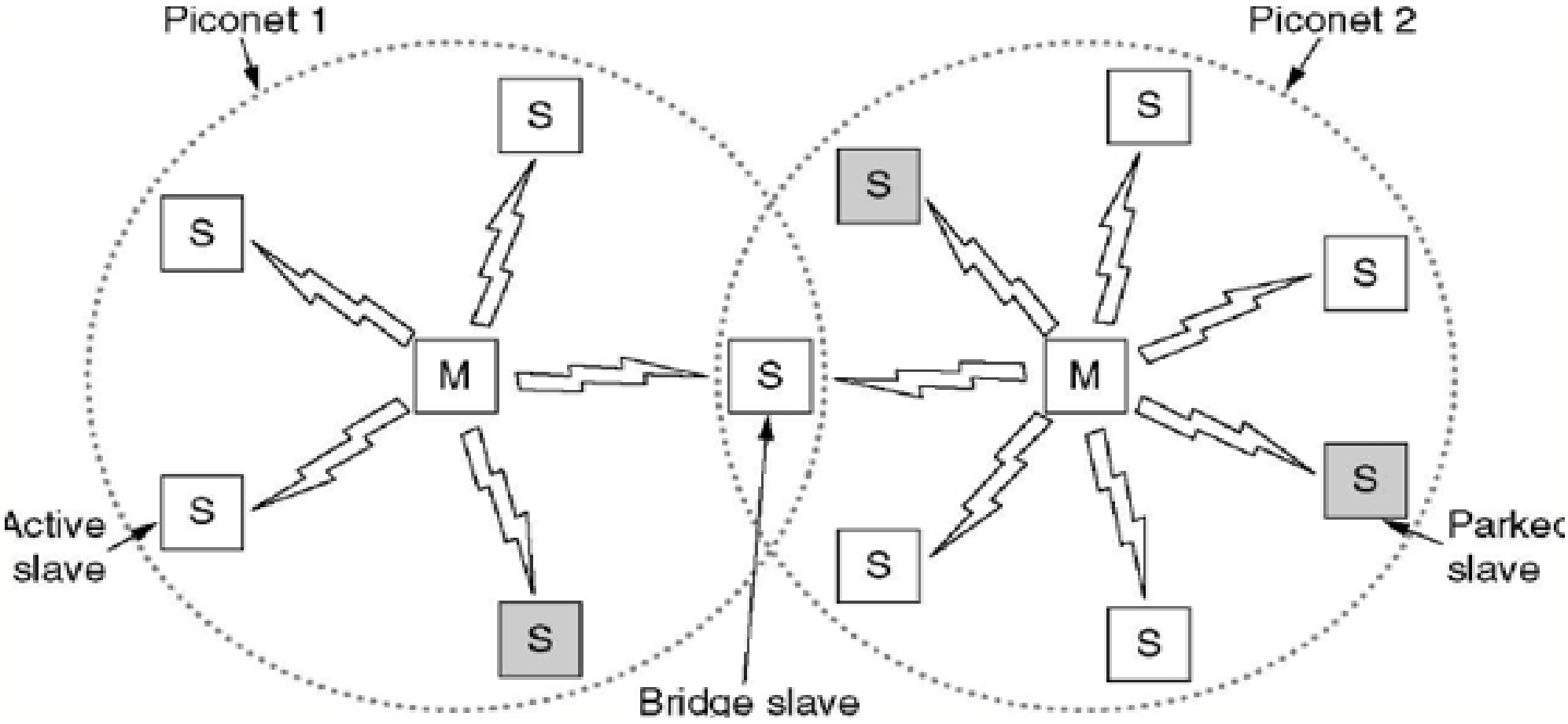
- IEEE WPAN (Wireless Personal Area Networks)
- 802.15 is based on Bluetooth
- 802.15 covers the physical layer and data link layer
- 802.15 is open
- In 2002, 802.15.1

Bluetooth: Architecture

- Piconet: The basic unit of a Bluetooth system
  - A *master* node
  - Up to seven *active* slave nodes within a distance of 10 meters.
  - Up to 255 *parked* nodes in the net. In *parked* state, a device cannot do anything except respond to an activation or beacon signal from the master.
- Scatternet: Multiple piconets can exist in the same (large) room and can even be connected via a bridge node.

Bluetooth: Architecture

Two piconets can be connected to form a scatternet.



Bluetooth: Architecture

- A piconet is a centralized TDM system, with the master controlling the clock and determining which device gets to communicate in which time slot.
  - All communication is between the master and a slave; direct slave-slave communication is not possible.
  - The reason for the master/slave design is to reduce the cost of the complete Bluetooth chips: under $5.

Bluetooth: Application

The Bluetooth profiles/applications

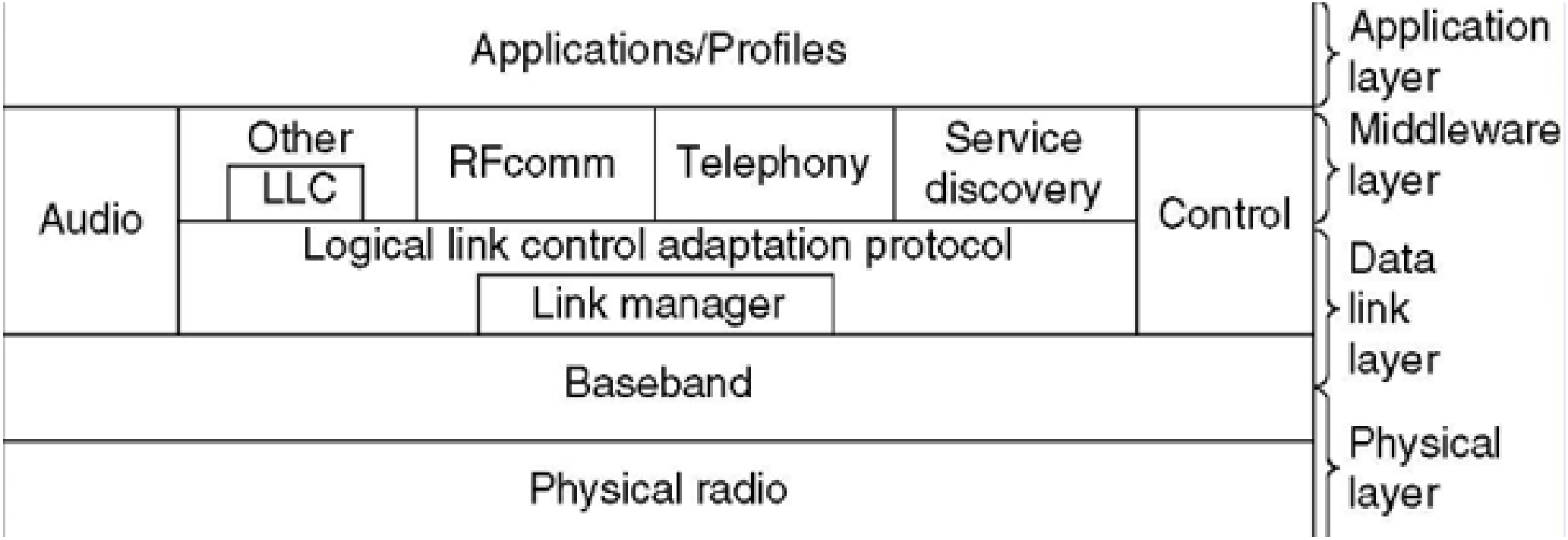
Name	Description
Generic access	Procedures for link management
Service discovery	Protocol for discovering offered services
Serial port	Replacement for a serial port cable
Generic object exchange	Defines client-server relationship for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial-up networking	Allows a notebook computer to call via a mobile phone
Fax	Allows a mobile fax machine to talk to a mobile phone
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie-talkie
Headset	Intended for hands-free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits a PDA to synchronize with another computer

Bluetooth: Application

- Generic access and service discovery are the basis. The rest profiles are optional.
- Serial port and generic object exchange
- LAN access, dial-up networking, FAX
- Cordless telephony, intercom, headset
- Object push, file transfer, synchronization.
- Why so many applications? Maybe Conway's law
  - **The software structure mirrors the structure of the group that produced it.**

Bluetooth: Protocol Stack

The 802.15 version of the Bluetooth protocol architecture.



Bluetooth: Protocol Stack

- The physical radio layer:
  - To deal with radio transmission and modulation.
  - Many of the concerns here have to do with the goal of making the system inexpensive so that it can become a mass market item.
- The baseband layer:
  - To deal with how the master controls time slots and how these slots are grouped into frames.
- Data link layer
  - The link manager handles the establishment of logical channels between devices, including power management, authentication, and QOS.
  - The logical link control adaptation protocol (L2CAP) shields the upper layers from the details of transmission.
  - Audio
  - control

Bluetooth: Protocol Stack

- Middleware layer
  - LLC
  - RFComm (Radio Frequency communication)
  - Telephony
  - Service discovery
- Application layer
  - Headset
  - ……

Bluetooth: Radio Layer

- The radio layer moves the bits from master to slave, or vice versa
- 2.4GHz ISM band
- The band is divided into 79 channels of 1MHz each
- To allocate the channels fairly, frequency hopping spread specturm is used with 1600hops/sec and a dwell time of 625usec.
- The interference among 802.11 and 802.15

Bluetooth: Baseband Layer (MAC)

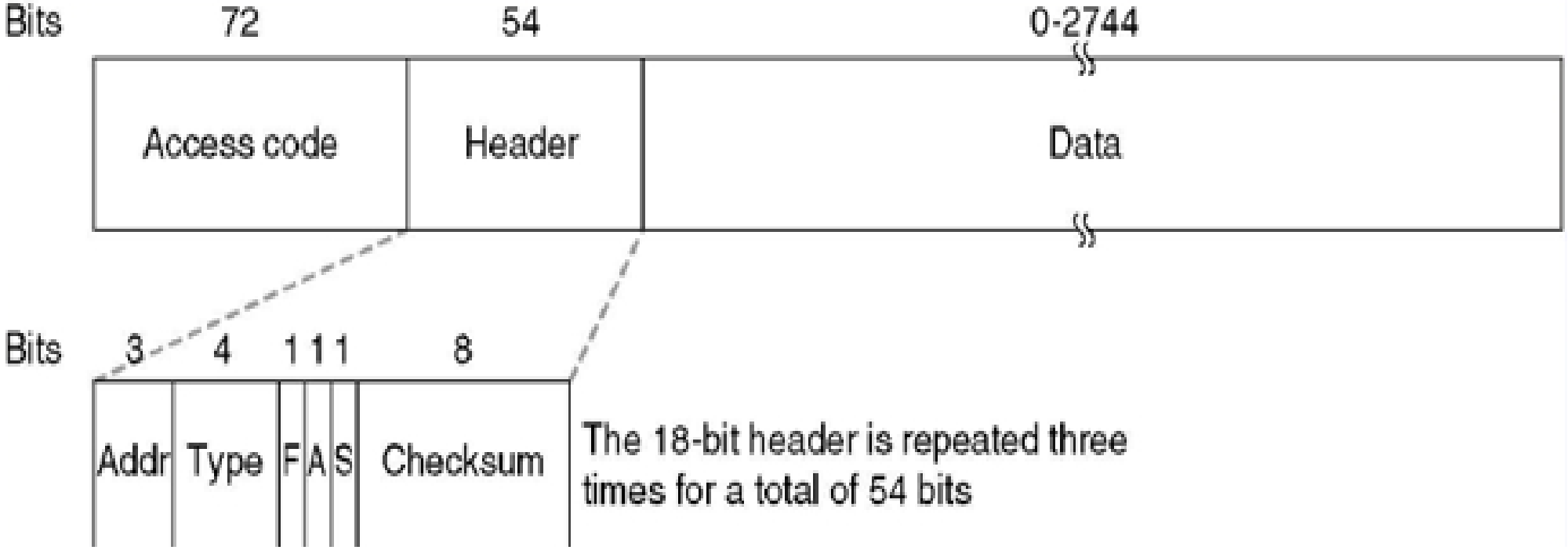
- To turn the raw bit stream into frames and defines some key formats.
- The frequency hopping timing. For a single 625 usec time slot.
  - 250-266 usec for becoming stable.
  - 126 bits for an access code and the header.
  - 240 bits for data.
- Two kinds of link
  - ACL (Asynchronous Connection-Less)
  - SCO (Synchronous Connection Oriented)

Bluetooth: L2CAP Layer

- Three major functions
  - It accepts packets of up to 64KB from the upper layers and breaks them into frames for transmission. At the far end, the frames are reassembled into packets again.
  - It handles the multiplexing and demultiplexing of multiple packet sources.
  - It handles the QoS requirements, both when links are established and during normal operation.

Bluetooth: Frame Structure

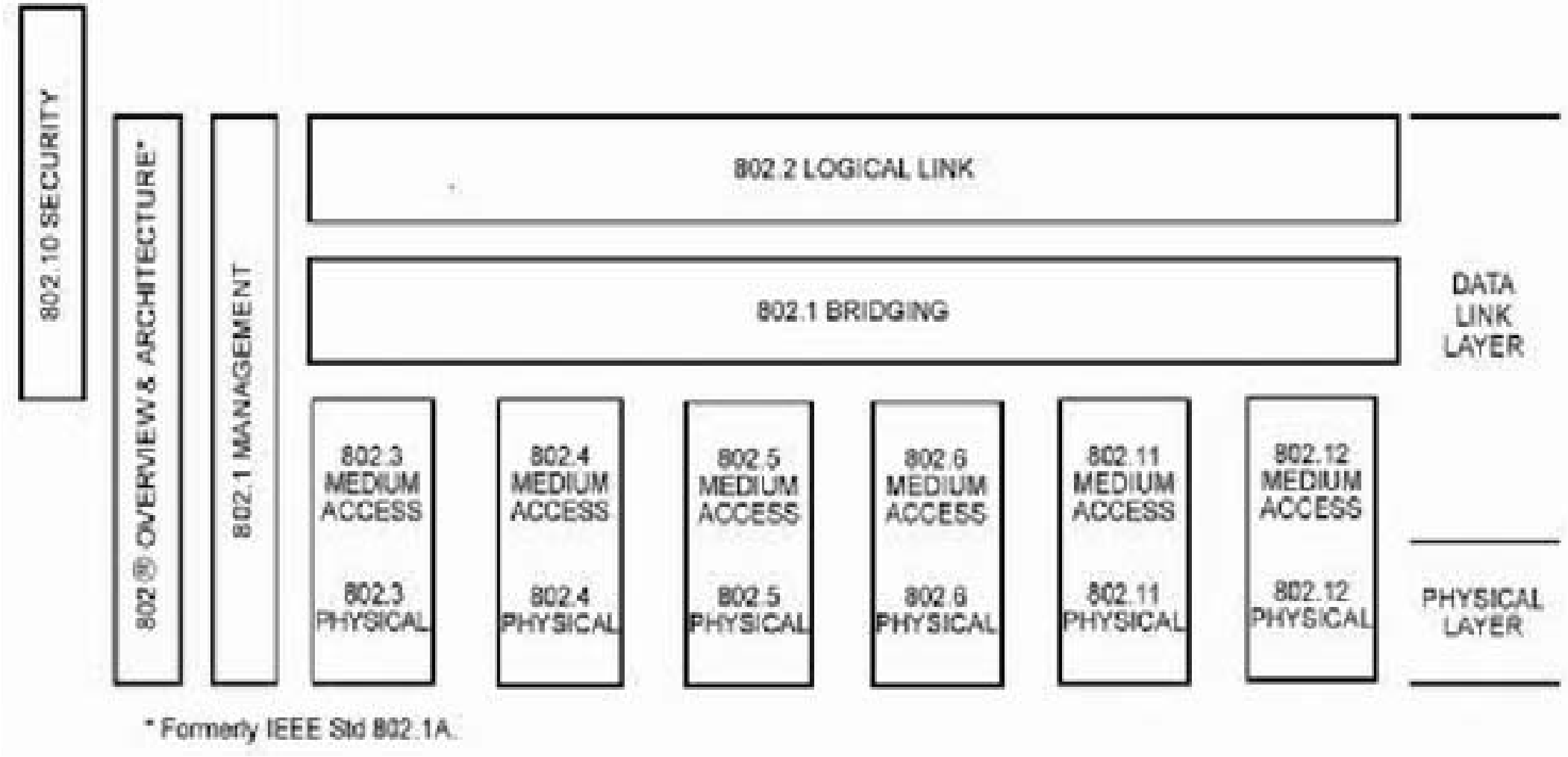
A typical Bluetooth data frame.



IEEE 802

- The survivors
  - 802.3: Ethernet (for wired LAN)
  - 802.11: WiFi (for wireless LAN)
- The potential ones
  - 802.15: Bluetooth
  - 802.16: WiMax (for Wireless MAN)
- The inactive ones
  - 802.4: Token bus
  - 802.5: Token ring
  - ….

IEEE 802


802.10 SECURITY
802.® OVERVIEW & ARCHITECTURE*
802.1 MANAGEMENT
802.2 LOGICAL LINK
802.1 BRIDGING
DATA LINK LAYER
802.3 MEDIUM ACCESS
802.3 PHYSICAL
802.4 MEDIUM ACCESS
802.4 PHYSICAL
802.5 MEDIUM ACCESS
802.5 PHYSICAL
802.6 MEDIUM ACCESS
802.6 PHYSICAL
802.11 MEDIUM ACCESS
802.11 PHYSICAL
802.12 MEDIUM ACCESS
802.12 PHYSICAL
PHYSICAL LAYER
* Formerly IEEE Std 802.1A.

IEEE 802: LLC (Logical Link Control)

- LLC
  - To hide the differences between the various kinds of 802 networks.
  - To provide a single format and interface to the network layer.

IEEE 802: LLC

- How LLC works
  - The network layer on the sending machine passes a packet to LLC, using the LLC access primitives.
  - The LLC sublayer adds an LLC header, containing sequence and acknowledgement numbers, and then passes the resulting structure into the payload field of an 802 frame for transmission.
  - At the receiver, the reverse process takes place.
- LLC provides three service options:
  - unreliable datagram service,
  - acknowledged datagram service,
  - reliable connection-oriented service.

Homework

1. A group of N stations share a 56-kbps pure ALOHA channel. Each station outputs a 1000-bit frame on average once every 100 sec, even if the previous one has not yet been sent (e.g., the stations can buffer outgoing frames). What is the maximum value of N?

2. Consider the delay of pure ALOHA versus slotted ALOHA at low load. Which one is less? Explain your answer.

3. Sixteen stations, numbered 1 through 16, are contending for the use of a shared channel by using the adaptive tree walk protocol. If all the stations whose addresses are prime numbers suddenly become ready at once, how many bit slots are needed to resolve the contention?

Homework

4.Six stations, A through F, communicate using the MACA protocol. Is it possible for two transmissions to take place simultaneously? Explain your answer.

5. Consider building a CSMA/CD network running at 1Gbps over a 1-km cable with no repeaters. The signal speed in the cable is 200,000 km/sec. What is the minimum frame size?

6. Please show the differences between

(a) The Ethernet CSMA/CD protocol and the 802.11 CSMA/CA protocol

(b) The MACA protocol and the 802.11 CSMA/CA protocol

Homework

7. An unscrupulous host, A, connected to an 802.3 (Ethernet) network biases their implementation of the binary exponential backoff algorithm so they always choose from {0,1} after a collision, in any situation.
Another host, B, is trying to send a frame at the same time as A. Assuming A and B collide exactly three times before one of their transmissions succeeds, what are the odds that B sends its frame before A(as opposed to A sending before B)?

Homework

8. Consider the following wireless network, where the circles are showing transmission ranges, and the presence of a host (letter) in a particular circle indicates it can hear that transmitter. If hosts A and C are both trying to send to host B will they encounter the hidden or exposed station problems? Does the MACA protocol help in this situation?

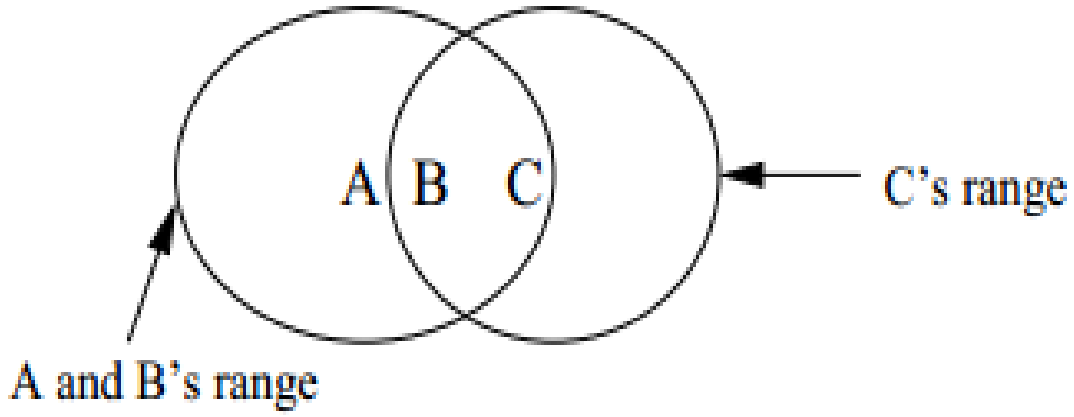


Figure 1: MACA Network showing transmission ranges for Question 8.

Homework

9. Consider the extended LAN connected using bridges B1 and B2in Fig. 4-41(b). Suppose the hash tables in the two bridges are empty. List all ports on which a packet will be forwarded for the following sequence of data transmissions:
(a) A sends a packet to C.
(b) E sends a packet to F.
(c) F sends a packet to E.
(d) G sends a packet to E.
(e) D sends a packet to A.
(f) B sends a packet to F.