BEng Course B38CN: Introduction to Communications and Networks

Chapter 4. The Medium Access Control Sublayer

Sheng Tong

Xidian University

School of Telecommunications Engineering

Room: I-304, Main Building, North Campus

E-mail: ts_xd@163.com

Acknowledgement: these slides are adapted from those from Prof. Cheng-Xiang Wang.

Contents (1/2)

Contents (2/2)

4 The Medium Access Control Sublayer

- This chapter deals with **broadcast networks** and their protocols.
- **Key issue** in Broadcast network: How to determine who gets to use the **broadcast channel** (**multiaccess channel** or **random access channel**) when there is competition for it?
- **MAC (medium access control) sublayer**: bottom part of the data link layer, especially important in LANs.

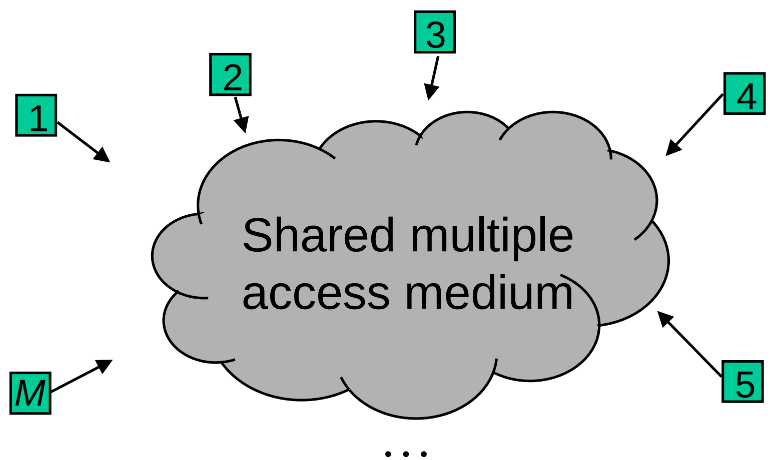

Fig. 4.1: Multiple access communications.

4.1 The Channel Allocation Problem

- How to **allocate** a single broadcast channel among multiple competing users?
  - Static and dynamic

4.1.1 Static Channel Allocation in LANs and MANs

- Example of traditional ways:
  - **Frequency Division Multiplexing (FDM)**: Divide the bandwidth into *N* equal sized portions, each user being assigned one portion.
  - **Time Division Multiplexing (TDM)**: Each user is statically allocated every *N*th time slot.
- **Collision free**; Suitable when users generate a steady stream of data.
- **Problems** occur for bursty traffic: waste resource.

4.1.2 Dynamic Channel Allocation in LANs and MANs

- **Primary function**: Minimize or eliminate the incidence of **collisions** to achieve a **reasonable utilization** of the medium.

- Five **key assumptions** for dynamic channel allocation:
  - **Station model**: The model consists of N independent stations (terminals), each with a program or user that generates frames for transmission.
    - Once a frame is generated, the station is blocked until the frame has been successfully transmitted.
  - **Single channel assumption**: no external ways to communicate.

Key Assumptions for Dynamic Channel Allocation (Cont.)

- **Collision assumption**: Collision occurs if two frames are transmitted simultaneously.
  - All stations can detect collisions.
  - A collided frame must be transmitted again later.
- **Time**:
  - **Continuous time**: Frame transmission can begin at any instant.
  - **Slotted time**: Time is devided into **discrete** intervals (slots). Frame transmissions always begin at the start of a slot.
- **(No) Carrier Sense**:
  - **Carrier sense**: Stations can tell if the channel is in use before trying to use it.
  - **No carrier sense**: Stations cannot sense the channel and they just transmit frames.

4.2 Multiple Access Protocols

4.2.1 ALOHA

- **Two versions**: pure and slotted (requires global time **synchronization**), depending on whether time is divided into discrete slots.
- **Pure ALOHA**: Let users transmit whenever they have data to be sent. If a collision occurs, the sender just waits a random time and retries.

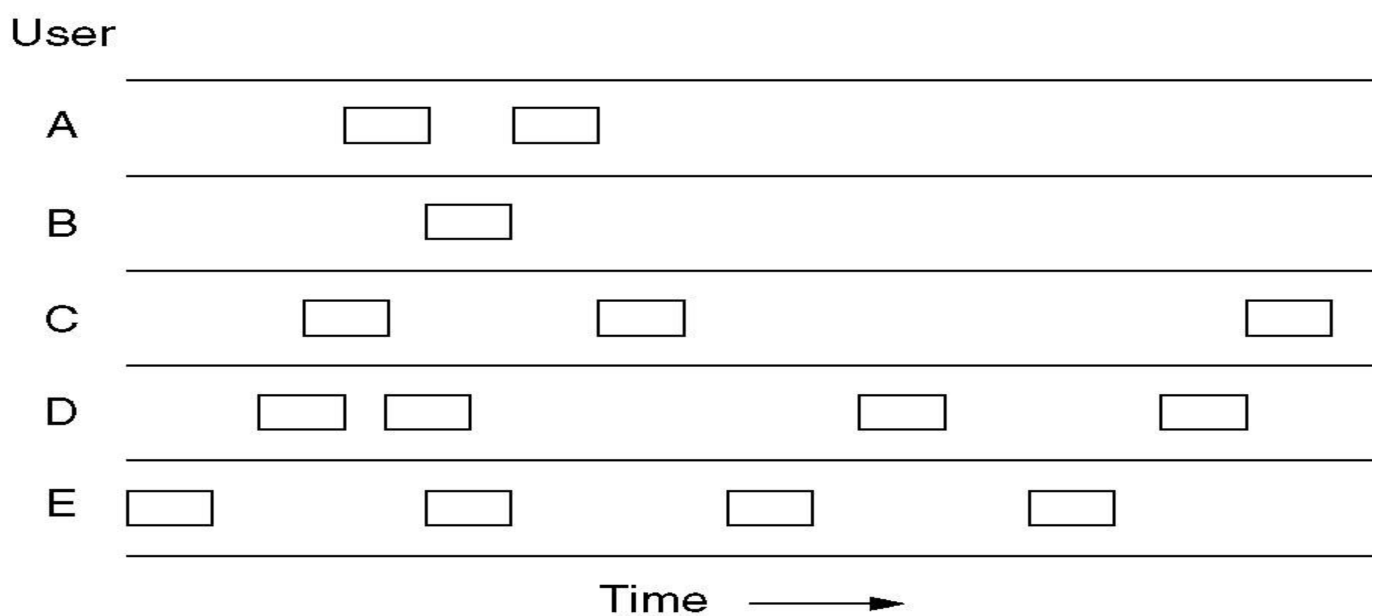

Fig. 4.2: In pure ALOHA, frames are transmitted at completely arbitrary times.

Vulnerable Period for a Frame with Pure ALOHA

- Under what conditions will the shaded frame arrive successfully?
- A frame will not suffer a **collision** if no other frames are sent within the **vulnerable period** t_0 to t_0+2t.

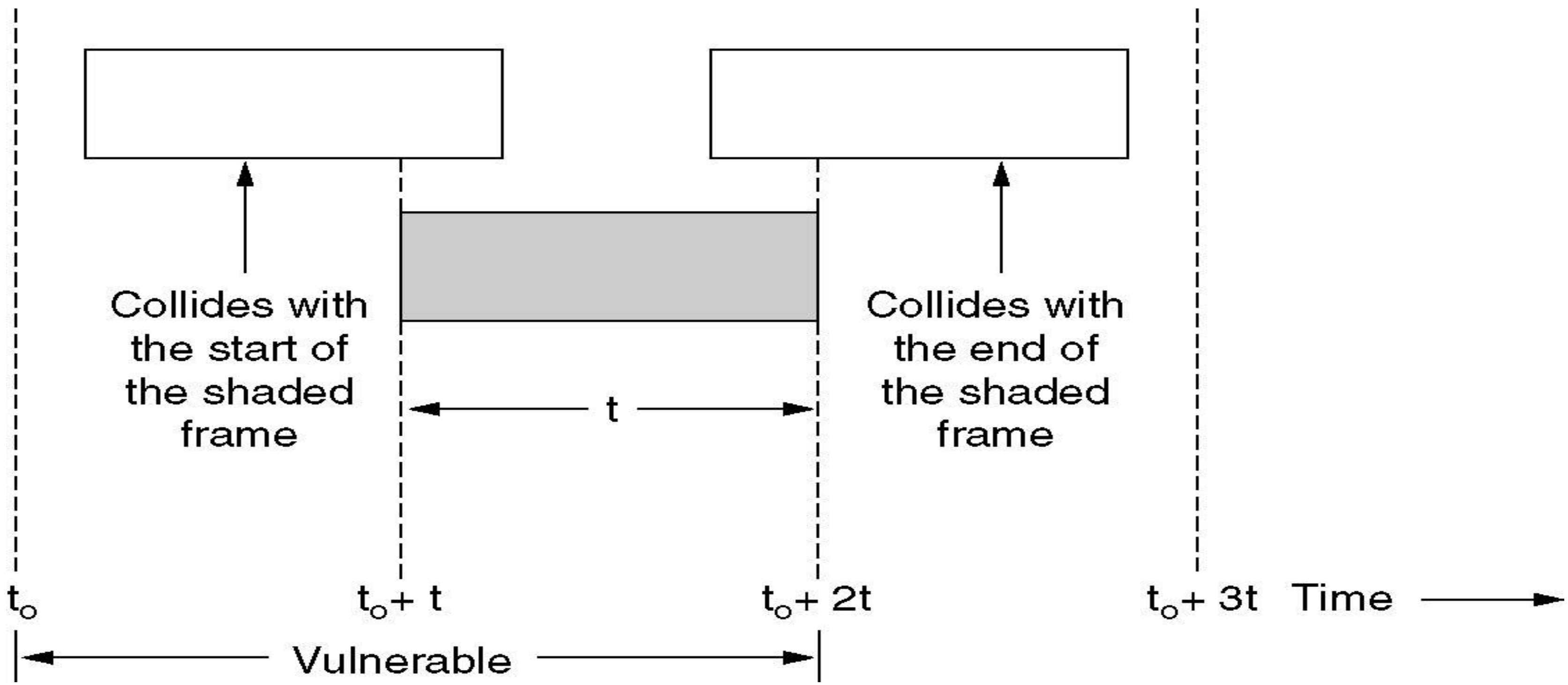

Fig. 4.3: Vulnerable period for the shaded frame.

Efficiency of Pure ALOHA

- **Frame time**: the time needed to transmit a standard, fixed-length frame, i.e., (frame length)/(bit rate).
- **Throughput S**: the average number of **successfully transmitted frames** per frame time.
- ***N***: the average number of **new frames generated** by users per frame time. Poisson distributed!
- ***G***: the average number of **transmission attempts**, old (retransmission) and new frames combined, per frame time. $G \geq N$ and $G \geq S$. Also Poisson distributed!
- P_0: the probability of a **transmission success**, i.e., the probability that a frame does not suffer a collision.

  ⇨ $S = GP_0 = Ge^{-2G}$.

Slotted ALOHA

- Divide time into **discrete** intervals, each interval corresponding to one frame.
- Requires the users to agree on **slot boundaries** (**synchronization**).
- A computer is not permitted to send until the start of the next slot.
  - ⇨ The **continuous** pure ALOHA →**discrete** slotted ALOHA!
- The vulnerable period is **halved**!
  - ⇨ The probability of a **transmission success**: $P_0=e^{-G}$.
  - ⇨ $S=GP_0=Ge^{-G}$.

Throughput of Pure ALOHA and Slotted ALOHA

- **Pure ALOHA**: maximum throughput $\boldsymbol{S}_{\mathbf{max}}=0.5/e\approx0.184$ at $G=0.5$.
- **Slotted ALOHA**: maximum throughput $\boldsymbol{S}_{\mathbf{max}}=1/e\approx0.368$ at $G=1$.

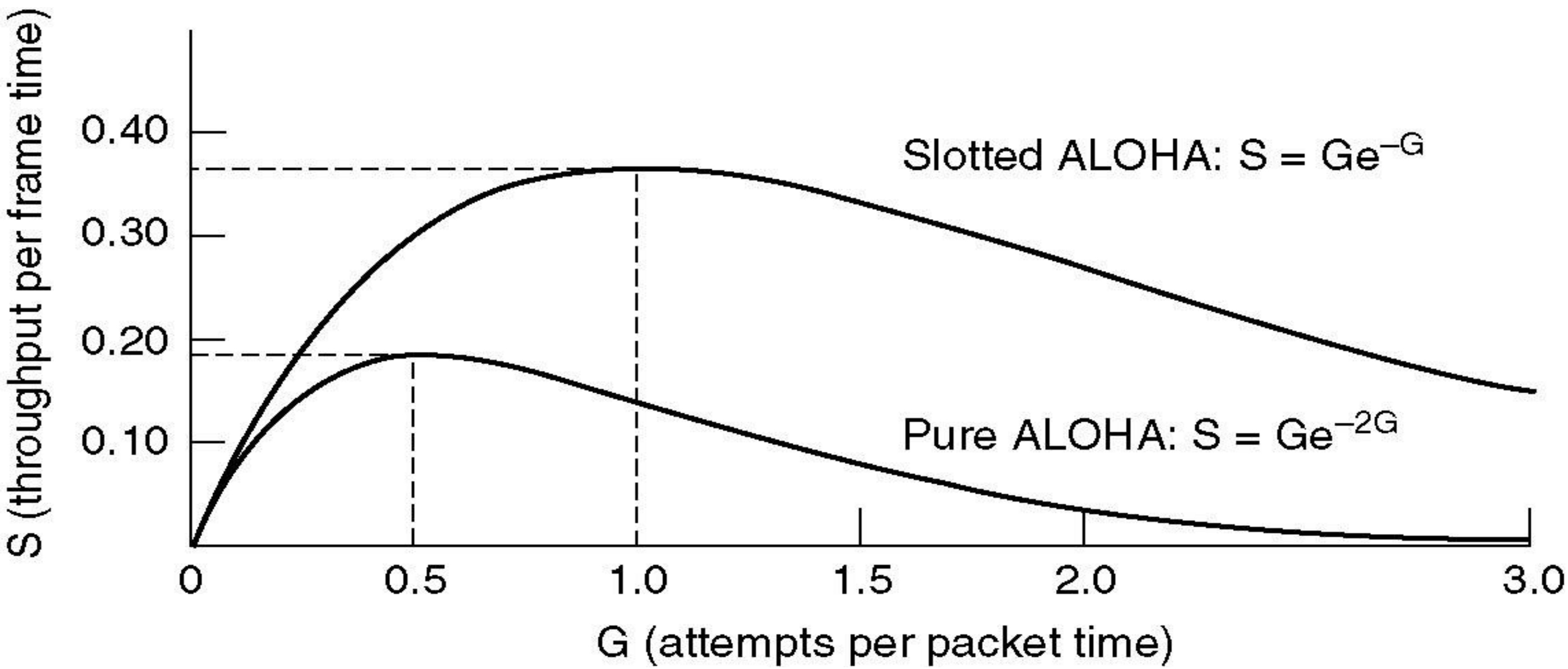

Fig. 4.4: Throughput versus offered traffic for ALOHA systems.

4.2.2 Carrier Sense Multiple Access Protocols

- **CSMA protocols**: better than ALOHA; **monitor** the channel before and/or during transmission.

- **1-persistent CSMA**: Listen whether the channel is free before transmitting. If busy, wait until it becomes free and then immediately start your transmission. The **name** is taken because the station transmits with a probability of 1 when it finds the channel idle.

- **Nonpersistent CSMA:** Less greedy – when the channel is busy, wait a random period of time (**not continuously sensing** the channel) before trying again. Better channel utilization but longer delay than 1-persistent CSMA.

- ***p*-persistent CSMA**: Used with **slotted systems**. If you find the channel idle during the current slot, you transmit with probability p, and defer until next slot with probability $1-p$.

Throughput Comparison of Random Access Protocols

- **Question**: Is 0-persistent CSMA really good?

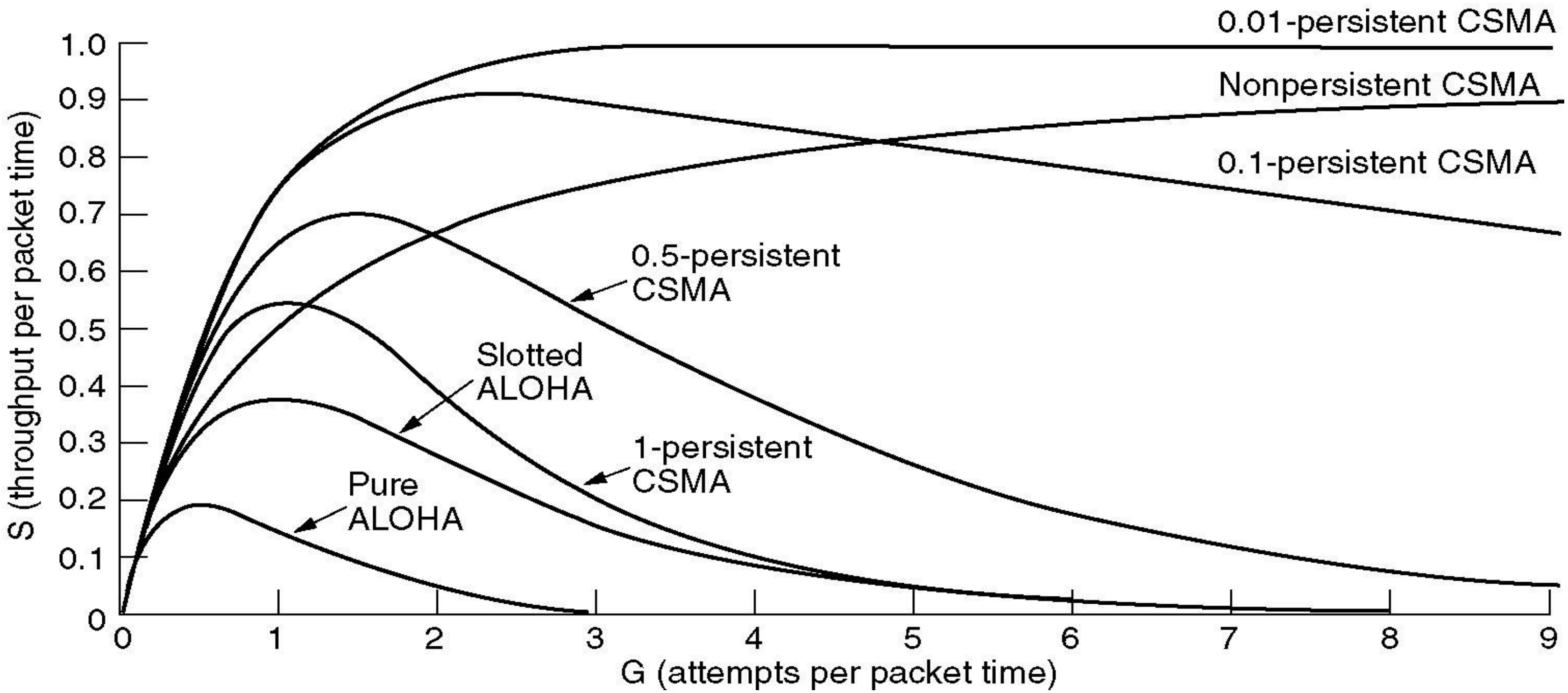

Fig. 4.5: Comparison of the channel utilization versus load for various random access protocols..

CSMA with Collision Detection

- **Improvement**: Sense the channel, but immediately stop transmission when you detect a collision. **Ethernet** works like this.
  1. **Listen** to see whether the channel is free. Transmission is delayed until the channel is no longer used.
  2. During transmission, keep listening in order to detect a collision. If a collision occurs, transmission **immediately stops**.
  3. If a collision occurs, wait a **random period** of time, and proceed with step 1.

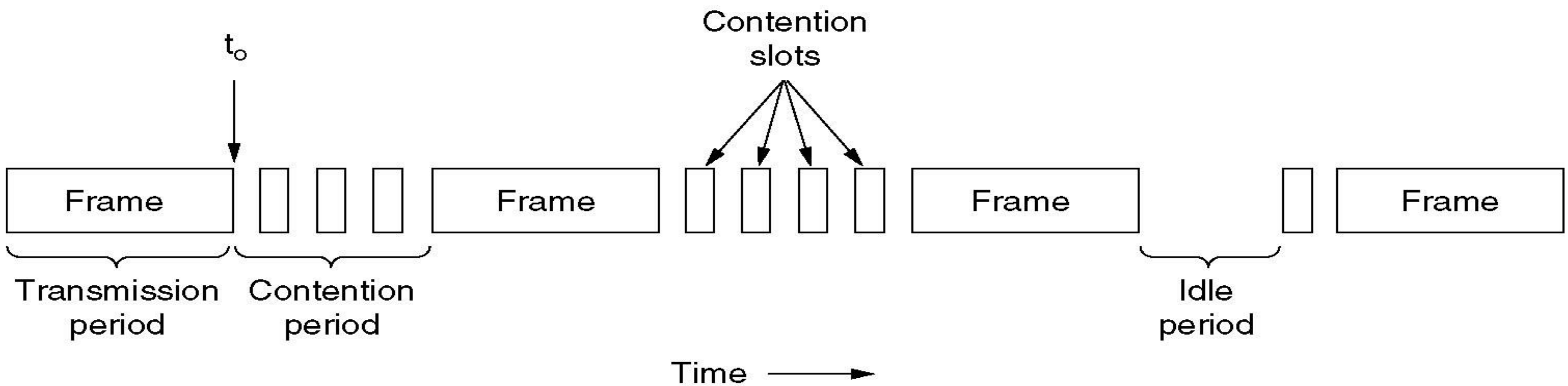

Fig. 4.6: CSMA/CD can be in one of three states: contention, transmission, or idle.

4.2.3 Collision-Free Protocols

- With CSMA/CD, collisions can still occur during the contension period.

  ⇒ Are there any protocols in which **collisions do not occur at all**?

- A **bit-map** protocol: The contention period contains *N* slots.
  - Starting from station 0, if station *j* (*j*=0, ..., *N*-1) wants to transmit a frame, it transmits a 1 bit into slot *j*. No other station is allowed to transmit during this slot.
  - 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.⇒**No collisions at all**!

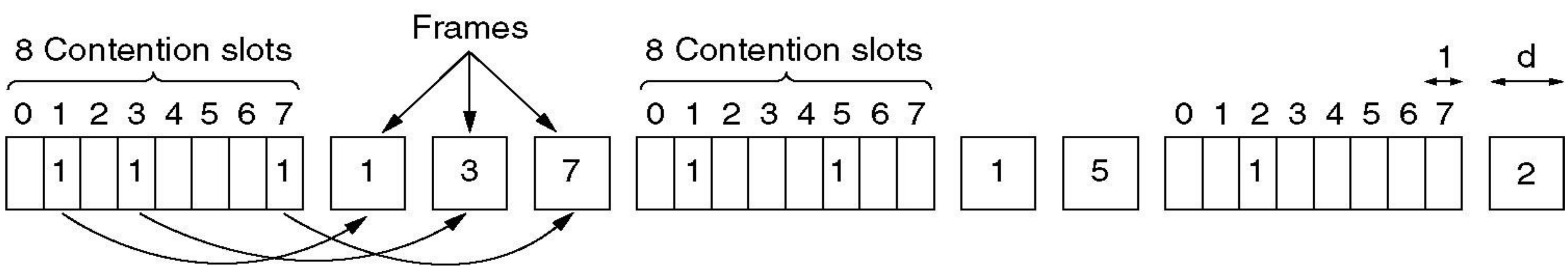

Fig. 4.7: The basic bit-map protocol.

Binary Countdown Protocols

- The binary countdown protocol used in **Datakit**:
  - All stations use **same-length binary addresses**. A station wanting to use the channel now braoadcasts its address as a binary bit string, **starting with** the **high-order bit**.
  - The bits in each address position from different stations are **OR**ed together.
  - 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.
  - The **winner** station will transmit a frame, after which another bidding cycle starts.
- **Mok and Ward's variation** of binary countdown:
  - Use **virtual station numbers**, with the virtual station numbers from 0 up to and including the successful station being circularly permuted after each transmission, in order to give **higher priority** to stations that have been silent unusually long.
  - **Example**: Stations *C*, *H*, *D*, *A*, *G*, *B*, *E*, *F* have priorities 7, 6, 5, 4, 3, 2, 1, and 0, respectively. A successful transmission by D will give a priority order of *C*, *H*, *A*, *G*, *B*, *E*, *F*, *D*.

The binary countdown protocol used in Datakit

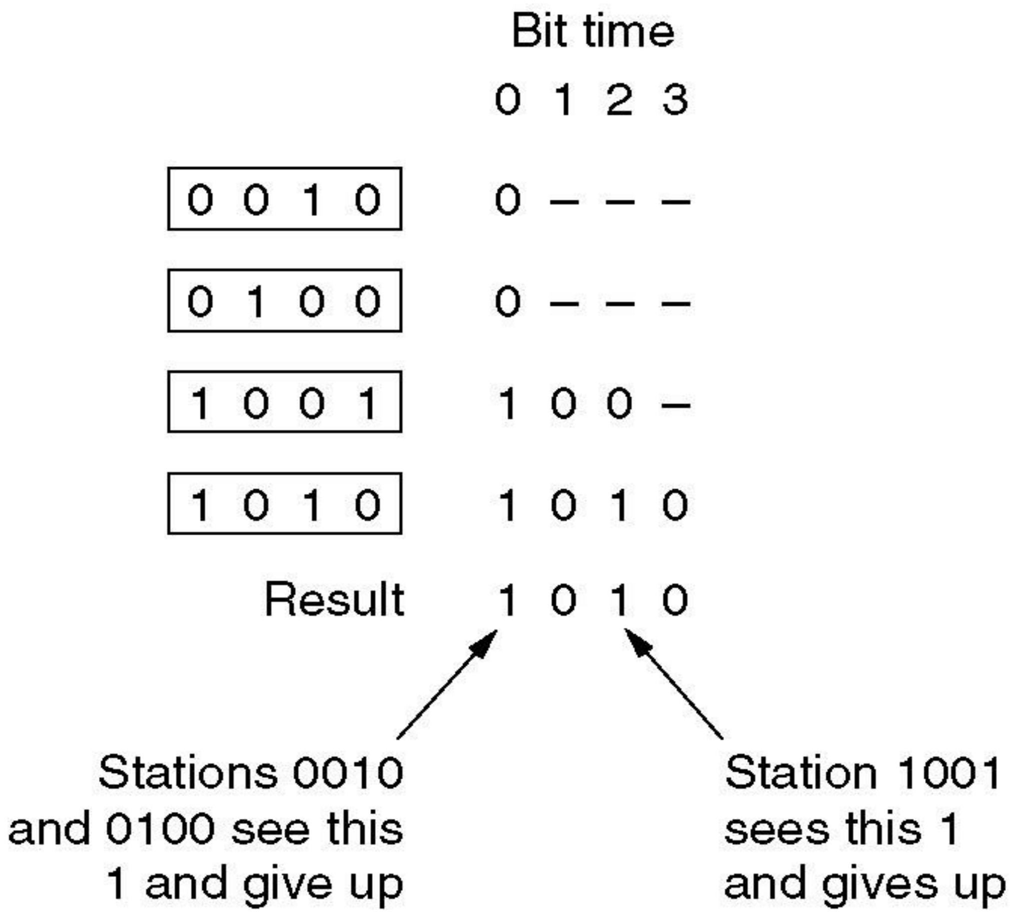

Fig. 4.8: The binary countdown protocol used in Datakit. A dash indicates silence.

4.2.4 Limited-Contention Protocols

- Two basic strategies for channel acquisition:
  - **Contention**: preferable under conditions of **light load** due to its **low delay**. As the load increases, the channel efficiency gets worse.
  - **Collision-free**: preferable under conditions of **high load** due to its **high channel efficiency**. At low load, it has high delay.

⇒ **Limited-contention protocols**: use contention at low load to provide low delay, but use a collision-free technique at high load to provide good channel efficiency.

The Adaptive Tree Walk Protocol

- Dynamically regulate the number of competing stations during a **contention period**.
- If there's a **collision** during the *k*th slot, divide the contenders into **two groups**.
- The **first group** gets to try it again during the next slot k+1. If no collisions occur then, the second group gets a try during the slot after that, i.e., slot k+2. Otherwise, the first group is split up again.

An Example of the Adaptive Tree Walk Protocol

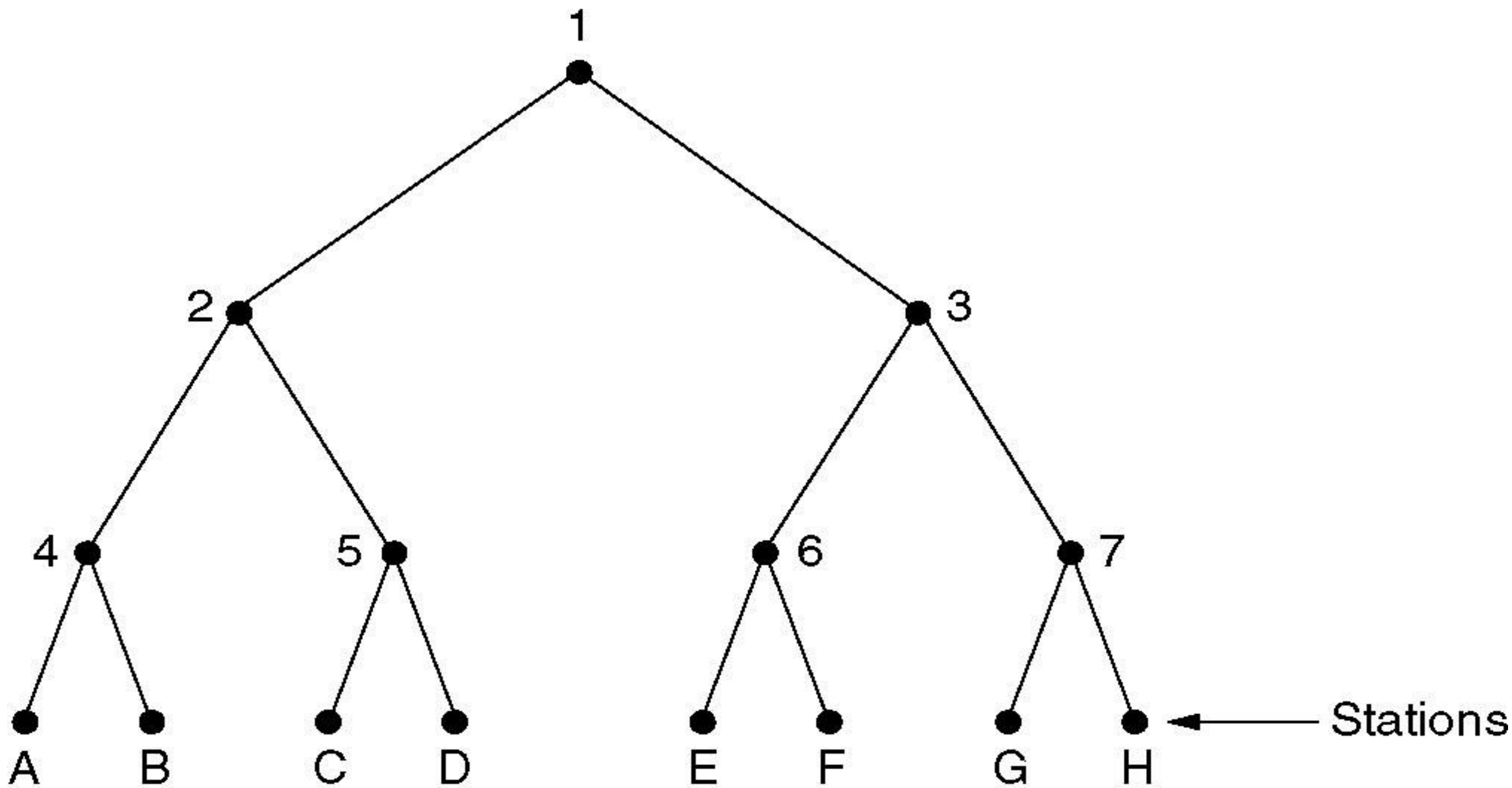

Fig. 4.9: The tree for eight stations.

4.3 Ethernet

- **IEEE 802.3**, CSMA/CD based.

4.3.1 Ethernet Cabling

4.3.2 Manchester Encoding

4.3.3 The Ethernet MAC Sublayer Protocol

4.3.4 The Binary Exponential Backoff Algorithm

4.3.5 Ethernet Performance

4.3.6 Switched Ethernet

4.3.7 IEEE 802.2: Logical Link Control

4.3.1 Ethernet Cabling

- **10Base5**: thick Ethernet; **10** Mbps, **B**aseband signalling, up to **5**00 meters per segment.
- **10Base2**: thin Ethernet; **10** Mbps, **B**aseband signalling, up to 185 meters per segment.
- **10 Base-T**: **10** Mbps, **B**aseband signalling, **T**wisted pair.
- **10Base-F**: **10** Mbps, **B**aseband signalling, **F**iber optics.

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

Fig. 4.10: The most common kinds of Ethernet cabling.

Ethernet Cabling

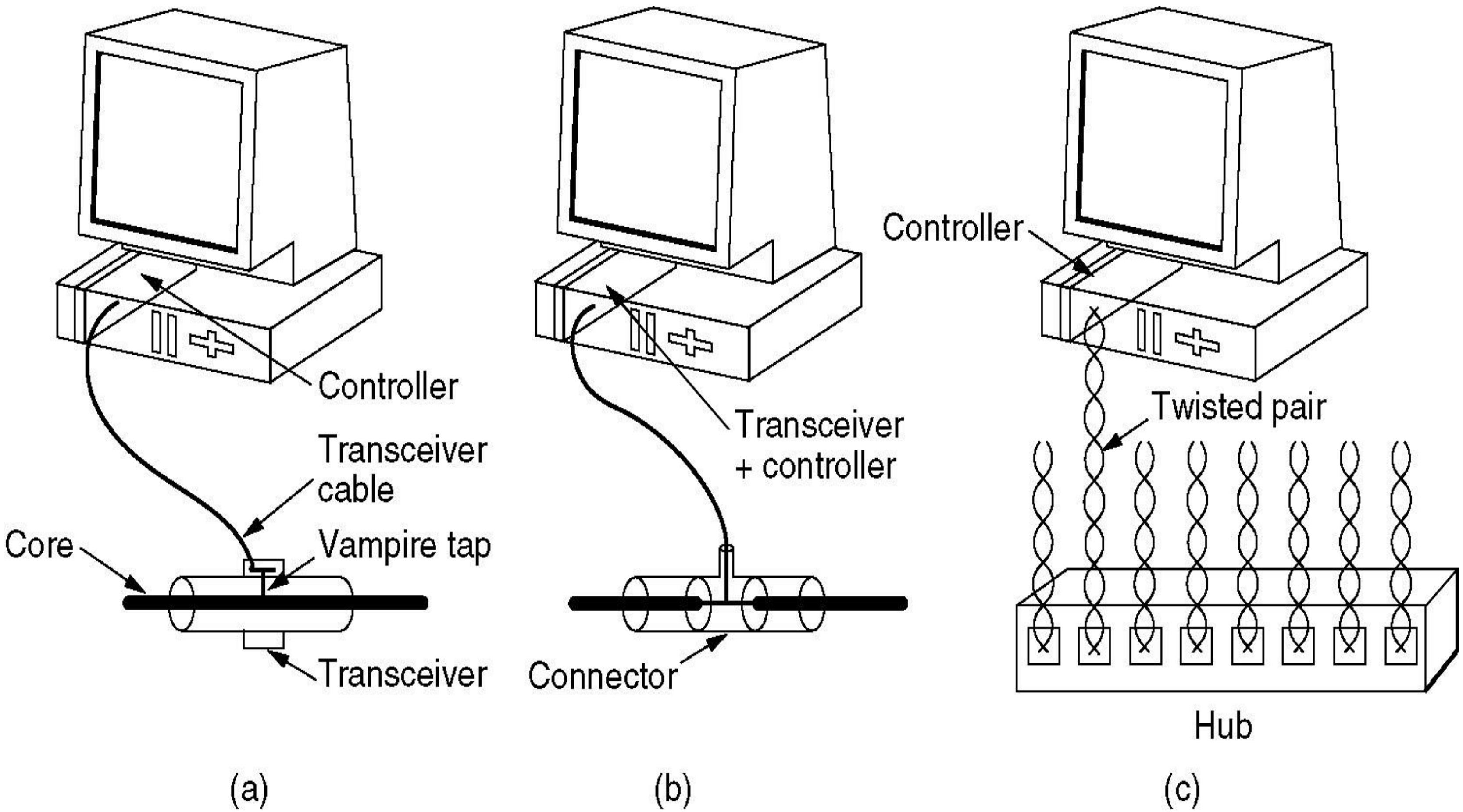

Fig. 4.11 Three kinds of Ethernet cabling. (a) 10Base5, (b) 10Base2, (c) 10Base-T.

Cable Topologies in Ethernet

- In **10Base-F** we can apply different schemes (linear, backbone, tree). Segmented networks with **repeaters** are used to build **large** networks.

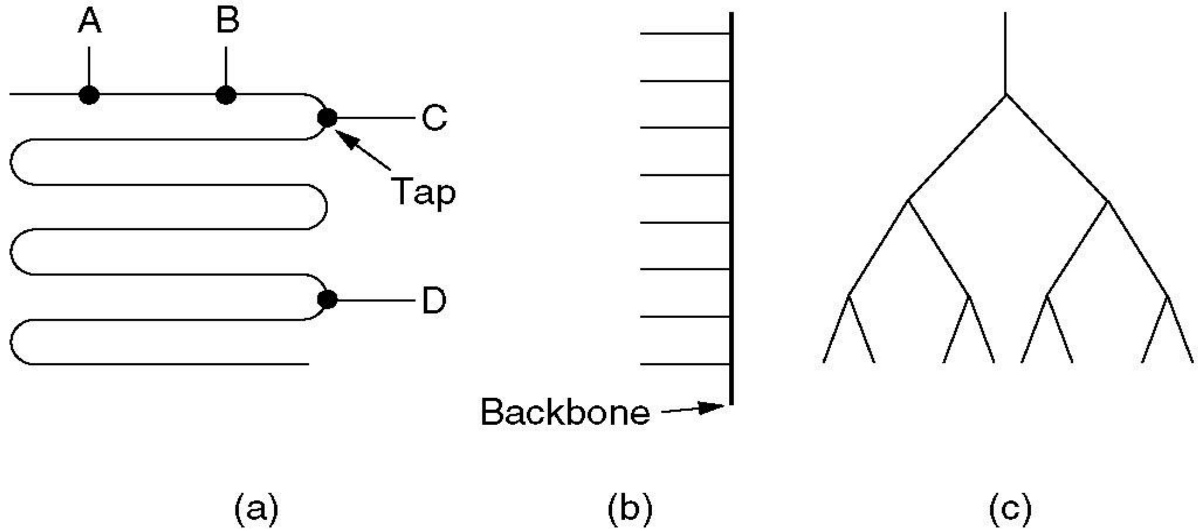

Fig. 4.12: Cable topologies. (a) Linear, (b) Spine, (c) Tree, (d) Segmented.

4.3.2 Manchester Encoding

- **Problem**: We cannot just send straight binary codes across the Ethernet, because stations can't distinguish a 0 bit (0 volts) from an idle sender (0 volts).
- **Manchester encoding**: 1 bit (high→low voltage); 0 bit (low→high); in all **Ethernet**.
- **Differential Manchester encoding**: 1 bit (absence of a transition at the start); 0 bit (presence of a transition at the start); in other LANs (e.g., **802.5 token ring)**.

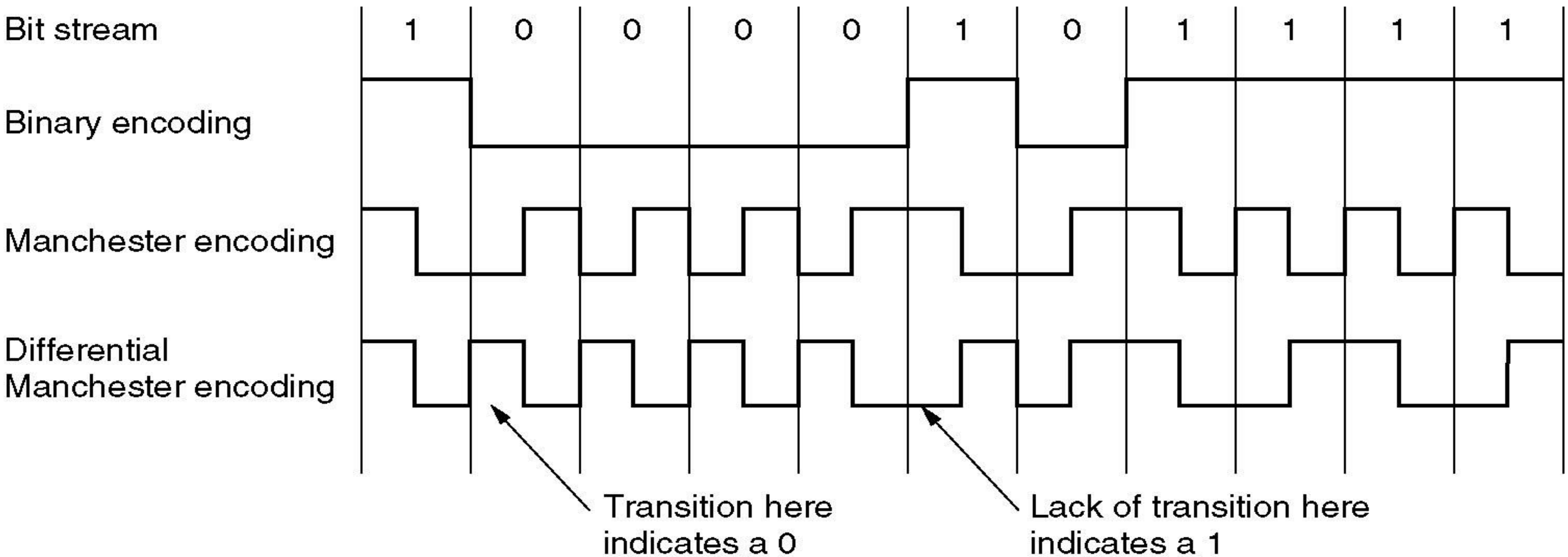

Fig. 4.13: (a) Binary encoding. (b) Manchester encoding. (c) Differential Manchester encoding.

4.3.3 Ethernet MAC Sublayer Protocol

- **Preamble:** 8/7 bytes of 10101010; synchronize the receiver's clock with the sender's.
- **SOF (start of frame):** Just a delimiter to tell that the real info is now coming.
- **Address:** Generally 48-bit fields. The leftmost bit indicates ordinary (0) or group (1) addresses. Second bit indicates global or local address.
- **Type**: Tells the receiver what to do with the frame. Minimum frame size: **64 bytes**.
- **Length:** Ranges from 0-1500. A **header** is necessary to be added to the data portion.
- **Pad:** If necessary, fill out the frame to the minimum size.
- **Checksum:** CRC-based.

Bytes	8		6	6	2	0-1500	0-46	4
(a)	Preamble		Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble	SOF	Destination address	Source address	Length	Data	Pad	Check-sum

Fig. 4.14: Frame formats. (a) DIX Ethernet. (b) IEEE 802.3.

4.3.4 The Binary Exponential Backoff Algorithm

- Ethernet is **CSMA/CD** based (sense the channel, wait until idle, and backoff after a random time when you detect a collision).
- How randomization is done **when a collision occurs**?

⇨ **Binary exponential backoff algorithm**:

  - After a collision, time is divided into **discrete slots**.
  - After the first collision, each station waits either 0 or 1 slot times before trying again.
  - After the second collision, each one picks either 0, 1, 2, or 3 at random and waits that number of slot times.
  - In general, after *i* collisions, a random number between 0 and 2^i-1 is chosen, and that number of slots is skipped.
  - After **10** collisions have been reached, the randomization interval is frozen at a **maximum of 1023 slots**.

4.3.5 Ethernet Performance

- **Channel Efficiency**$=1/(1+2BLe/cF)$.
  - ***B***: the network bandwidth; ***L***: the cable length; ***e***: the number of contention slots per frame; ***c***: light speed; ***F***: the frame length.

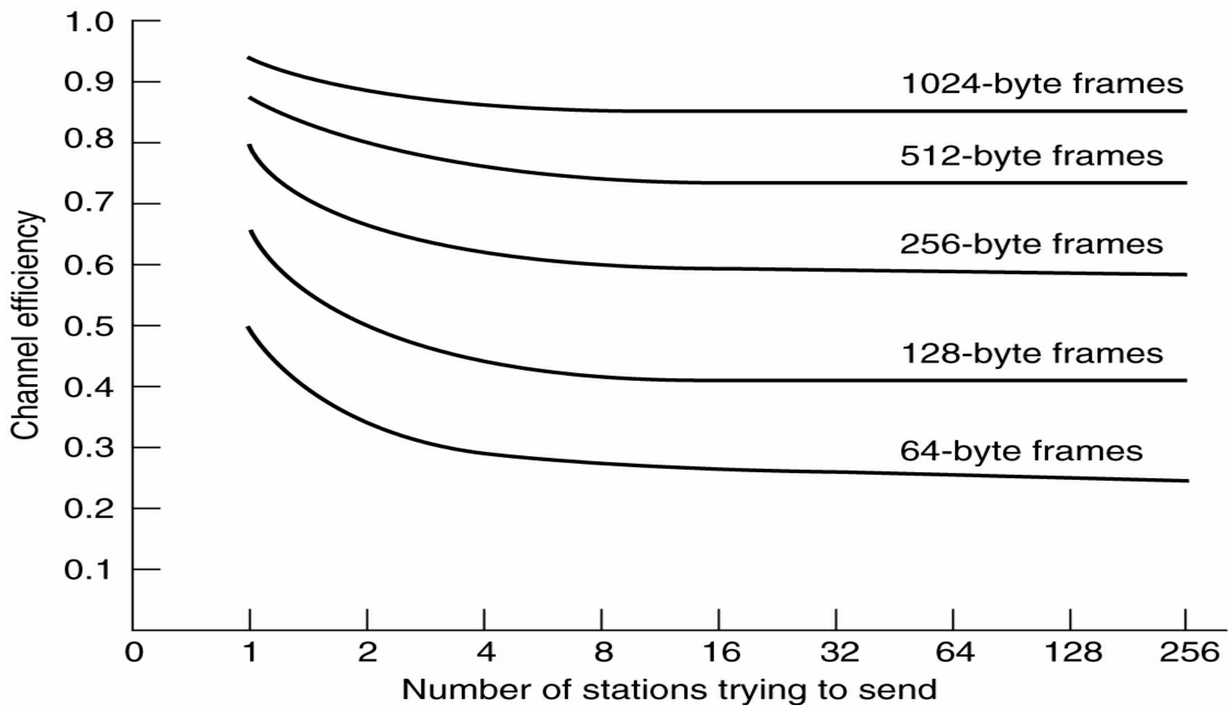

Fig. 4.15: Efficiency of Ethernet at 10 Mbps with 512-bit slot times.

4.3.6 Switched Ethernet

- **Problem**: As more stations are added to an Ethernet, the traffic will go up, and so will the possibility of collisions.⇨Eventually, the LAN will saturate.
- **Solution**: Divide the network into separate sub-LANs and connect them through a high-speed **switch**.

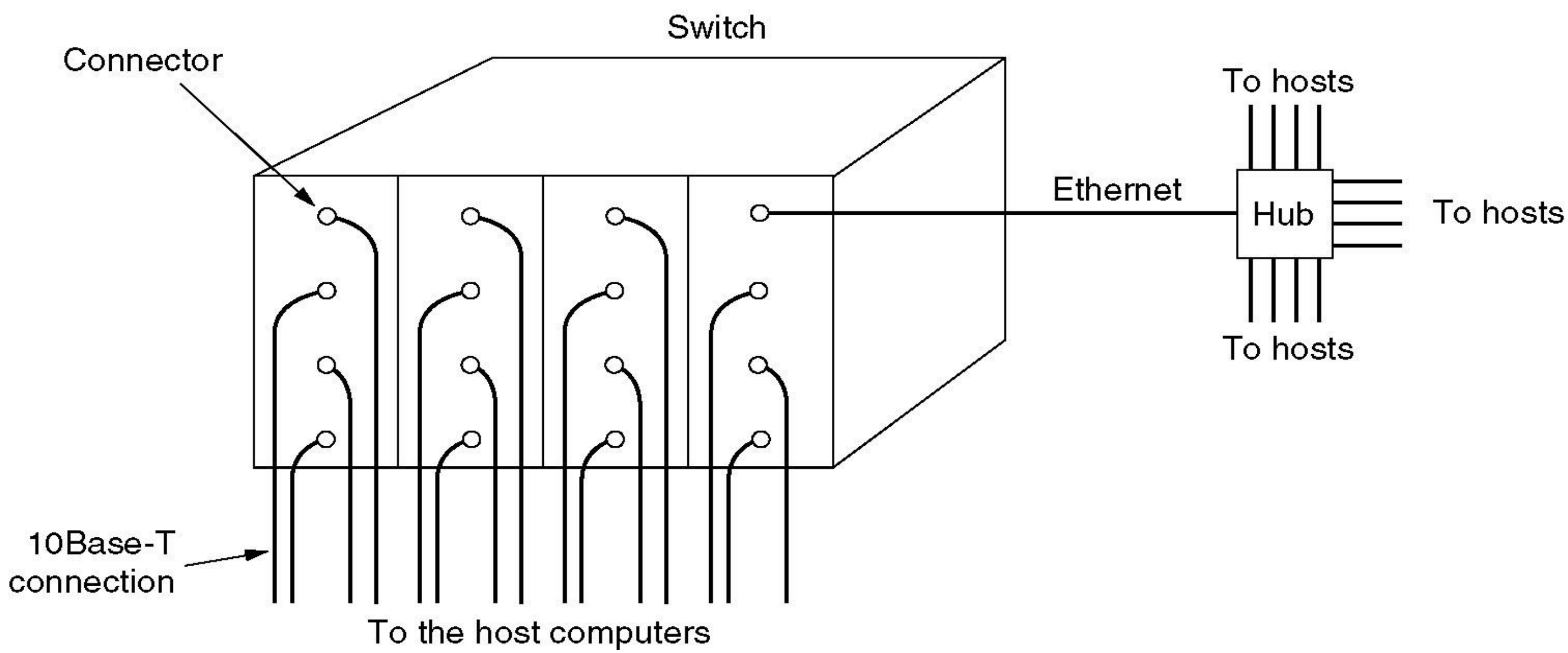

Fig. 4.16: A simple example of switched Ethernet.

4.3.7 IEEE 802.2: Logical Link Control

- The **upper half** of the data link layer.
- **LLC header**: a destination access point, a source access point, and a control field.
- **Three service options**: unreliable datagram service, acknowledged datagram servce, and reliable connection-oriented service.

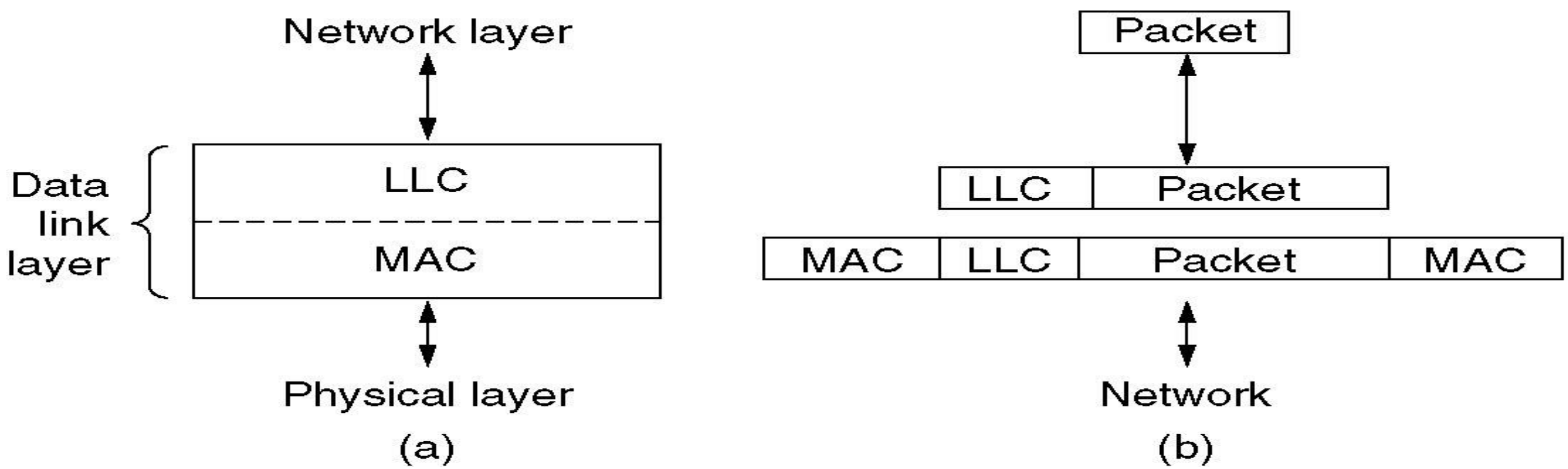

Fig. 4.17: (a) Position of LLC. (b) Protocol formats.

4.4 Wireless LANs

4.4.1 The 802.11 Protocol Stack

4.4.2 The 802.11 Physical Layer

4.4.3 The 802.11 MAC Sublayer Protocol

4.4.4 The 802.11 Frame Structure

4.4.5 Services

4.4.1 The 802.11 Protocol Stack

- **Physical layer**: 5 transmission techniques.
- **MAC sublayer**: determines how the channel is allocated.
- **LLC syblayer**: hides the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.

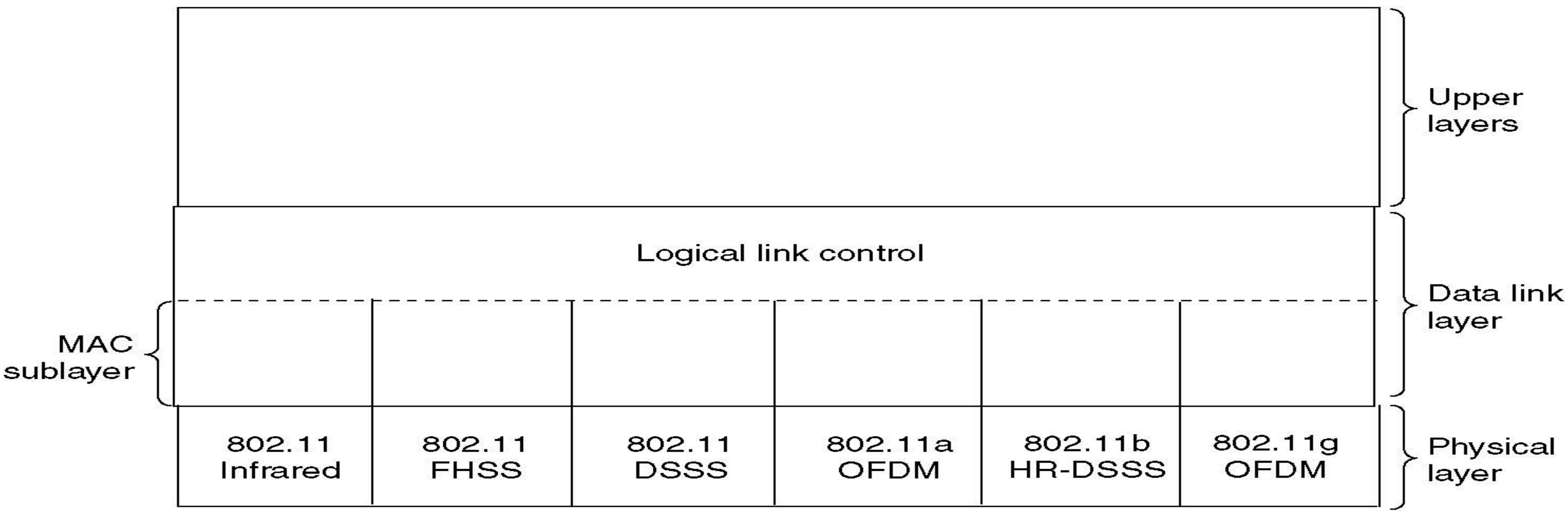

Fig. 4.18: Part of the 802.11 protocol stack.

4.4.2 The 802.11 Physical Layer

- **Infrared**: Two permitted speeds, 1 Mbps and 2 Mbps. Not very popular due to the low bandwidth and the fact that sunlight degrades performance.
- **FHSS (Frequency Hopping Spread Spectrum)**: Use 79 channels, each 1 MHz wide, starting at the low end of the unlicensed 2.4-GHz ISM band. Support data rates of 1 or 2 Mbps. In effect, frames are sent at different frequencies each time. Low bandwidth, but good resistance against security attacks, multipath fading, and interference from other devices. Popular for building-to-building links.
- **DSSS (Direct Sequence Spread Spectrum)**: Similar to CDMA, restricted to 1-2 Mbps.
- **OFDM (Orthogonal Frequency Division Multiplexing)**: High speed wireless LANs. Can reach 54 Mbps in the wider 5-GHz ISM band. Split a wide band into many narrow bands (52 frequencies, 48 for data and 4 for synchronization). Good spectrum efficiency and good immunity to multipath fading.
- **HR-DSSS (High Rate DSSS)**: Support data rates of 1, 2, 5.5, and 11 Mbps in the 2.4-GHz band.

4.4.3 The 802.11 MAC Sublayer Protocol

- **Two problems**: **hidden station problem** and **exposed station problem**; due to the fact that not all stations are within radio range of each other.
- **Solutions**: **DCF** (Distributed Coordination Function) and **PCF** (Point Coordination Function).

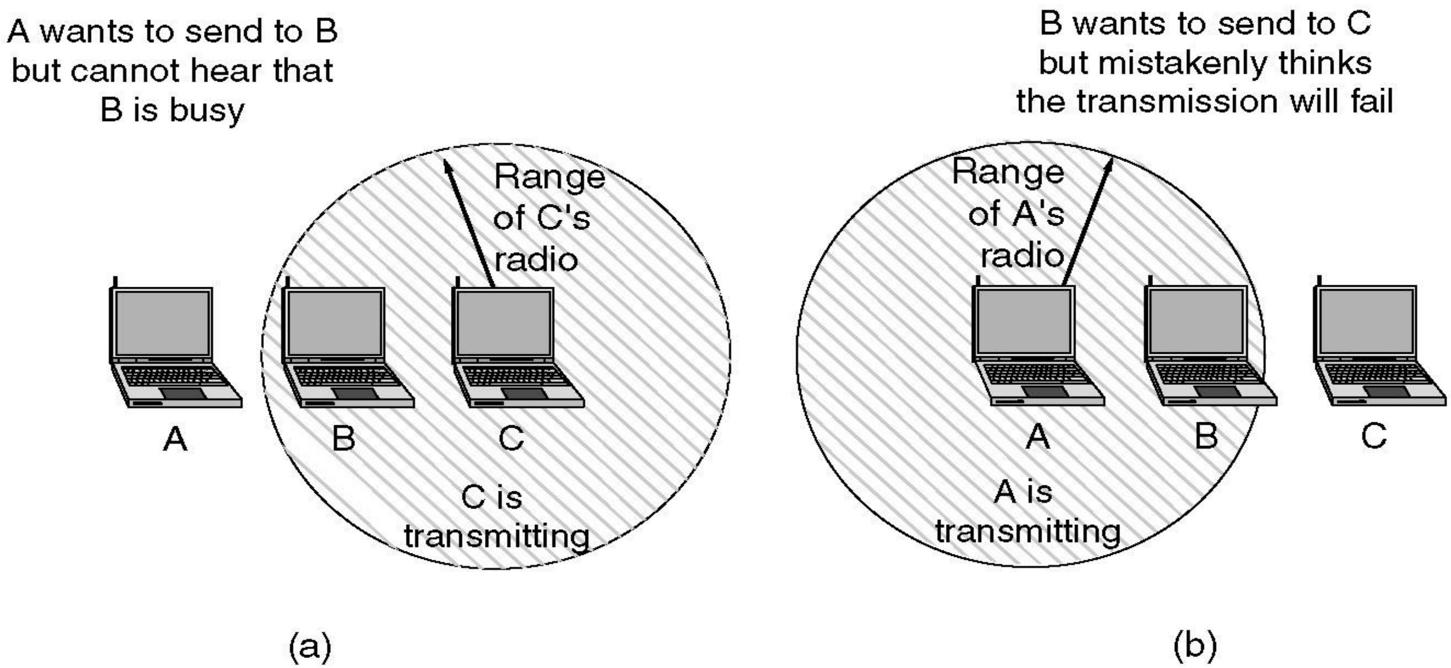

Fig. 4.19: (a) The hidden station problem. (b) The exposed station problem.

DCF

- **DCF**: **no central control**; supported by **all implementations**; use a protocol called **CSMA/CA** (CSMA with Collision Avoidance).
- **Two operation methods**:
  - Sense the channel and send only if it's free. Don't sense the channel during transmission. If a collision occurred, wait a random time and try again later.
  - **MACAW** (Multiple Access with Collision Avoidance for Wireless): Sender transmits RequestToSend (RTS) frame. Receiver replies with ClearToSend (CTS) frame. RTS and CTS announce the duration of the transfer. Nodes overhearing RTS/CTS keep quiet for that duration.

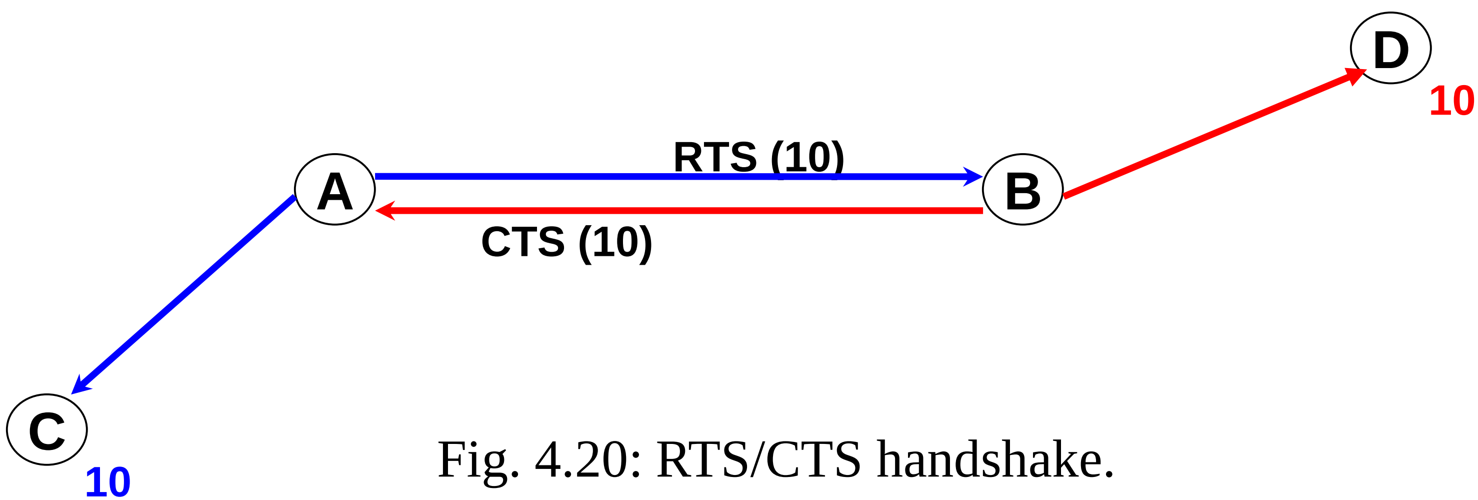

Fig. 4.20: RTS/CTS handshake.

MACAW

- Receiver sends **ACK** when has frame. Neighbors keep silent until see ACK.
- **NAV** (Network Allocation Vector): virtual channel; signals not transmitted, just for internal reminder to keep silent for a certain period.

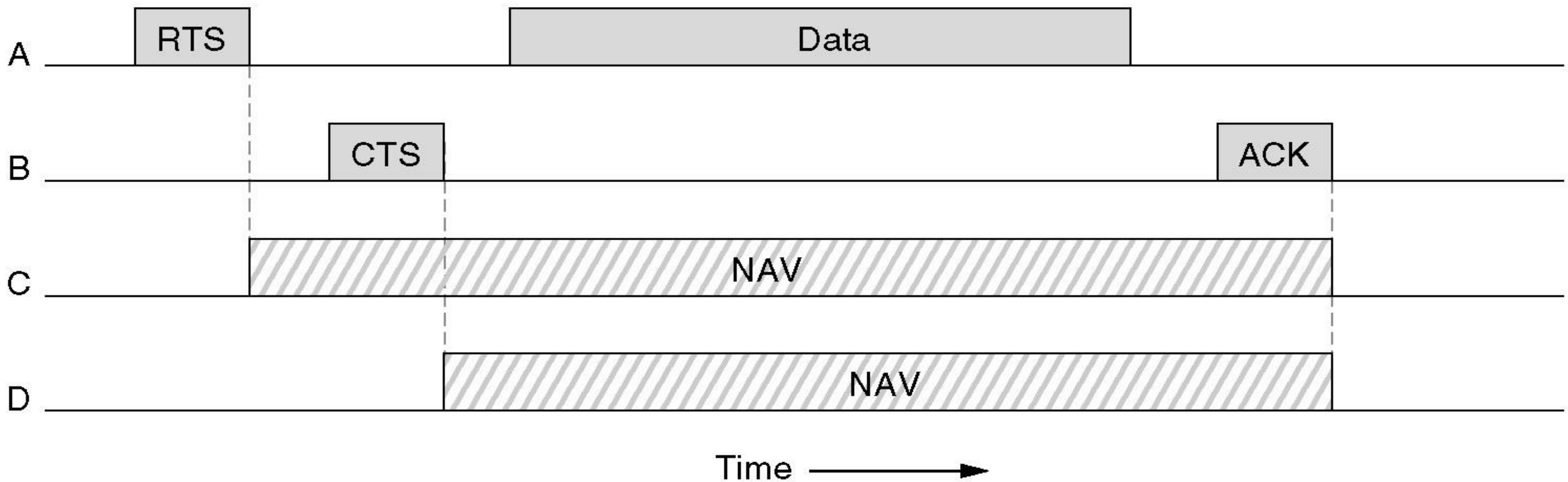

Fig. 4.21: The use of virtual channel sensing using CSMA/CA.

PCF

- **Optional** choice for 802.11.
- **Essence:** Let a single **base station** control all activities in its cell. **No collisions** at all!
- **Basic mechanism:** The base station broadcasts a **beacon frame** periodically (10 to 100 times per second). This frame contains system parameters, such as hopping frequencies and clock synchronization, and invites new stations to sign up for transmission.

4.4.4 The 802.11 Frame Structure

- **Duration:** Tells how long the transmission of this frame will take, allowing other stations to set their NAV accordingly.
- **Addresses:** Source/destination *in* a cell; and source/destination base stations *outside* the cell when dealing with intercell traffic.
- **Sequence:** allows fragments to be numbered. Uses 12 bits to identify the frame and 4 bits to identify the fragment.

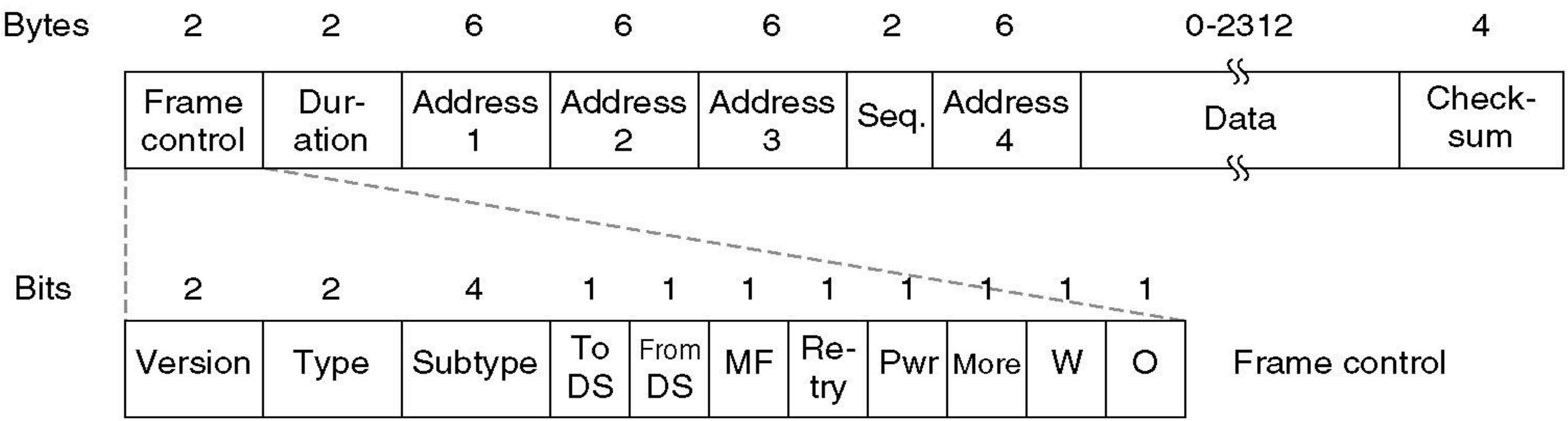

Fig. 4.22: The 802.11 data frame.

The 802.11 Frame Structure

- **Frame control field**: 11 subfields.
  - **Version**: which one of the two protocol versions.
  - **Type:** Data, control, or management frame.
  - **Subtype:** RTS, CTS, or ACK.
  - **DS (D**istribution **S**ystem**):** Is the frame entering/leaving the current cell?
  - **MF:** Frames are allowed to be fragmented to increase reliability. This bit tells whether **M**ore **F**ragments will follow.
  - **Retry:** Is this a retransmission?
  - **Power management:** Used by a base station to activate/passivate a station (important in view of power saving).
  - **More:** indicates that the sender has additional frames for the receiver.
  - **W:** The frame is encrypted using the Wired Equivalence Privacy algorithm.
  - **O:** Stick to ordered delivery of frames if this bit is **on**.

4.4.5 Services

- Each wireless LAN must provide **nine services**:
  - **Five distribution services**: provided by the base stations; deal with station mobility as they enter and leave cells; manage cell membership and interact with stations **outside the cell**.
    - **Association**: used by mobile stations to connect them to base stations.
    - **Disassociation**: used by mobile/base stations before breaking the relationship.
    - **Reassociation**: used by mobile stations to change its preferred base station.
    - **Distribution**: determines how to route frames sent to the base station.
    - **Integration**: handles the translation from the 802.11 frame format to a non-802.11 network frame format.
  - **Four station services**: **intracell**; related to actions within a single cell; used after association has taken place.
    - **Authentication**, **deauthentication**, **privacy**, and **data delivery**.

4.5 Broadband Wireless

- **Interchangeable terms:** 802.16, wireless MAN, or wireless local loop.
- **Goal:** Use wireless connection **between** buildings (e.g., avoiding the use of the local loop).
- **Comparison of 802.11 with 802.16 (Why devise a new standard?)**
  - Buildings do not move, so much of the mobility stuff from 802.11 is not needed.
  - Each cell has many more users than will a typical 802.11 cell; Need **more bandwidth**; **10-66 GHz** frequency range.
  - Broadband connections can be supported by **powerful radios** (money is less of a problem), making **power management** less of an issue.
  - We may need to cross **longer distances**, up to several kilometers.
  - ⇨ **802.11** was designed to be **mobile Ethernet**, whereas **802.16** was designed to be **wireless cable television**.

The 802.16 Protocol Stack

- **Physical medium dependent sublayer**: 3 modulation schemes.
- **Transmission convergence sublayer**: hide the different technologies from the data link layer.
- **Security sublayer**: more crucial for public outdoor networks.
- **Service specific convergence sublayer**: similar to LLC sublayer.

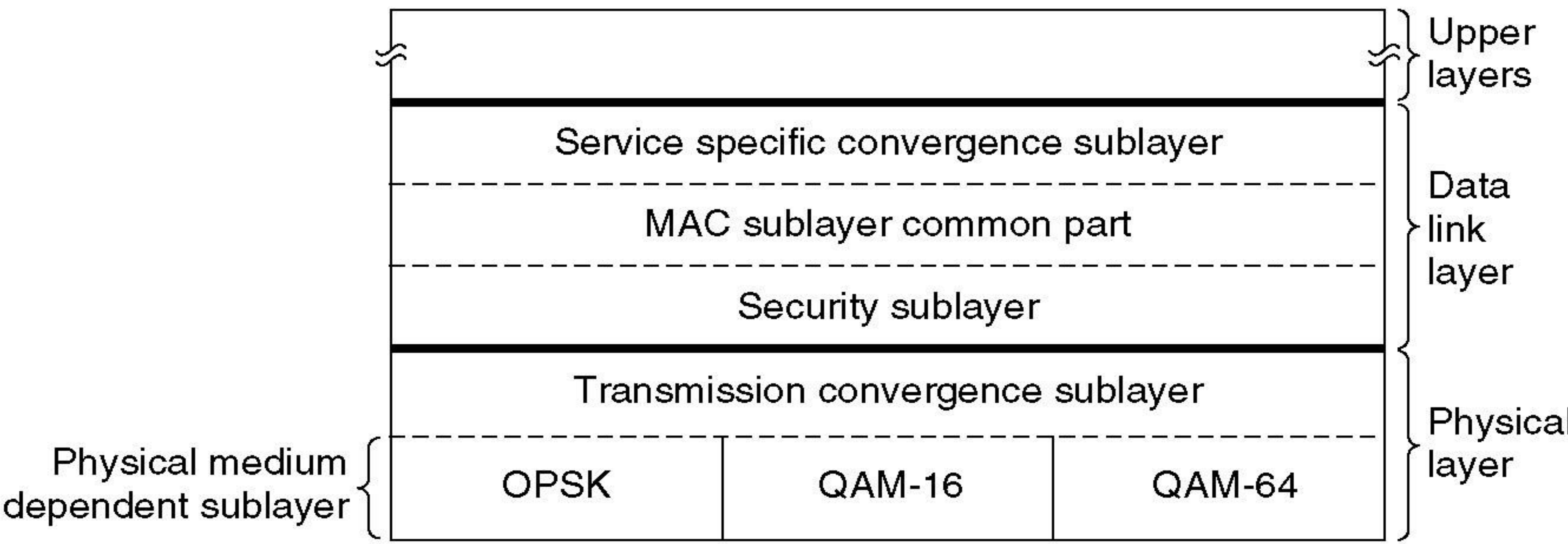

Fig. 4.23: The 802.16 protocol stack.

The 802.16 Physical Layer

- **Short range**: QAM-64, 6 bits/baud, 150 Mbps.
- **Medium range**: QAM-16, 4 bits/baud, 100 Mbps.
- **Long range**: QPSK, 2 bits/baud, 50 Mbps.
- The farther the subscriber is from the base station, the lower the date rate.

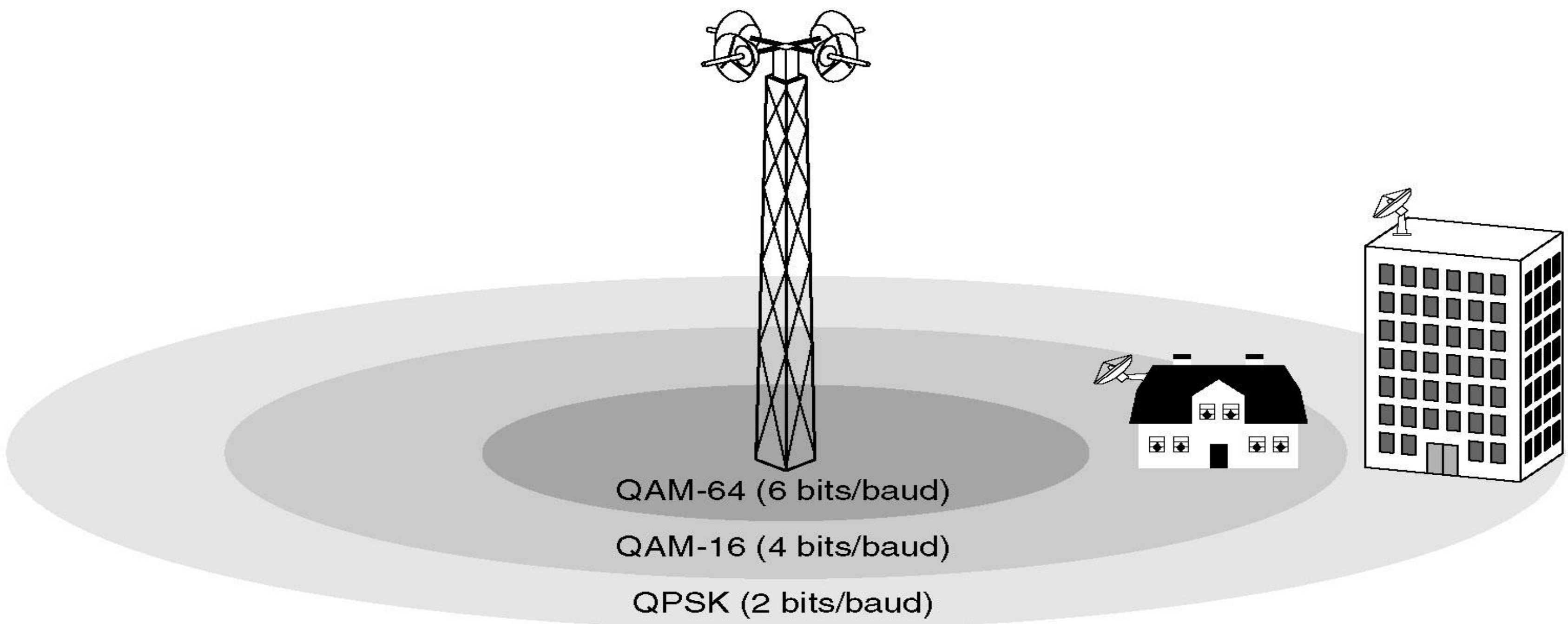

Fig. 4.24: The 802.16 transmission environment.

Summary

Method	Description
FDM	Dedicate a frequency band to each station
WDM	A dynamic FDM scheme for fiber
TDM	Dedicate a time slot to each station
Pure ALOHA	Unsynchronized transmission at any instant
Slotted ALOHA	Random transmission in well-defined time slots
1-persistent CSMA	Standard carrier sense multiple access
Nonpersistent CSMA	Random delay when channel is sensed busy
P-persistent CSMA	CSMA, but with a probability of p of persisting
CSMA/CD	CSMA, but abort on detecting a collision
Bit map	Round robin scheduling using a bit map
Binary countdown	Highest numbered ready station goes next
Tree walk	Reduced contention by selective enabling
MACA, MACAW	Wireless LAN protocols
Ethernet	CSMA/CD with binary exponential backoff
FHSS	Frequency hopping spread spectrum
DSSS	Direct sequence spread spectrum
CSMA/CA	Carrier sense multiple access with collision avoidance

Fig. 4.25: Channel allocation methods and systems for a common channel.