Chapter 14

Wireless LANs

14-1 IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Topics discussed in this section:

Architecture
MAC Sublayer
Physical Layer

Architecture

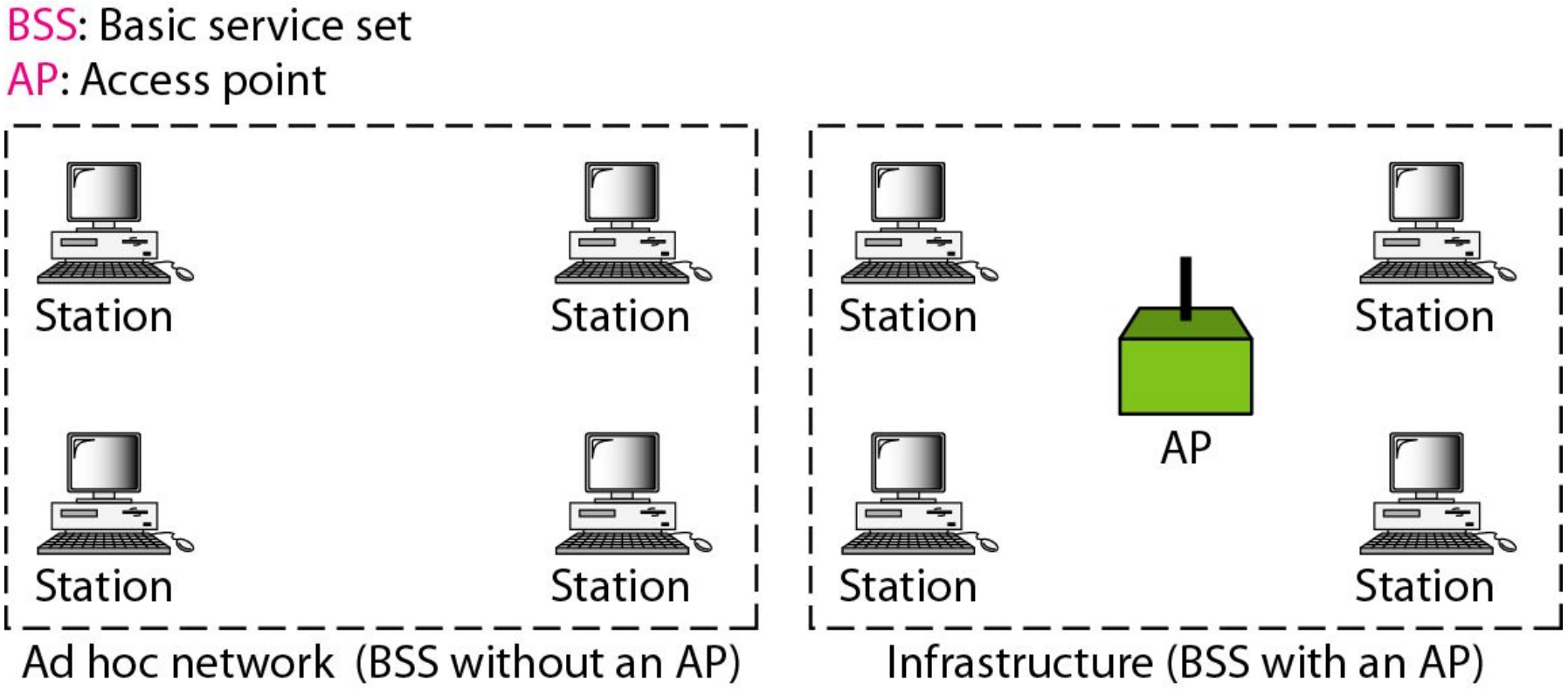
The standard defines two kinds of services:
Basic service set (BSS) ,and
Extended service set (ESS).

Note

A BSS without an AP is called an ad hoc network;
a BSS with an AP is called an infrastructure network.

A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
The **BSS without an AP** is a stand-alone network and cannot send data to other BSSs.It is called an *ad hoc architecture. In this architecture, stations can form a network* without the need of an AP; they can locate one another and agree to be part of a BSS.
A **BSS with an AP** is sometimes referred to as an *infrastructure network.*

Figure 14.1 *Basic service sets (BSSs)*



Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system, which is usually a wired* LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses **two types of stations: mobile and stationary**. The **mobile stations are normal stations inside a BSS**. The **stationary stations are AP stations** that are part of a wired LAN.

Figure 14.2 *Extended service sets (ESSs)*

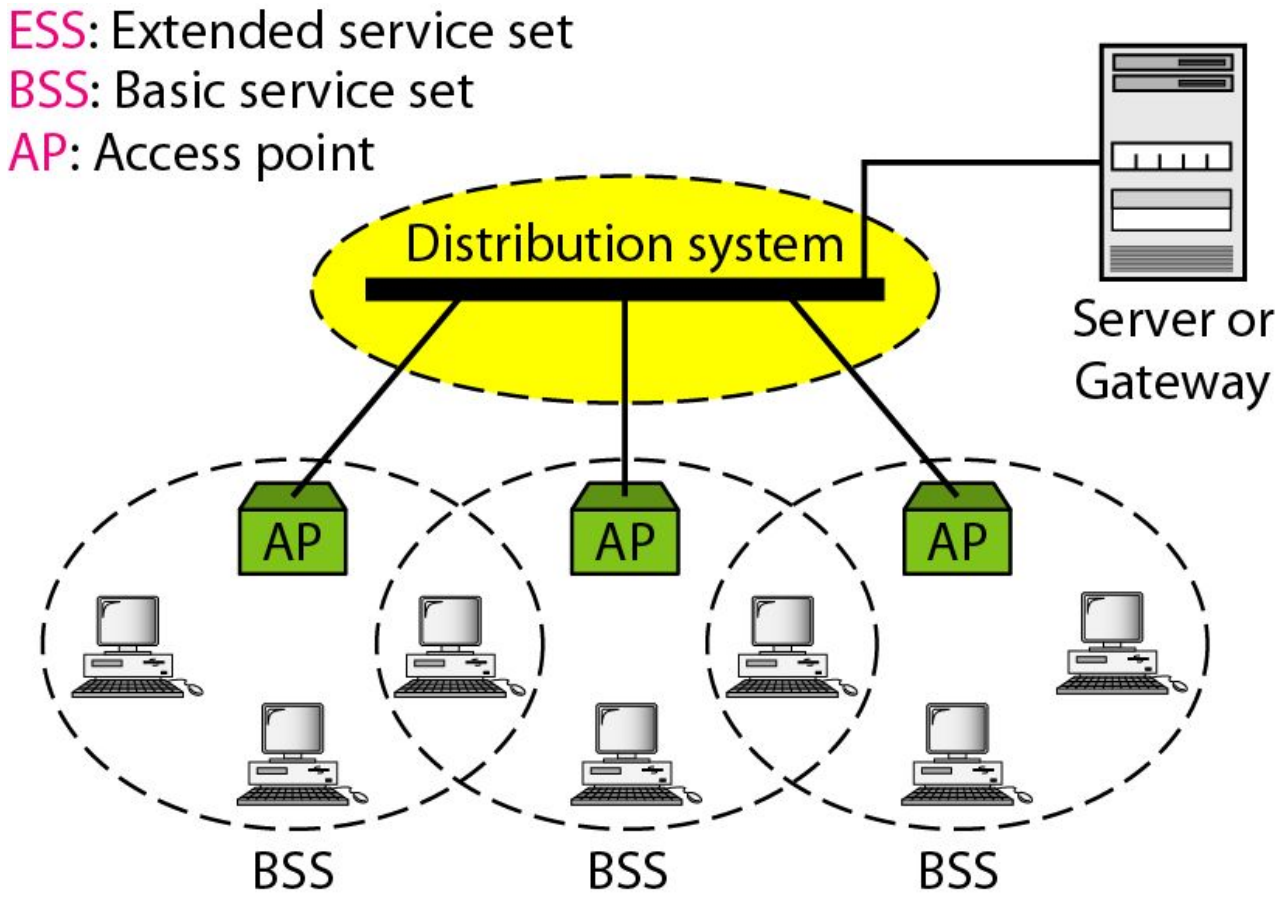
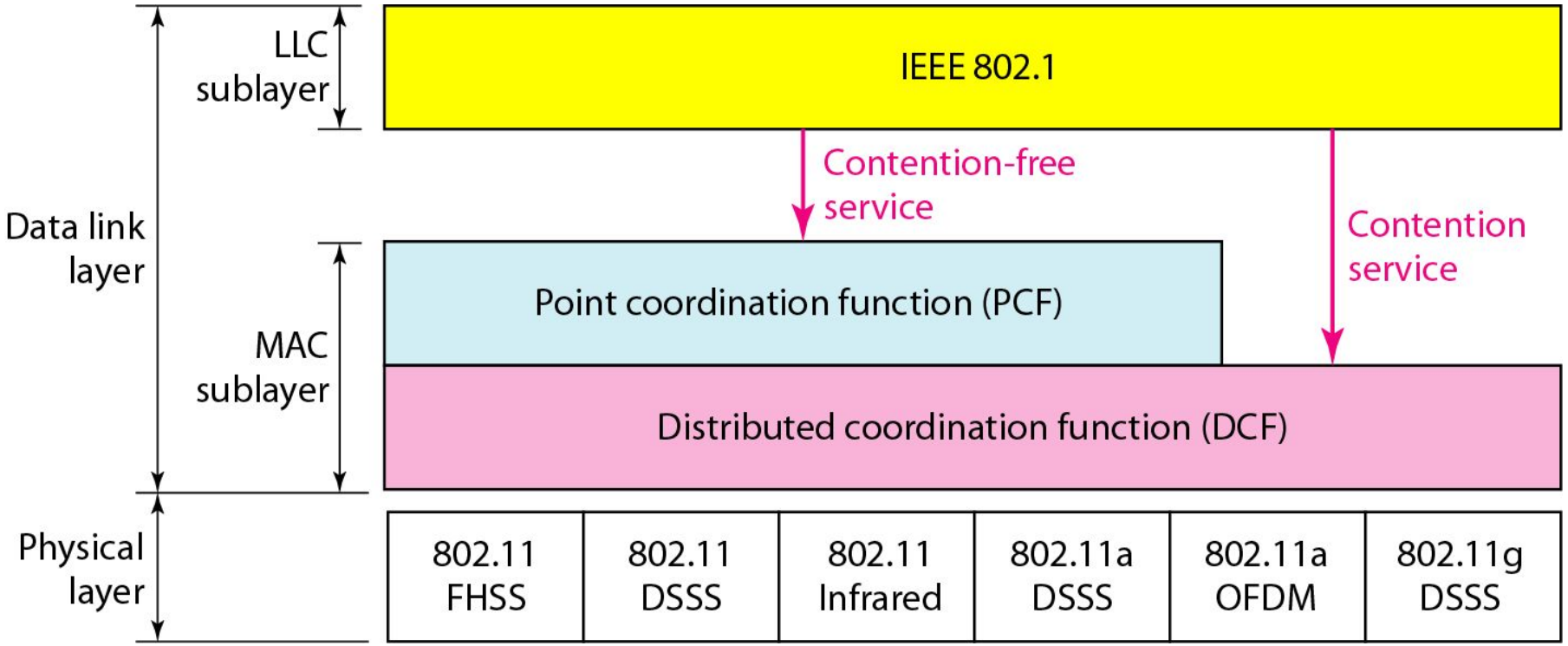


Figure 14.3 *MAC layers in IEEE 802.11 standard*



DCF uses *CSMA/CA as the* access method. Wireless LANs cannot implement *CSMA/CD for three reasons:*

I. For collision detection a station must be able to send data and receive collision signals at the same time. This can mean costly stations and increased bandwidth requirements.

2. Collision may not be detected because of the hidden station problem.

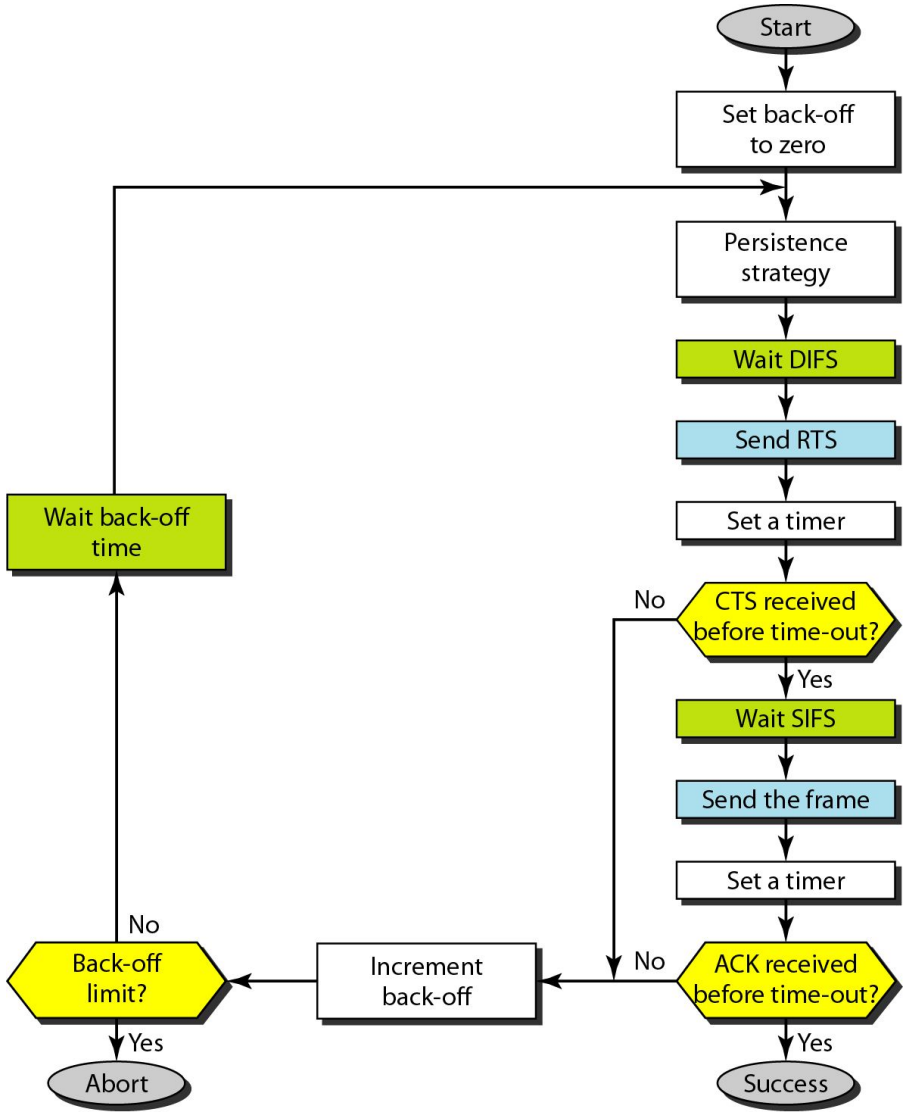
3. The distance between stations can be great. Signal fading could prevent a station at one end from hearing a collision at the other end.

Point Coordination Function (PCF)

The point coordination function (PCF) is an **optional access method** that can be **implemented in an infrastructure network (not in an ad hoc network).** It is implemented on top of the DCF and is used mostly for time-sensitive transmission.

PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

Figure 14.4 *CSMA/CA flowchart*



Network Allocation Vector (NAV)

When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel.

The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.

Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.

Figure 14.5 *CSMA/CA and NAV*

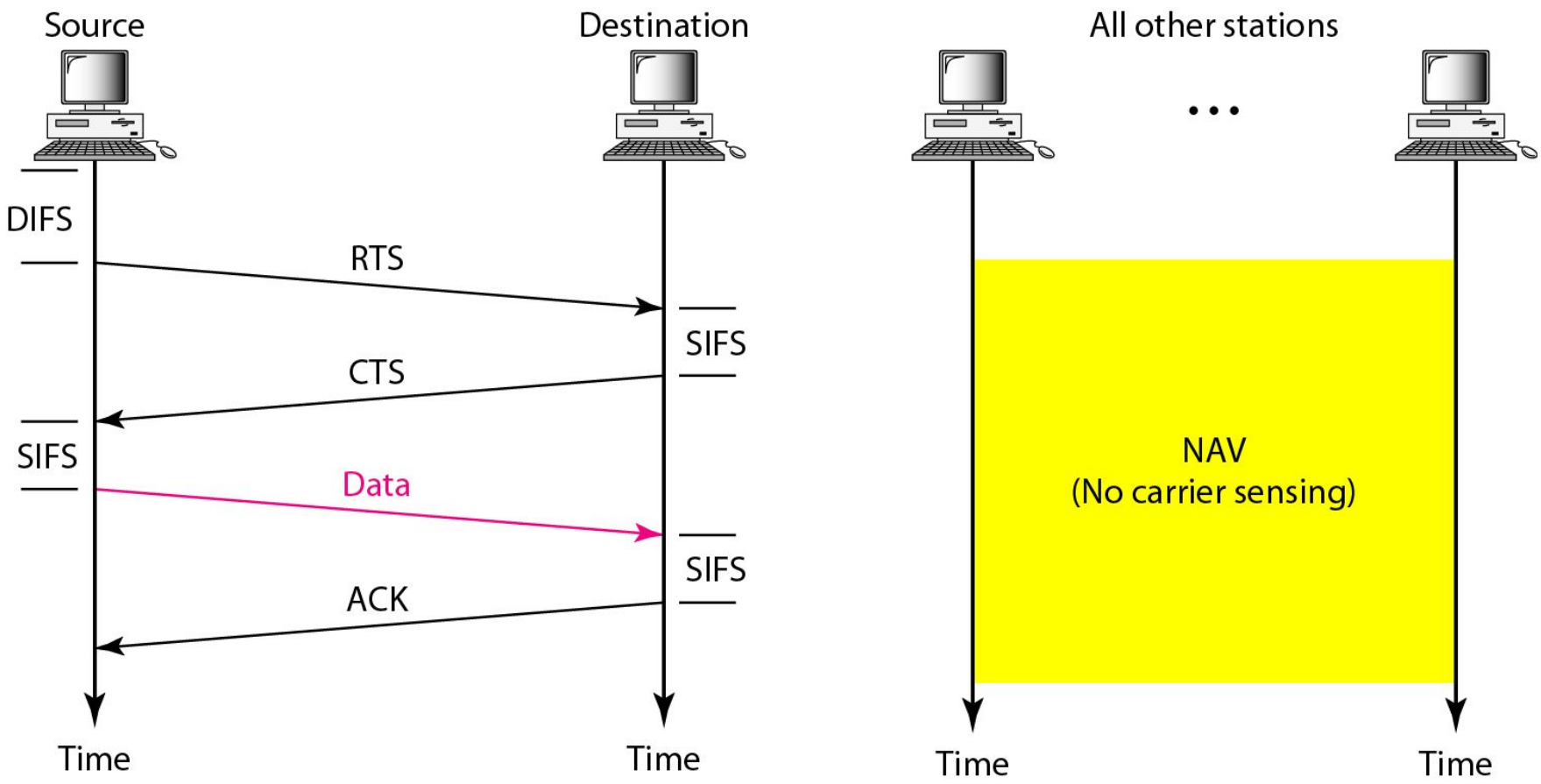


Figure 14.6 *Example of repetition interval*

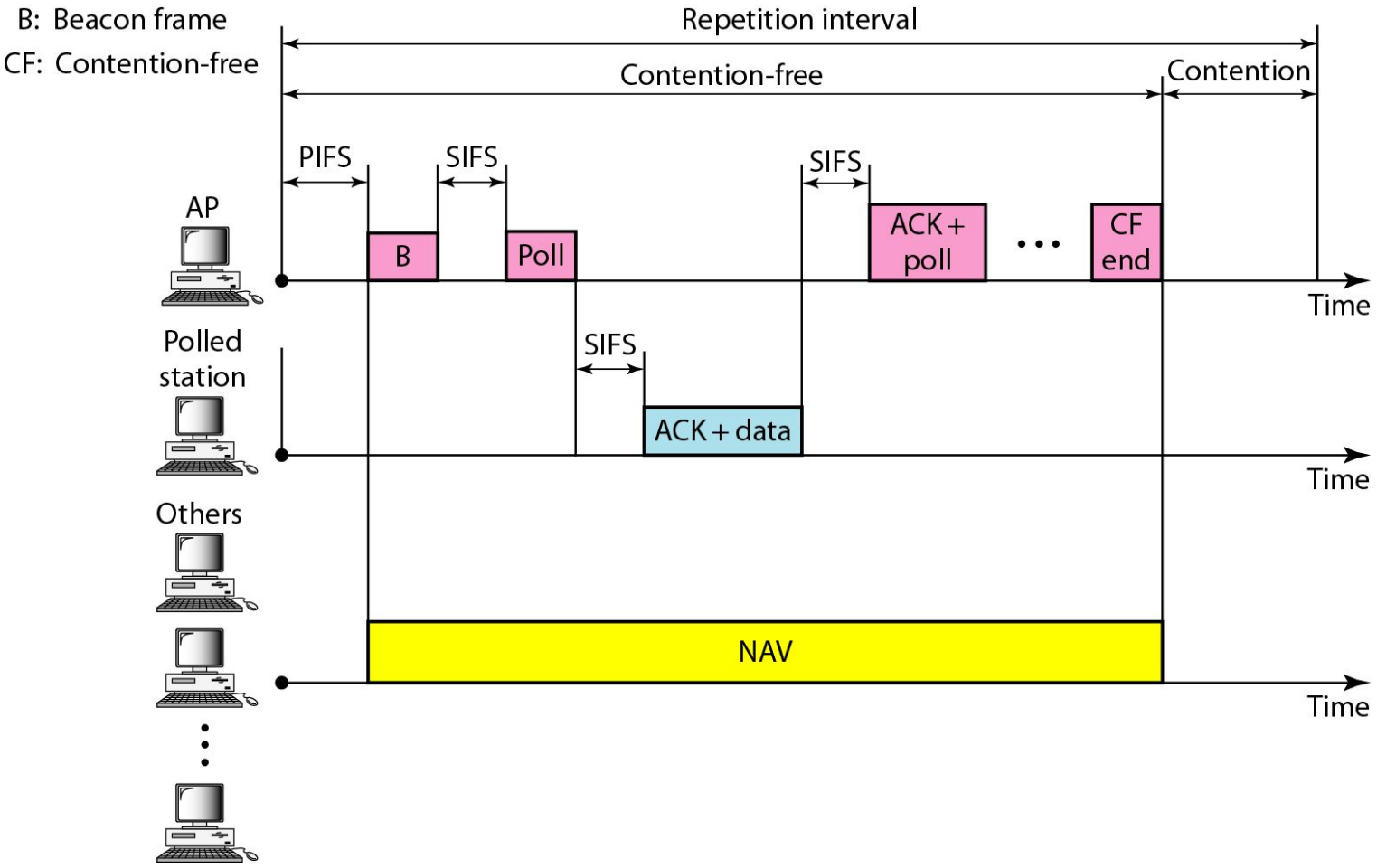
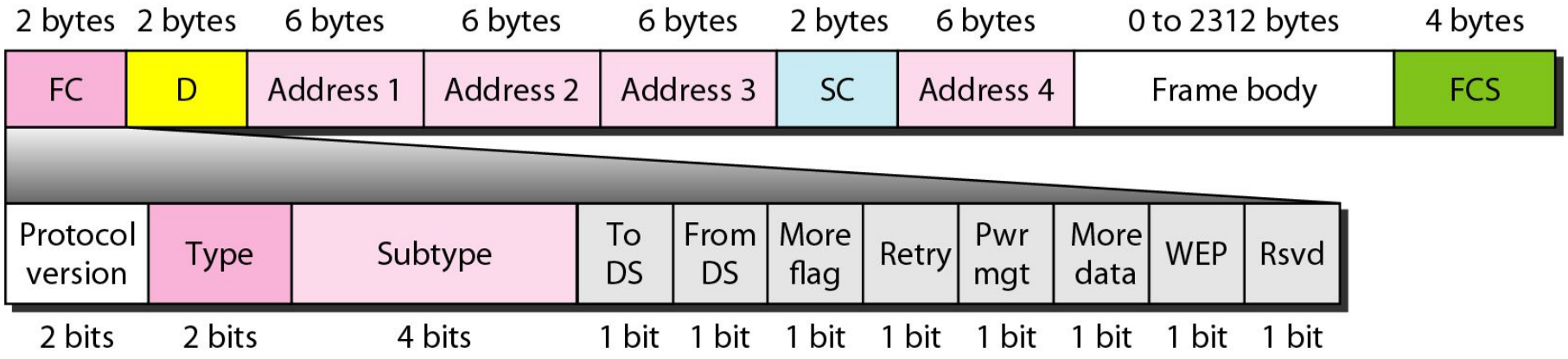


Figure 14.7 *Frame format*



FC: Frame Control
D:Duration of transmission
SC:Sequence control of frame

Table 14.1 *Subfields in FC field*

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

Frame Types

A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data frames.

Management Frames: Management frames are used for the initial communication between stations and access points.

Control Frames: Control frames are used for accessing the channel and acknowledging frames.

Data Frames: Data frames are used for carrying data and control information.

Figure 14.8 *Control frames*

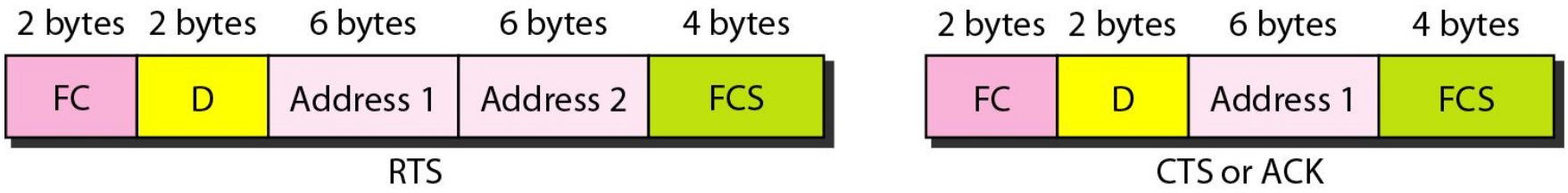


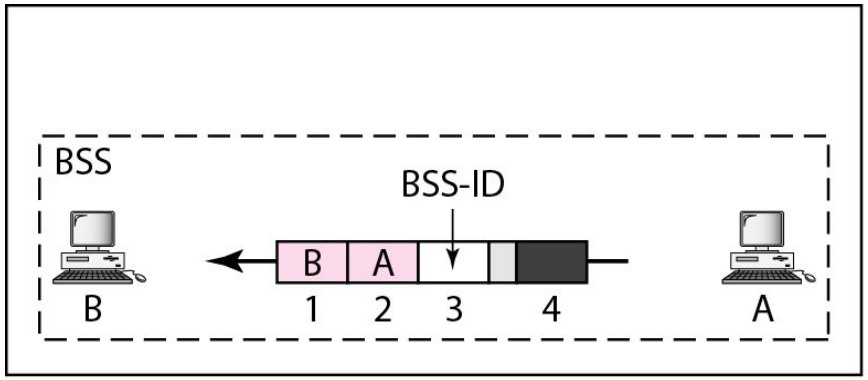
Table 14.2 *Values of subfields in control frames*

Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

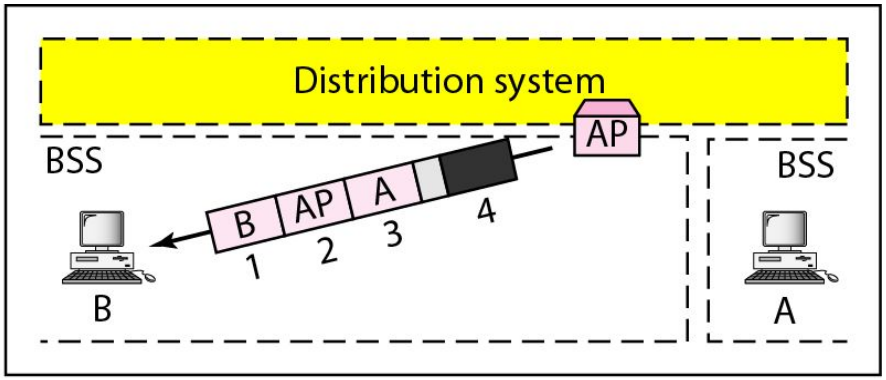
Table 14.3 *Addresses*

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

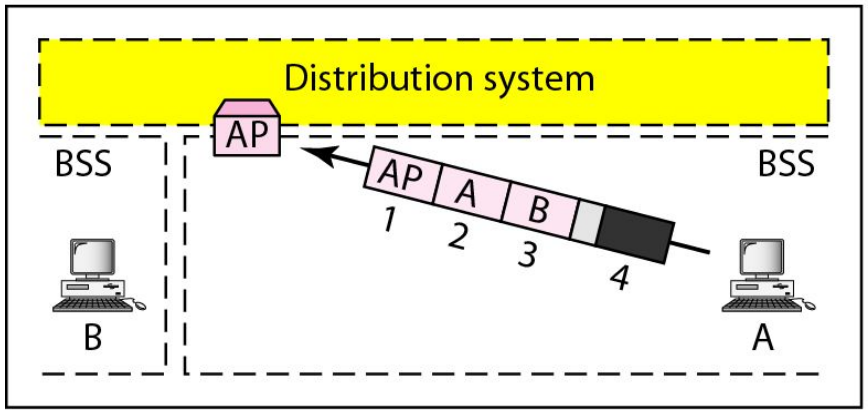
Figure 14.9 *Addressing mechanisms*



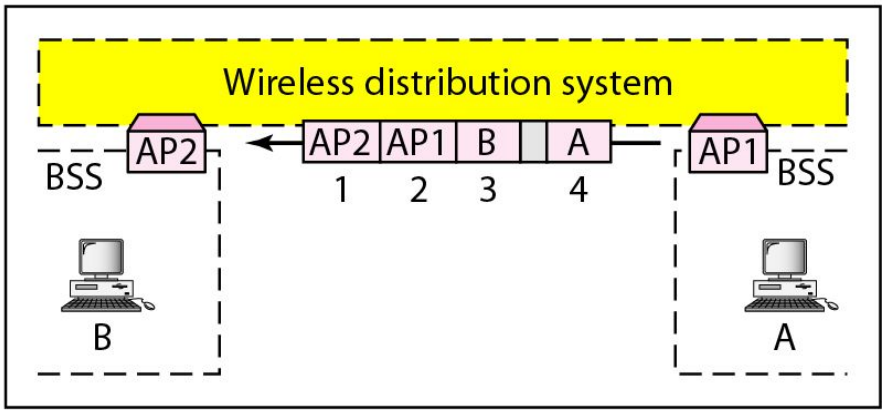
a. Case 1



b. Case 2

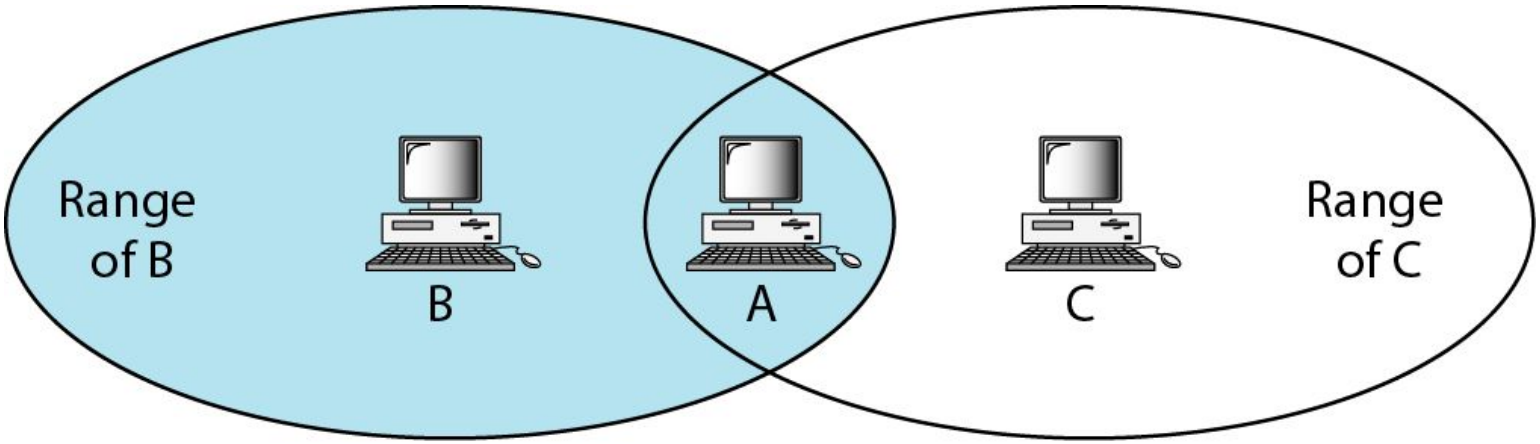


c. Case 3



d. Case 4

Figure 14.10 *Hidden station problem*



Note

The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

Figure 14.11 *Use of handshaking to prevent hidden station problem*

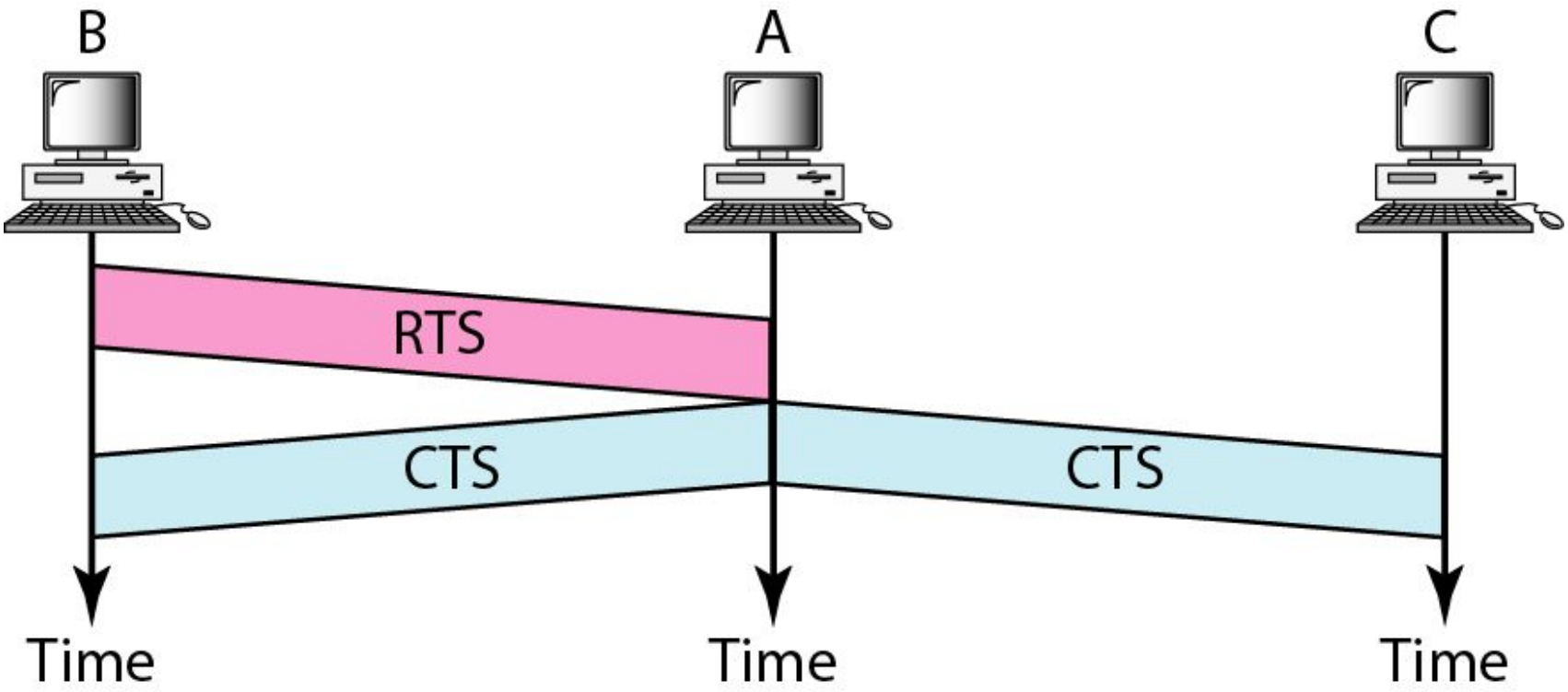


Figure 14.12 *Exposed station problem*

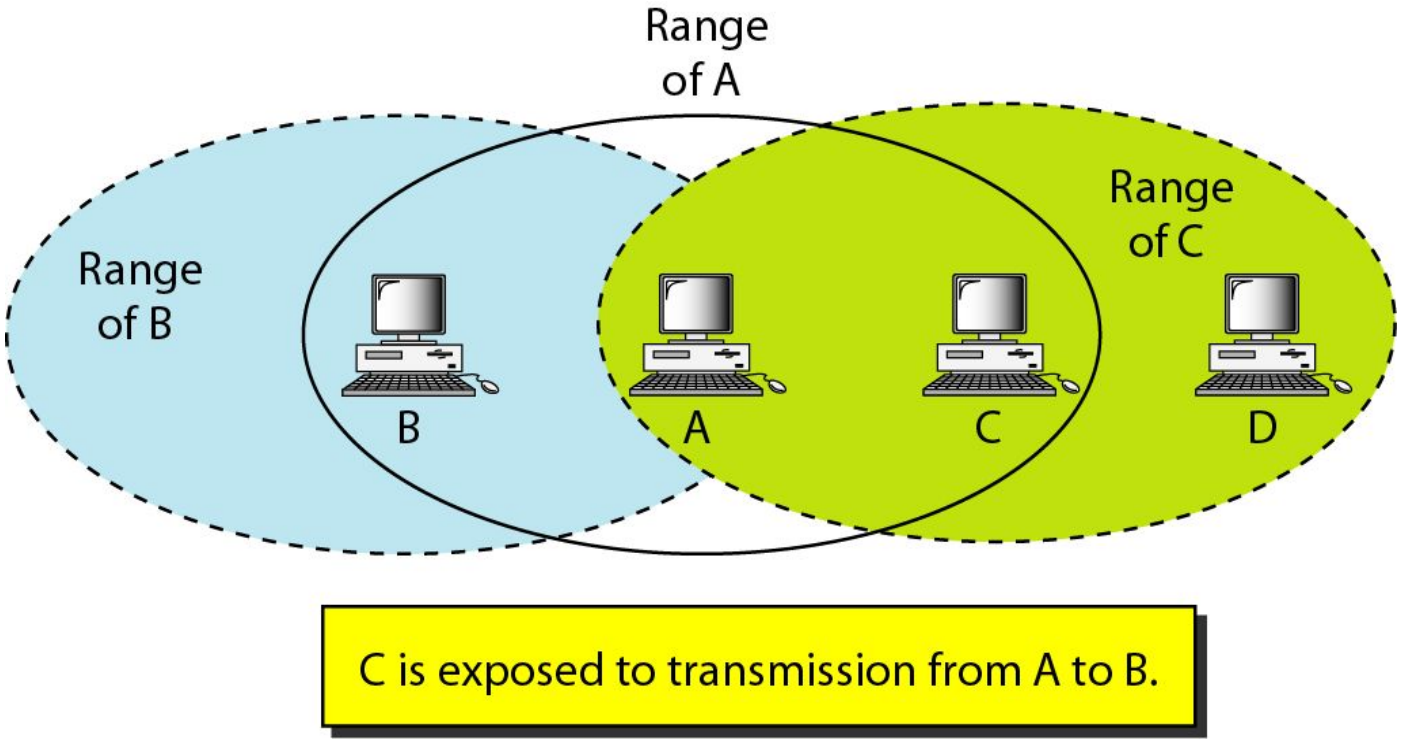


Figure 14.13 *Use of handshaking in exposed station problem*

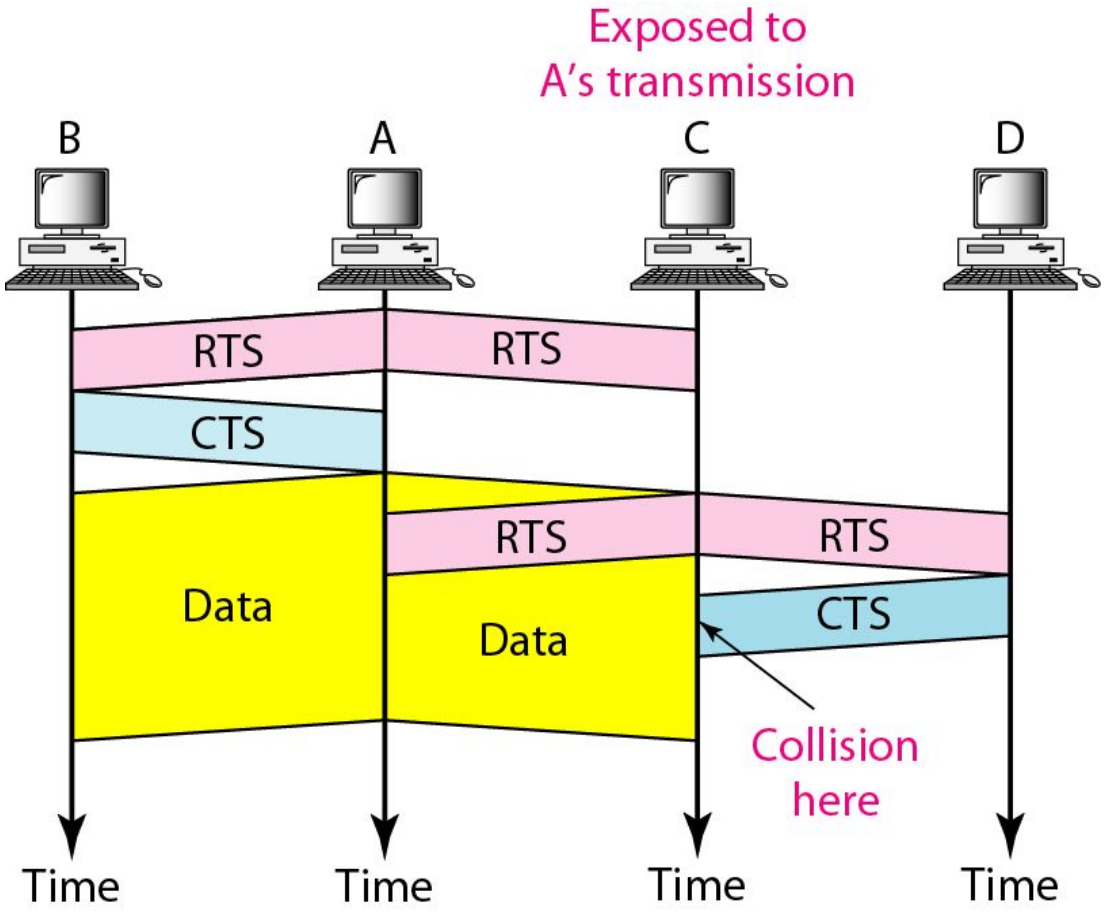


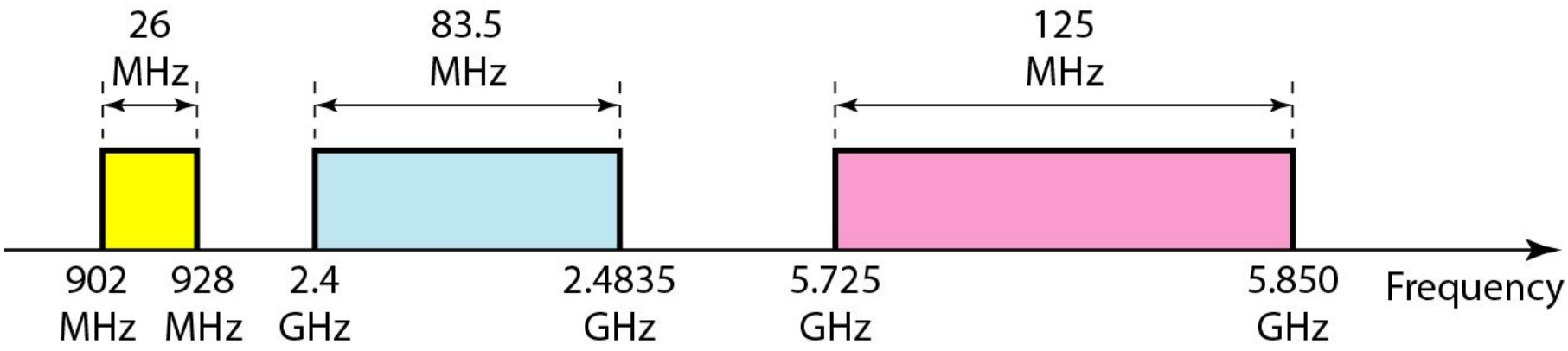
Table 14.4 *Physical layers*

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

All implementations, except the infrared, operate in the *industrial, scientific,* and *medical (ISM) band.*

direct sequence spread spectrum,

Figure 14.14 *Industrial, scientific, and medical (ISM) band*



14-2 BLUETOOTH

***Bluetooth** is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.*

Topics discussed in this section:

Architecture
Bluetooth Layers
Baseband Layer
L2CAP

Figure 14.19 *Piconet*

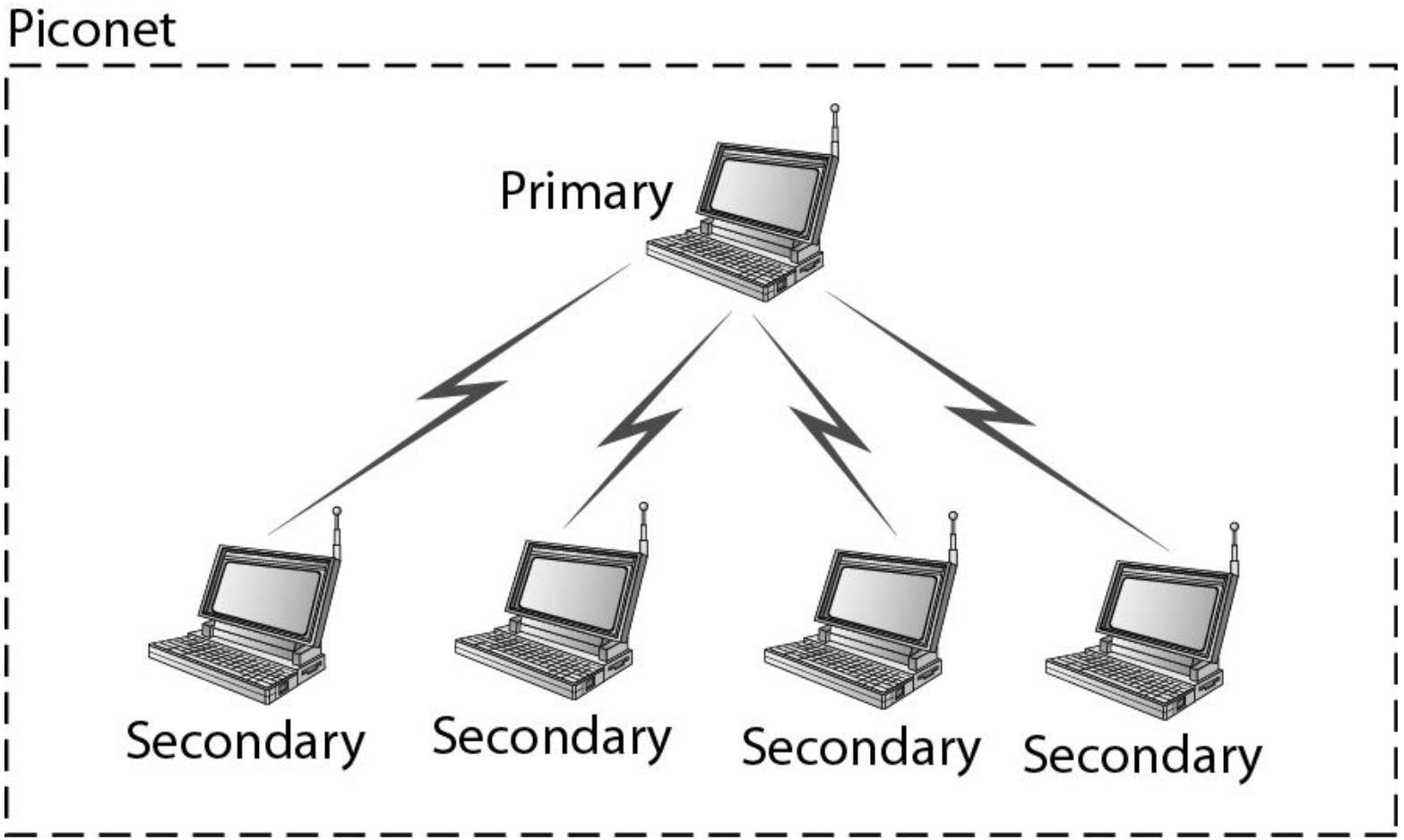


Figure 14.20 *Scatternet*

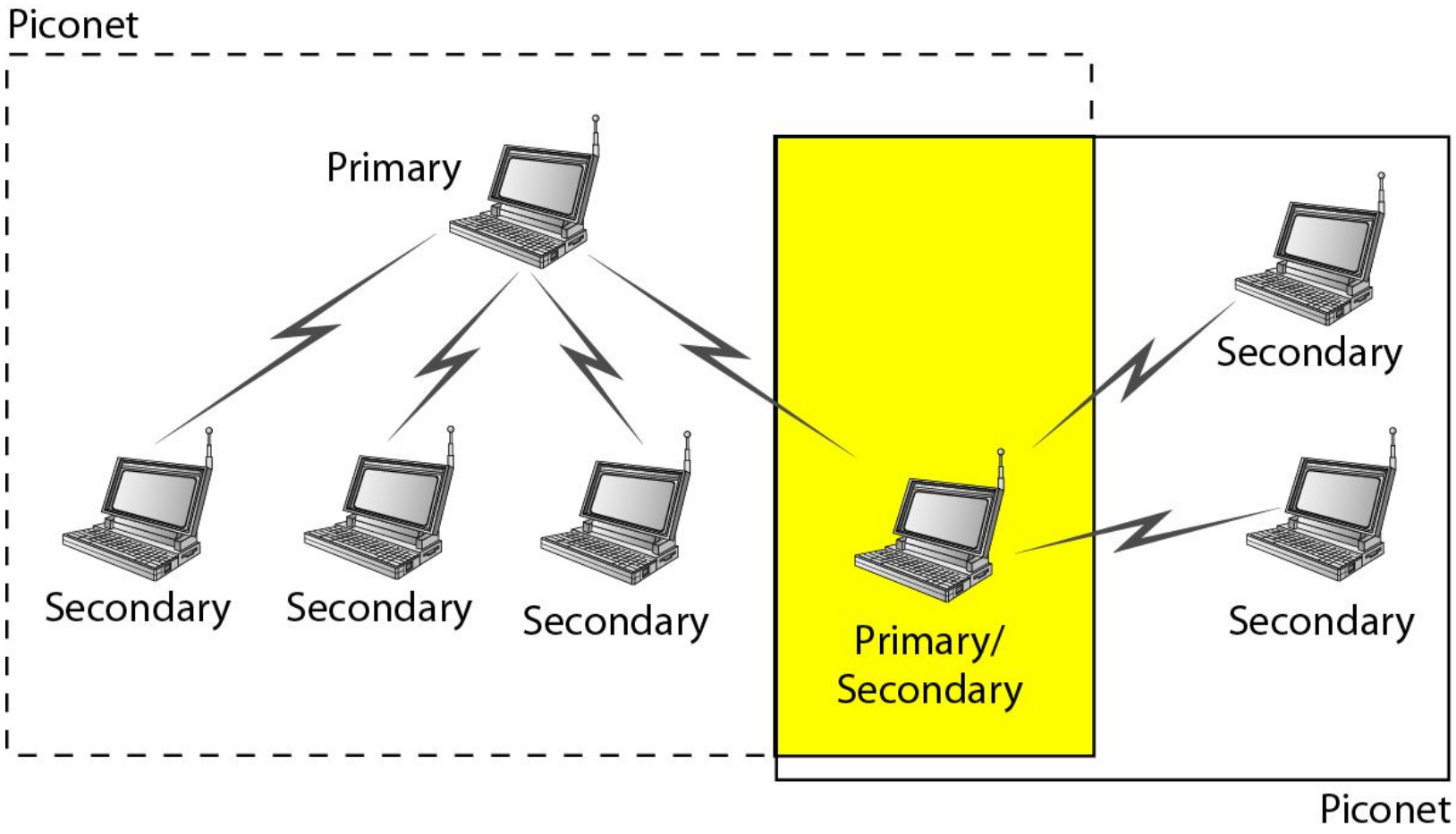
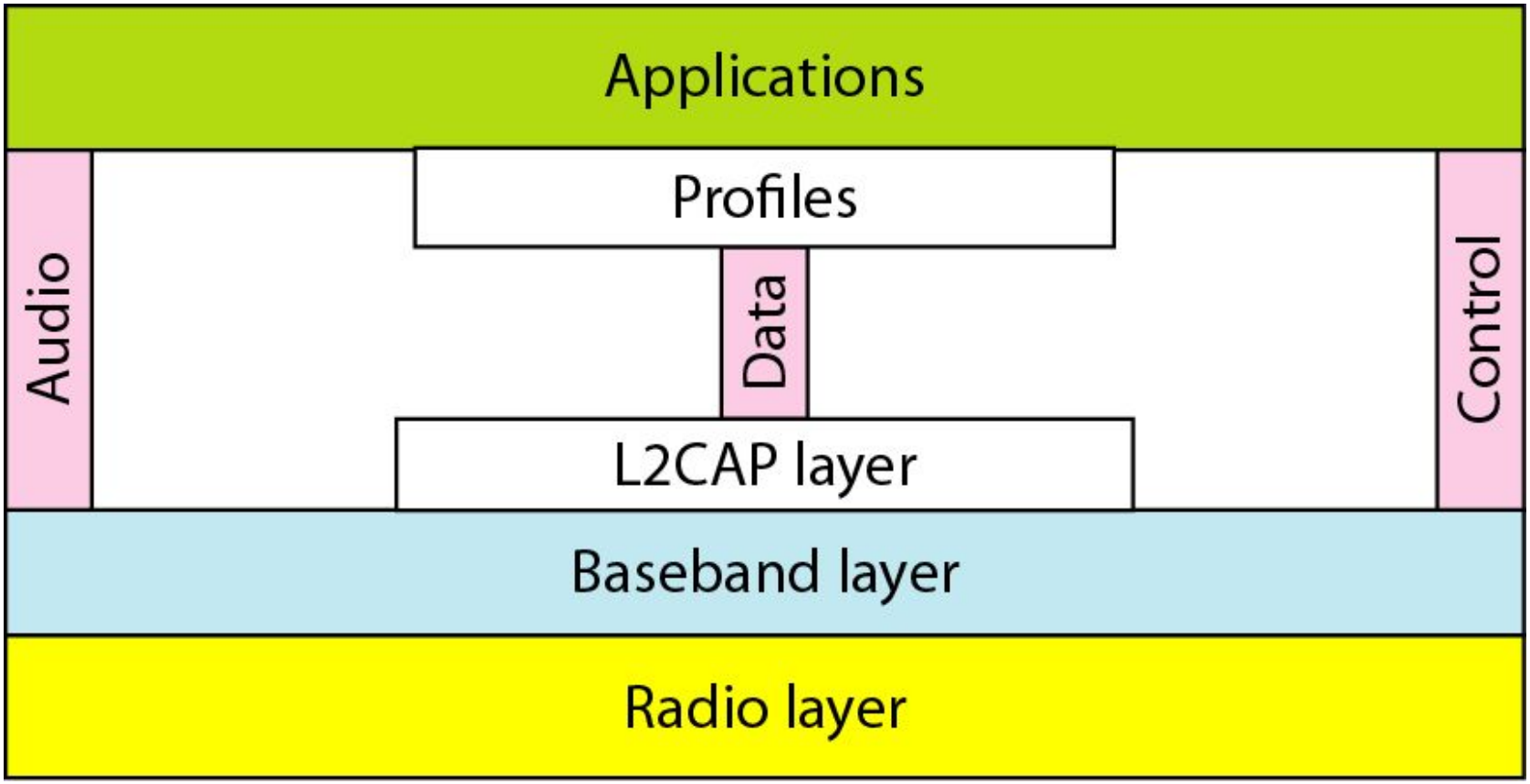


Figure 14.21 *Bluetooth layers*



Radio Layer

The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.

Band

Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.

FHSS

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.

Modulation

To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering)

Baseband Layer

The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA

Figure 14.22 *Single-secondary communication*

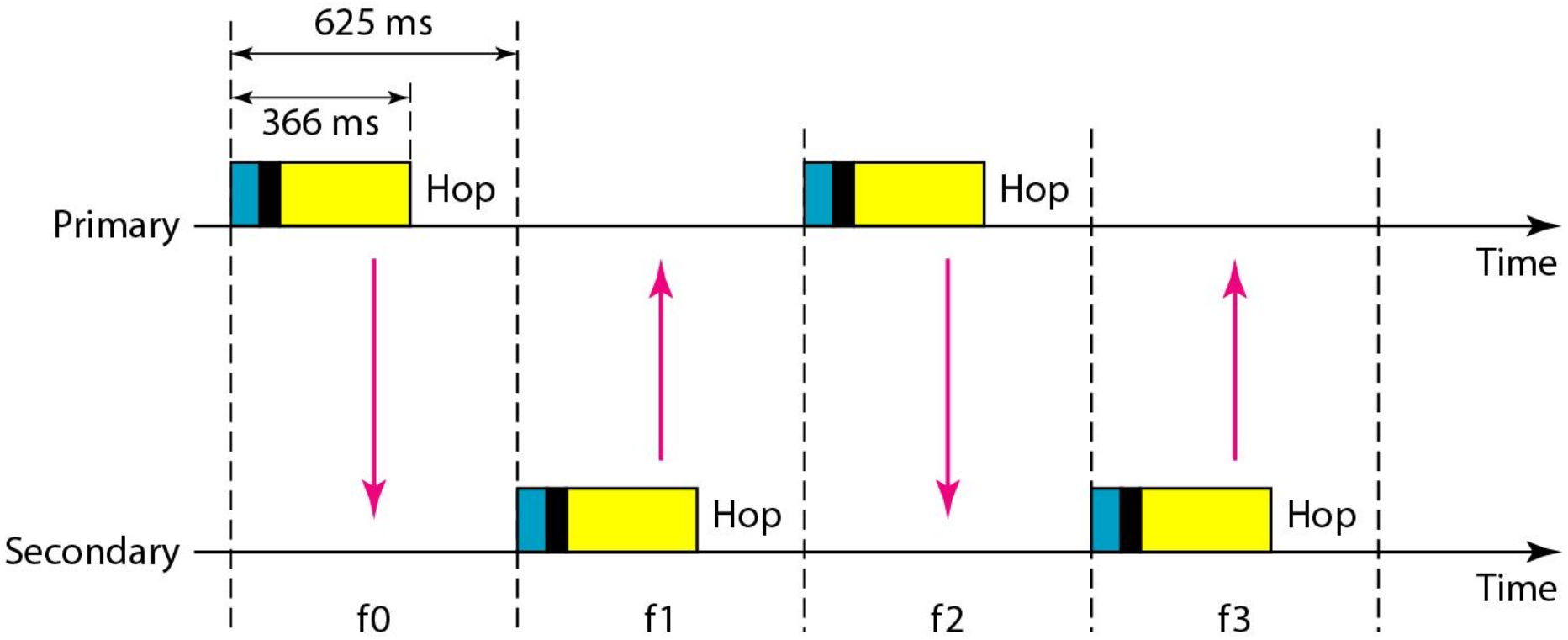
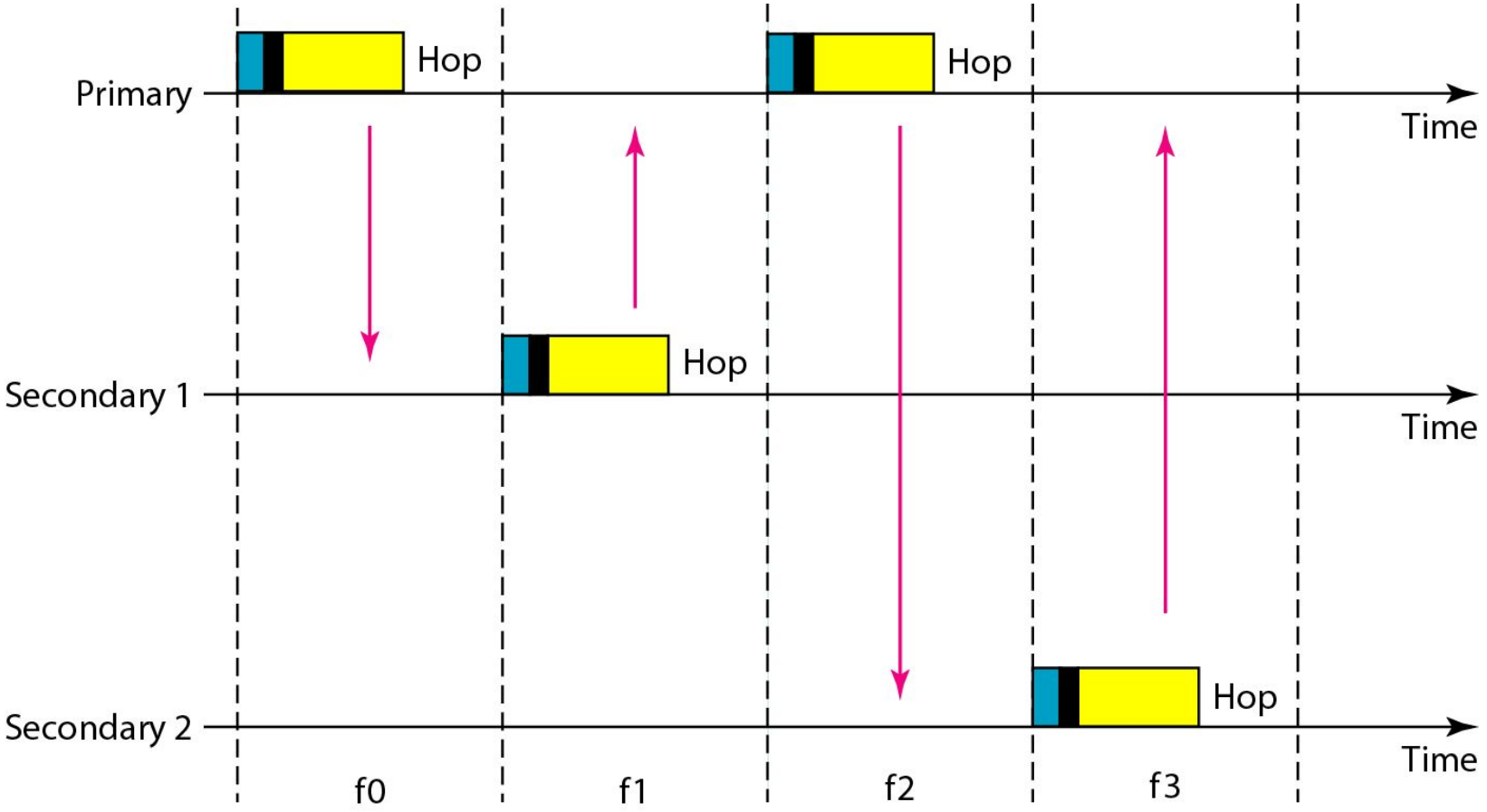


Figure 14.23 *Multiple-secondary communication*



Physical Links

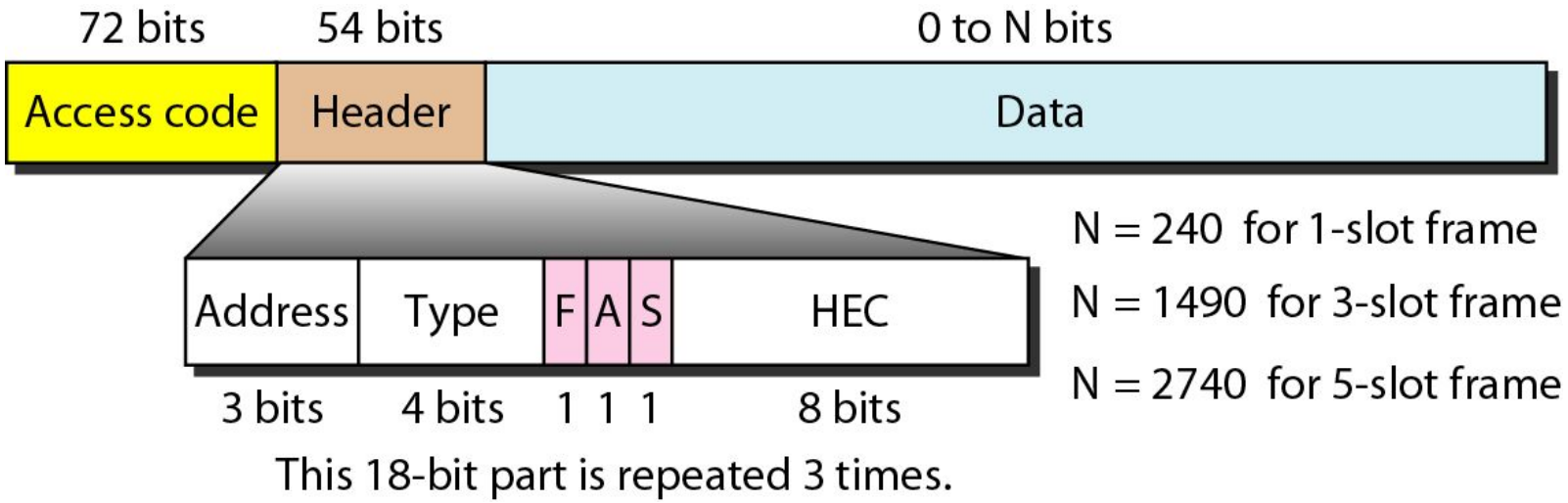
Two types of links can be created between a primary and a secondary:

SCQ links and ACL links.

SCQ : A synchronous connection-oriented (SCQ) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery). In an SCQ link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals. SCQ is used for real-time audio where avoiding delay is all-important.

ACL : An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency. In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted.

Figure 14.24 *Frame format types*



Access code. This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.

Header. This 54-bit field is a repeated I8-bit pattern. Each pattern has the following subfields:

1. Address. The 3-bit address subfield can define up to seven secondaries (I to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.

2. Type. The 4-bit type subfield defines the type of data coming from the upper layers.

3. F. This I-bit subfield is for flow control. When set (I), it indicates that the device is unable to receive more frames (buffer is full).

4. A. This I-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; I bit is sufficient for acknowledgment.

5. S. This I-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; I bit is sufficient for sequence numbering.

6. HEC. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.

Figure 14.25 *L2CAP data packet format*

L2CAP

The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link; SCQ channels do not use L2CAP.

L2CAP has specific duties: multiplexing, segmentation and reassembly, quality of service (QoS), and group management for multicasting.