Chapter 11: Data Link Control

Outline

11.1 DLC SERVICES

11.2 DATA-LINK LAYER PROTOCOLS

11-1 DLC SERVICES

Recall that the data-link layer is divided into two sublayers: data link control (DLC) and media access control (MAC).

DLC deals with procedures for communication between two adjacent nodes, i.e., node-to-node communication, regardless whether the link is point-to-point or broadcast. DLC functions include framing and flow and error control.

MAC deals with procedures to handle access to a shared link (next chapter).

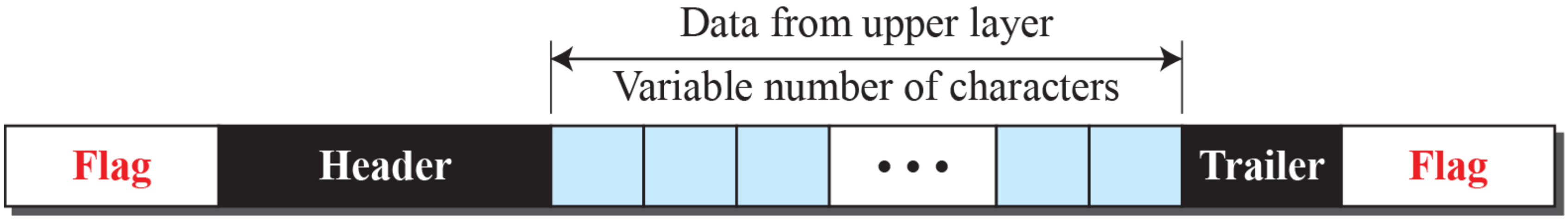
11.1.1 Framing

The data-link layer pack bits into frames, so that each frame is distinguishable from another. Framing (fixed-size or variable-size) separates messages from one source to a destination by adding a sender address and a destination address. The destination address defines where the packet is to go and the sender address helps the recipient acknowledge the receipt.

In variable-size framing, the end of one frame and the beginning of the next frame needs to be defined. We look at character-oriented framing and bit-oriented framing.

Figure 11.1: Character-Oriented Framing

In character-oriented framing, data to be carried are 8-bit characters from a coding system such as ASCII. To separate one frame from the next, an 8-bit (1 character) flag composed of protocol-dependent special characters is added at the beginning and the end of a frame to signal the start or end of a frame.



Character-oriented framing was popular when only text was exchanged by the data-link layers. However, for information types such as audio or video, any character used for the flag could also be part of the information.

Figure 11.2: *Byte stuffing and unstuffing*

A byte-stuffing (or character-stuffing) strategy was added to character-oriented framing: a special character (e.g., ESC) is added to the data portion of the frame when there is a character with the same pattern as the flag. Whenever the receiver encounters the special character, it removes it from the data portion and treats the next character as data.

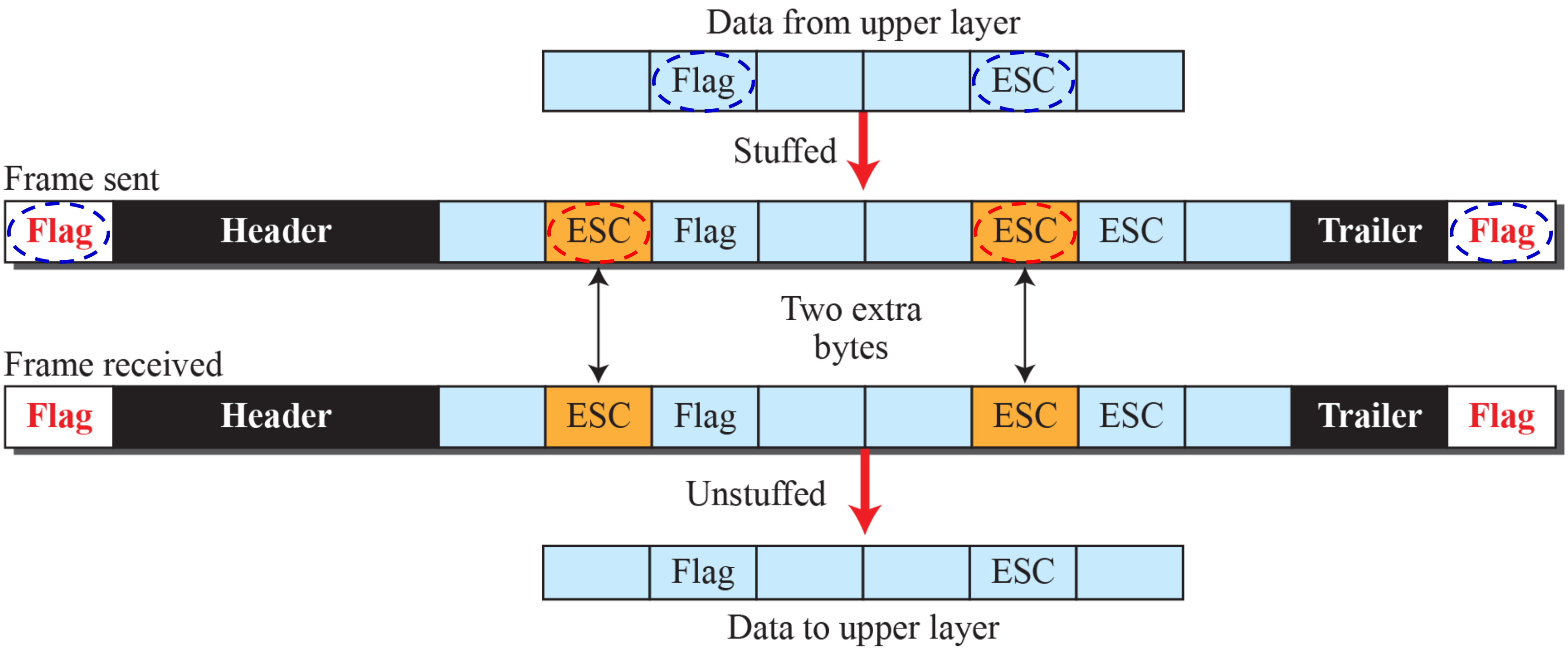


Figure 11.3: *A frame in a bit-oriented protocol*

However, universal coding systems, such as <u>Unicode</u>, have 16-bit and 32-bit characters that <u>conflict</u> with <u>8-bit characters</u> used in byte-stuffing, hence, the tendency is moving toward <u>bit-oriented framing</u>.

In bit-oriented framing, the <u>data</u> section of a frame is a <u>sequence of bits</u>. Most protocols use a special 8-bit pattern <u>flag</u>, e.g., 01111110, as a <u>delimiter</u> to define the beginning and end of the frame.

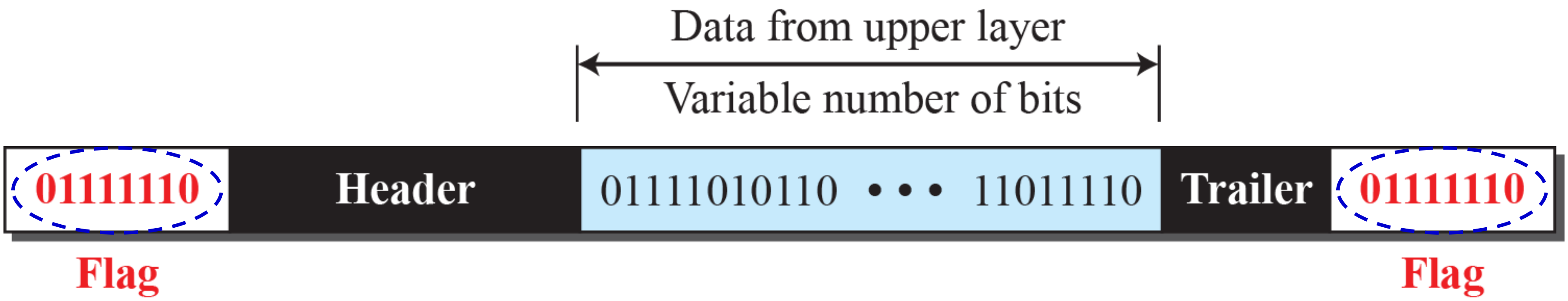
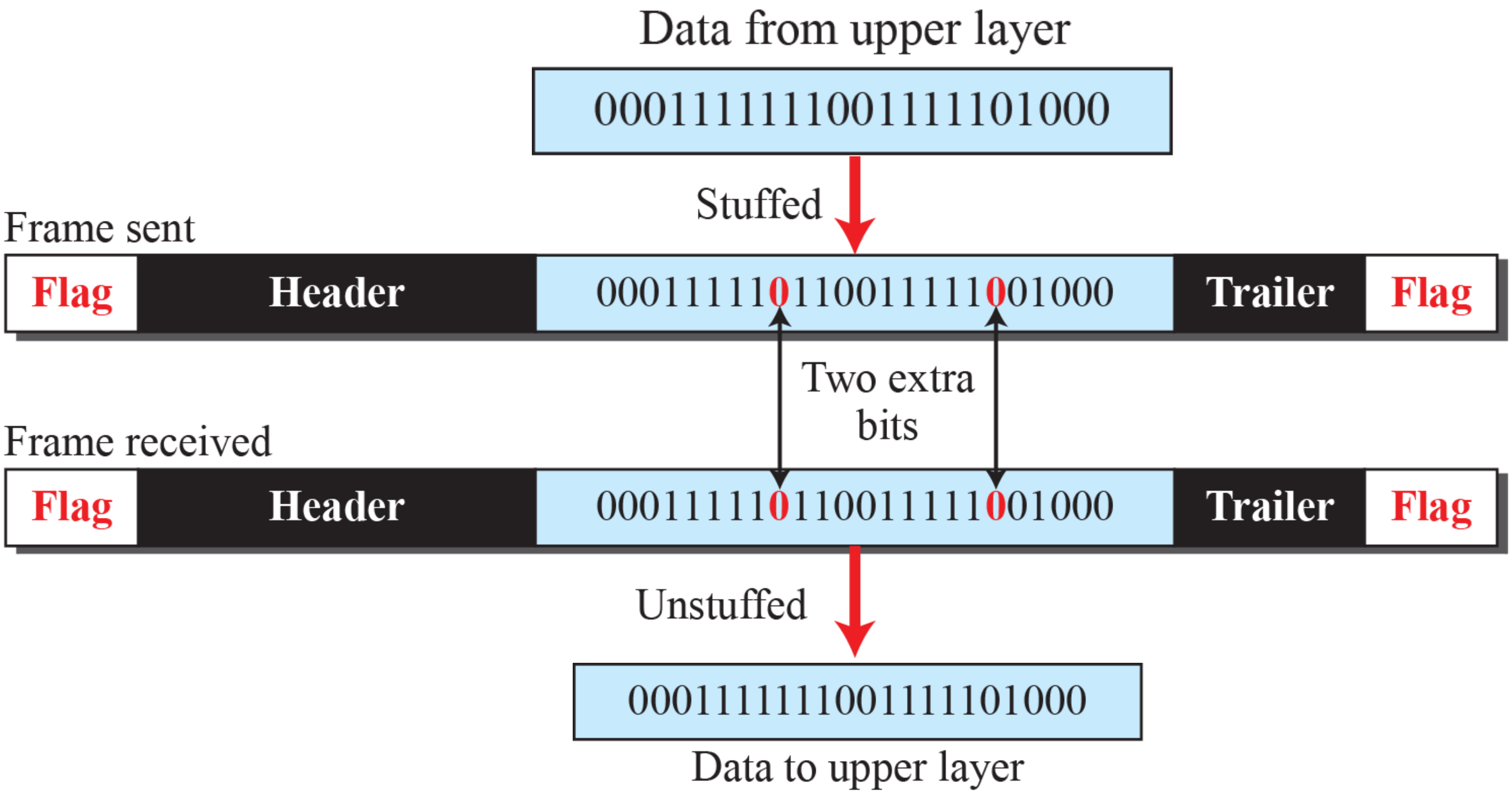


Figure 11.4: *Bit stuffing and unstuffing*

To prevent the issue where the flag pattern also appears in the data, bit stuffing adds a single bit to the data to prevent the data from looking like a flag, e.g., if the delimiter 01111110 is used, an extra 0 is added whenever five consecutive 1s follow a 0 in the data. Note that even if a 0 follows after five 1s, a 0 is still stuffed.



Data from upper layer

0001111111001111101000

Stuffed

Frame sent

Flag	Header	000111110110011111001000	Trailer	Flag

Two extra bits

Frame received

Flag	Header	000111110110011111001000	Trailer	Flag

Unstuffed

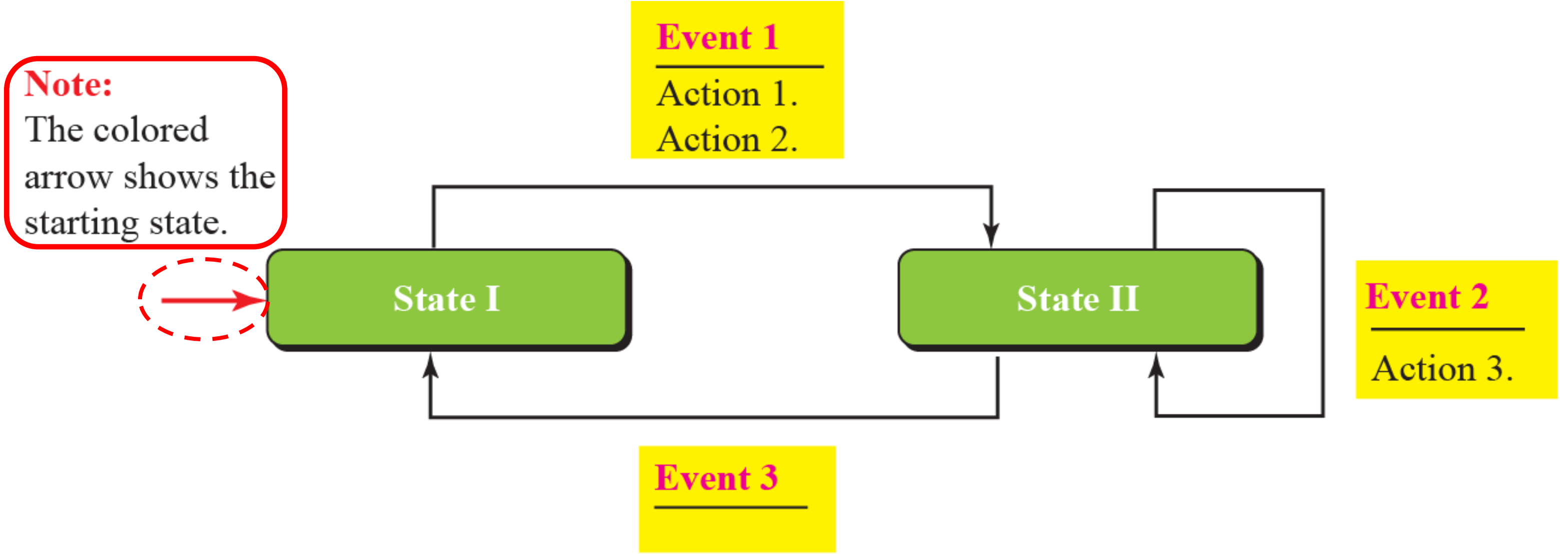
0001111111001111101000

Data to upper layer

11-2 DATA-LINK LAYER PROTOCOLS

The behavior of a data-link layer protocol can be shown as a finite state machine (FSM):

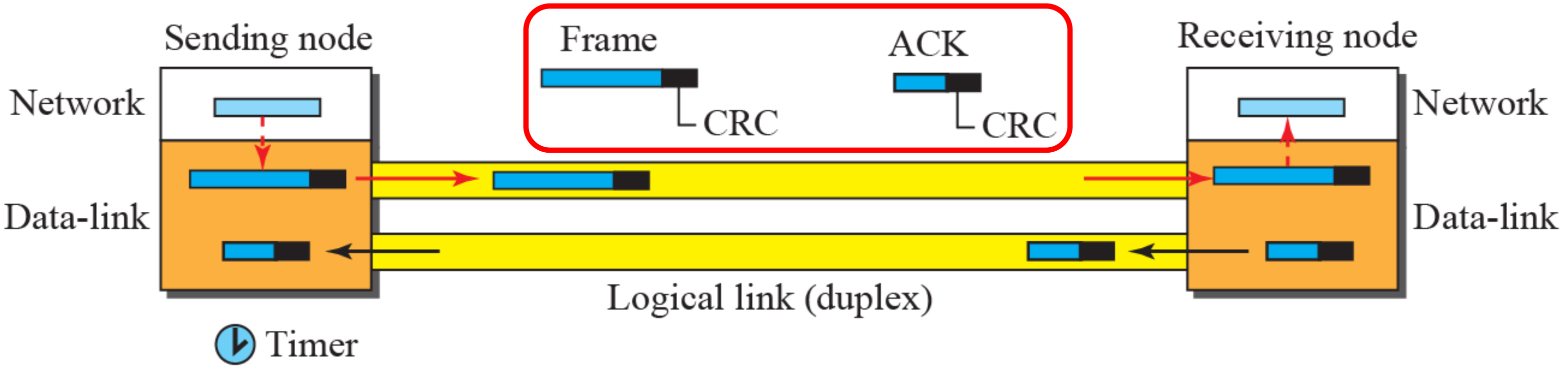
A FSM has a finite number of states and the machine is always in one of the states until an event occurs. One of the states must be defined as the initial state. Each event is associated with two reactions: (i) defining the list of actions to be performed and (ii) defining the next state.



11.2.2 Stop-and-Wait Protocol

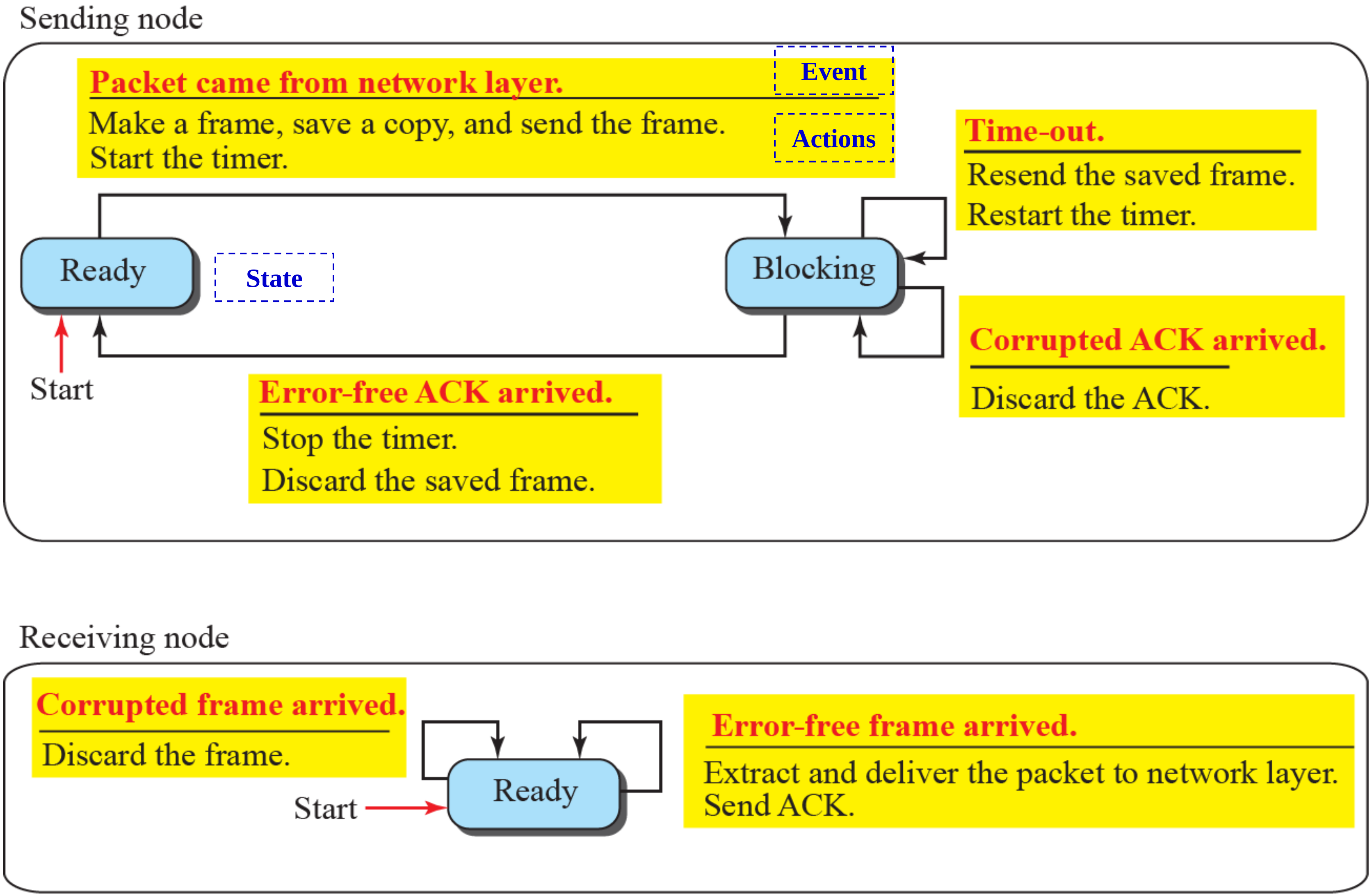
A DLC protocol that uses both flow and error control is called the Stop-and-Wait protocol.

In this protocol, the sender sends one frame at a time and waits for an acknowledgment before sending the next one. To detect corrupted frames, a CRC is added to each data frame. Every time the sender sends a frame, it starts a timer: if an acknowledgment arrives before the timer expires, it sends the next frame if it has one to send; if the timer expires, the sender resends the previous frame assuming that the frame was either lost or corrupted.



Note that only one frame and one acknowledgment can be in the channels at any time.

Figure 11.11: FSM for the Stop-and-Wait protocol



Sending node

Packet came from network layer.

Make a frame, save a copy, and send the frame.
Start the timer.

Event

Actions

Ready

State

Blocking

Start

Time-out.

Resend the saved frame.
Restart the timer.

Corrupted ACK arrived.

Discard the ACK.

Error-free ACK arrived.

Stop the timer.
Discard the saved frame.

Receiving node

Corrupted frame arrived.

Discard the frame.

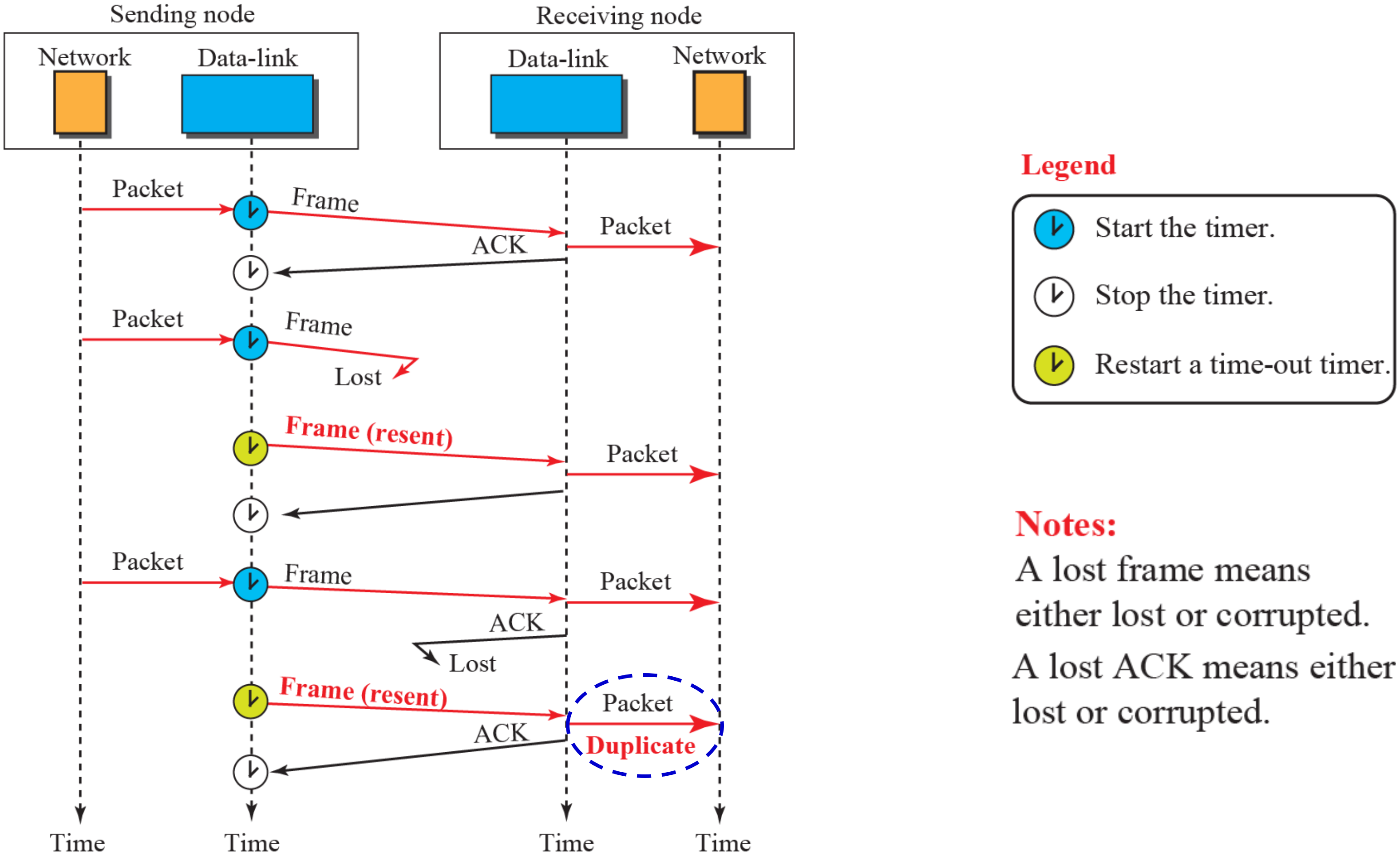
Start

Ready

Error-free frame arrived.

Extract and deliver the packet to network layer.
Send ACK.

Example



Notes:

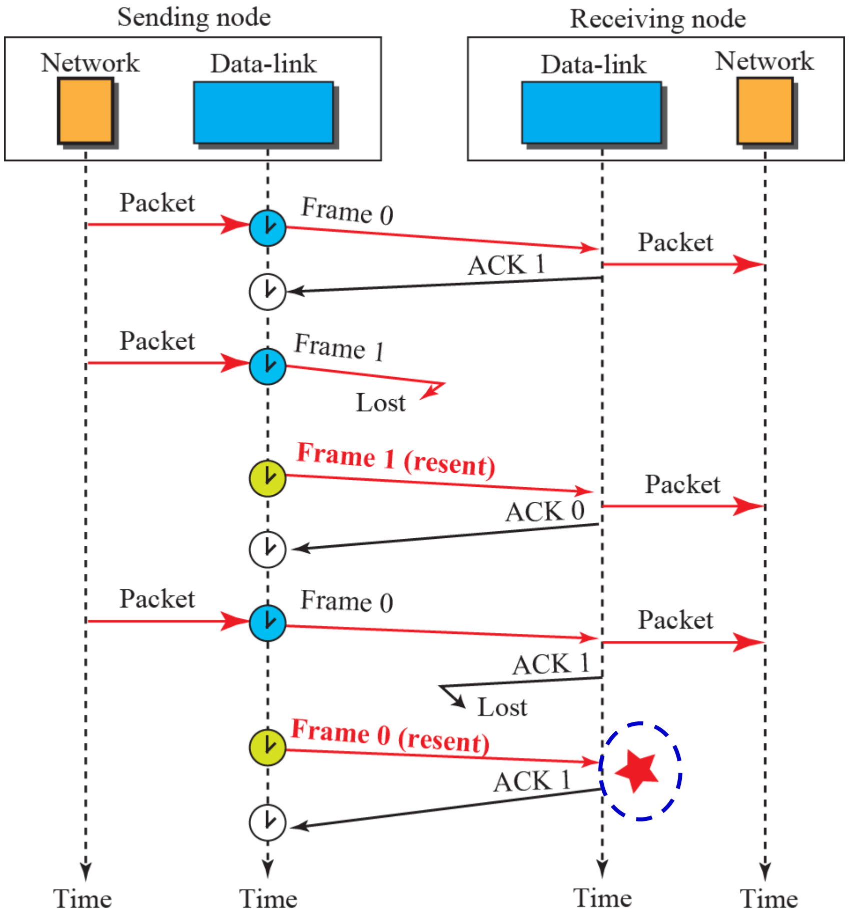
A lost frame means either lost or corrupted.

A lost ACK means either lost or corrupted.

The first frame is sent and acknowledged. The second frame is sent, but lost. After time-out, it is resent. The third frame is sent and acknowledged, but the acknowledgment is lost. The frame is resent. However, there is a problem with this scheme: the network layer at the receiving node received two copies of the third packet (a problem that needs to be corrected).

Example

Duplicate packets, as much as corrupted packets, need to be avoided. Adding sequence numbers and acknowledgment numbers can prevent duplicates.



Legend

● Start the timer.

○ Stop the timer.

● Restart a time-out timer.

Notes:

A lost frame means either lost or corrupted.

A lost ACK means either lost or corrupted.

★

Frame 0 is discarded because the receiver expects frame 1.

In this scheme, the sequence numbers start with 0 and the acknowledgment start with 1 (and alternate thereafter). The first frame is sent and acknowledged. The second frame is sent, but lost. After a time-out, it is resent. The third frame is sent and acknowledged, but the acknowledgment is lost. The frame is resent and acknowledged.

Chapter 12: Media Access Control

Outline

12.1 RANDOM ACCESS

12-1 RANDOM ACCESS

In random-access or contention methods, no station is superior to another station and none is assigned control over another. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision may depend on whether the state of the medium is idle or busy.

Two features give this method its name: (i) transmission is random among the stations and (ii) stations compete with one another to access the medium.

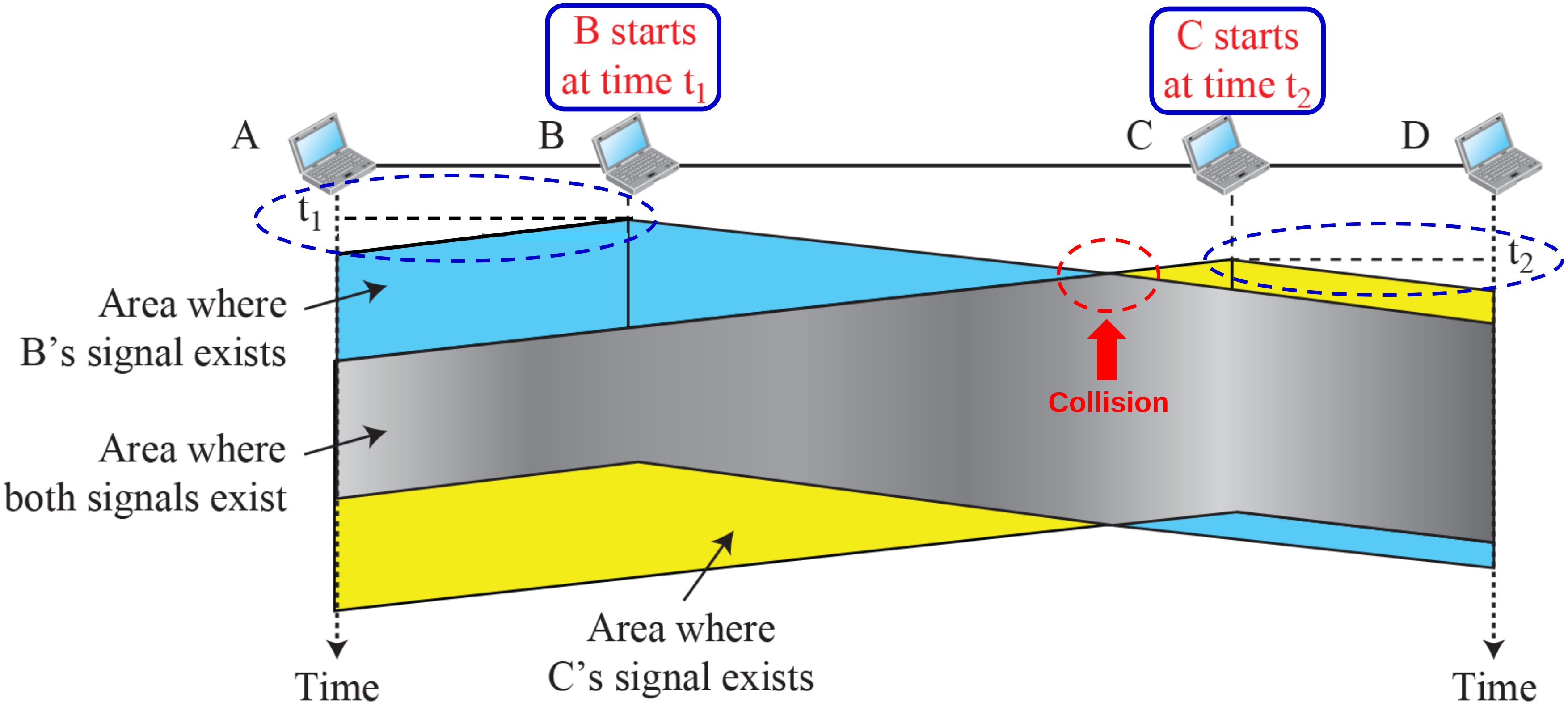
12.1.2 CSMA

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.

In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

Figure 12.7: Space/time model of a collision in CSMA

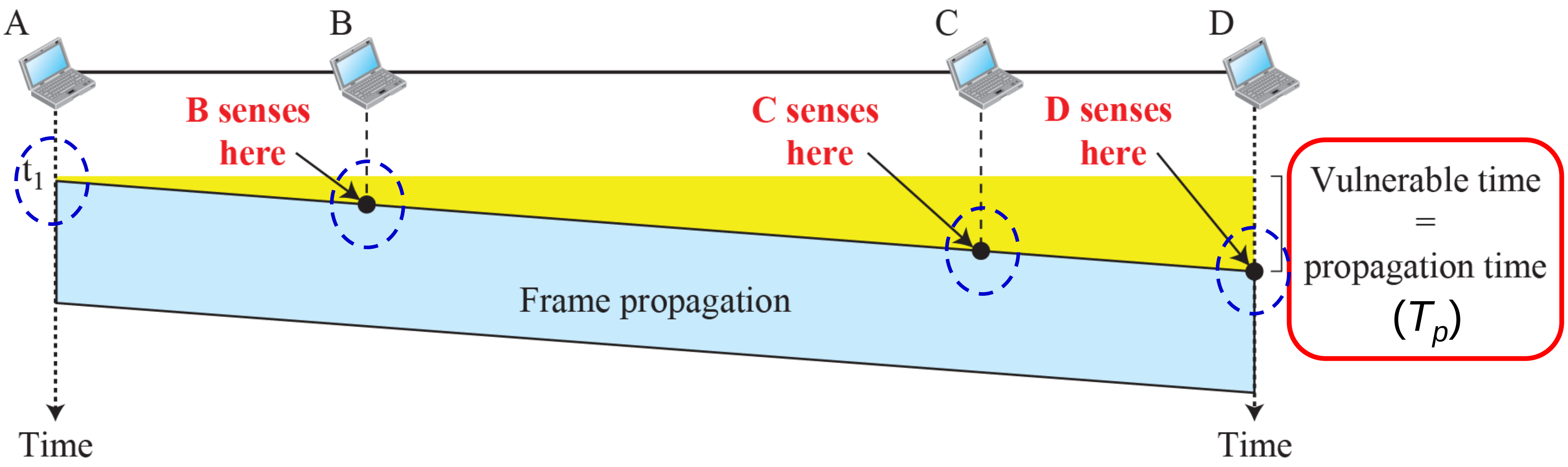
CSMA can reduce the possibility of collision, but it cannot eliminate it. The possibility of collision still exists because of propagation delay: when a station sends a frame, it still takes time for the first bit to reach every station and for every station to sense it.



B starts at time t_1
C starts at time t_2
A
B
C
D
t_1
t_2
Area where B's signal exists
Area where both signals exist
Collision
Area where C's signal exists
Time
Time

Figure 12.8: Vulnerable time in CSMA

The <u>vulnerable time</u> for CSMA is the maximum <u>propagation time</u>, T_p, the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame and any other station tries to send a frame during this time, a collision will result. However, if <u>the first bit of the frame reaches the end of the medium</u>, <u>every station will have heard the bit</u> and will <u>refrain from sending</u>.



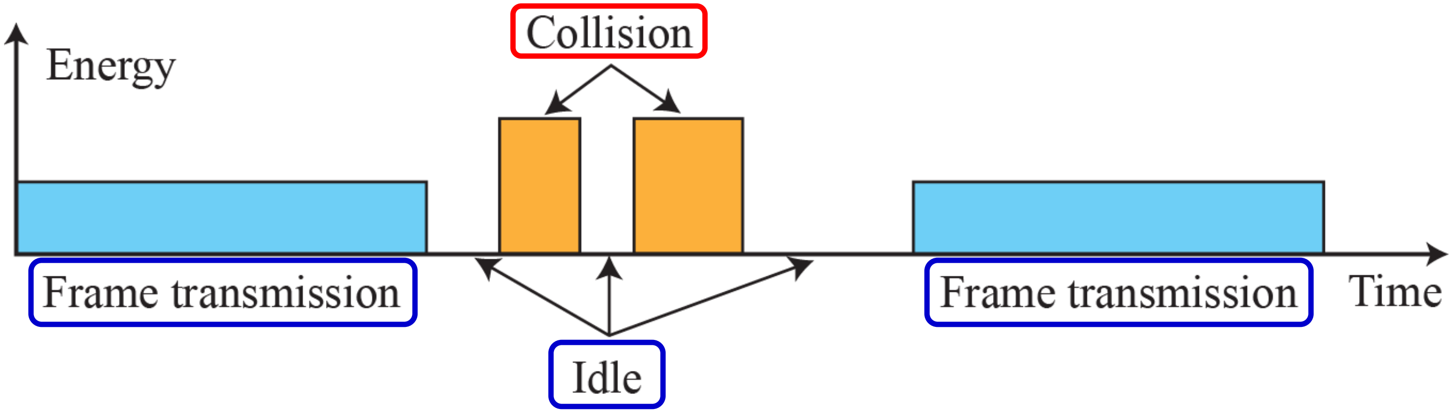
12.1.3 CSMA/CD

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If it was successful, the station is done. If, however, there was a collision, the frame is sent again.

Figure 12.14: *Energy level during transmission, idleness, or collision*

To understand CSMA/CD, let's see how a station monitors the energy level on the channel to determine if the channel is idle, busy or in collision mode. Depending on the energy level in the channel:



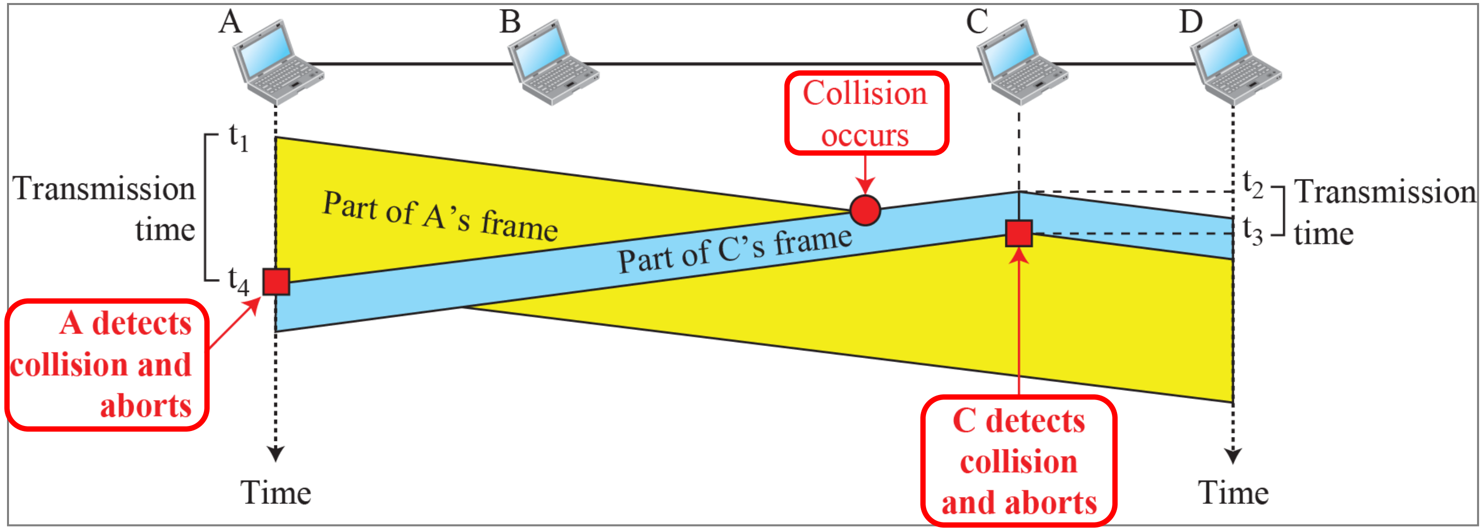
1) At zero level: channel is idle.

2) At normal level: channel is busy. A station has successfully captured the channel and is transmitting a frame.

3) At abnormal level: channel is in collision mode. There is a collision and the energy level is twice the normal level.

Figure 12.11: Collision and Abortion in CSMA/CD

In CSMA/CD, a station monitors the medium after it sends a frame to see if the transmission was successful. Let's look at the first bits transmitted by the two stations involved in the collision:



@t_1: A starts sending the bits of its frame.

@t_2: C has not yet sensed the first bit sent by A and starts sending the bits of its frame. A collision occurs sometime after t_2.

@t_3: C detects a collision and immediately aborts transmission.

@t_4: A detects a collision and immediately aborts transmission.

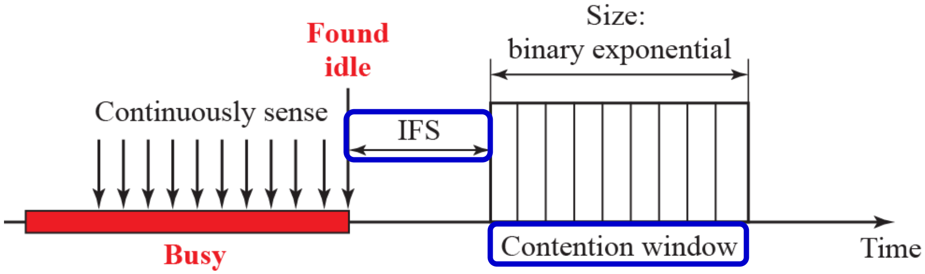
A transmits for duration (t_4 - t_1) and C transmits for duration (t_3 - t_2).

12.1.4 CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks. Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space (IFS), the contention window and acknowledgments along with Ready to Send (RTS) and Clear to Send (CTS) frames:

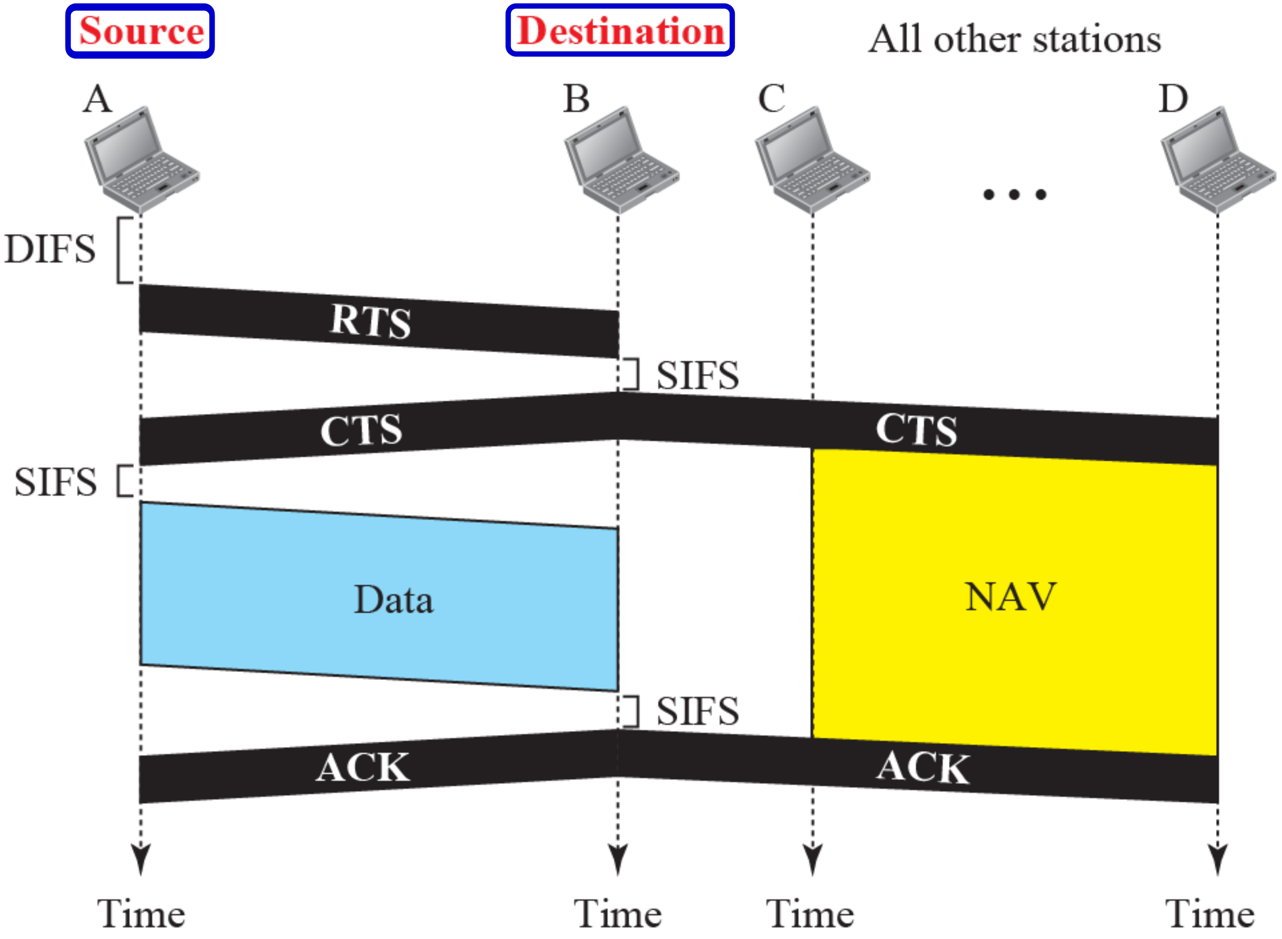
Interframe Space: Collisions are avoided by deferring transmission even if the channel is idle. It waits for a IFS period of time as the channel may appear idle even though a distant station may have started transmission.

Contention Window: A station that is ready to send chooses a random (binary exponential) number of slots as its wait time.



Acknowledgment: The use of positive acknowledgment and time-out timers helps guarantee that the receiver has received the frame.

Figure 12.17: CSMA/CA and NAV



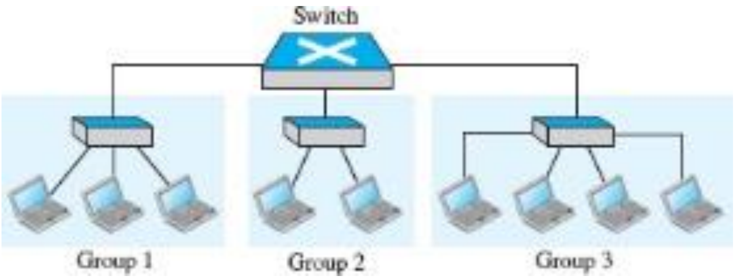
DIFS: Distributed Coordination Function (DCF) Interframe Space

SIFS: Short Interframe Space

NAV: Network Allocation Vector - When a station sends a RTS frame, it includes the duration of the time it needs to occupy the channel. The stations that are affected by this transmission create a NAV timer that shows how much time must pass before these stations are allowed to check the channel for idleness.

6-2 VIRTUAL LANs

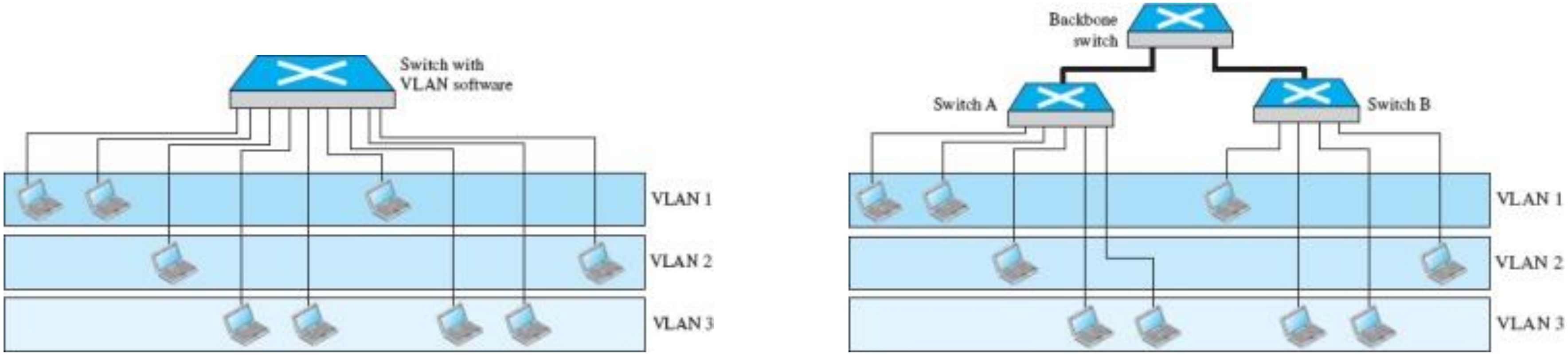
A station is considered part of a local area network (LAN) if it physically belongs to that LAN. The criterion of membership is geographic.



What would happen if the administrator needed to move two stations from Group 1 to Group 3?

Figure 6.10: *A switch connecting three LANs*

A virtual local area network (VLAN) is a local area network configured by software, not by physical wiring.



These figures show the same switched LAN divided into VLANs. The idea of VLAN technology is to divide a LAN into logical, instead of physical, segments.

Each VLAN is a work group in the organization and any station can be logically moved to another VLAN.

6.2.1 Membership

What characteristic can be used to group stations together in a VLAN?

Interface Numbers: Some VLAN vendors use switch interface numbers as a membership characteristic.
(e.g., stations connecting to ports 1 and 3 belong to VLAN 1; stations connecting to ports 4 and 10 belong to VLAN 2)

MAC Addresses: Some VLAN vendors use the 48-bit MAC address as a membership characteristic.

Combination: Some VLAN vendors allow all these characteristics to be combined.

6.2.4 Advantages

There are several advantages to using VLANs.

Cost and Time Reduction: VLANs can reduce the migration cost of stations going from one group to another.

(Physical reconfiguration takes time and is costly, it is much easier and quicker to move it by software)

Creating Virtual Work Groups: VLANs can be used to create virtual work groups.

(e.g., in a campus environment, individuals working on the same project can send broadcast messages to one another without the necessity of belonging to the same department)

Security: VLANs provide an extra measure of security.

(Individuals belonging to the same group can send broadcast messages with the assurance that users in other groups will not receive these messages)