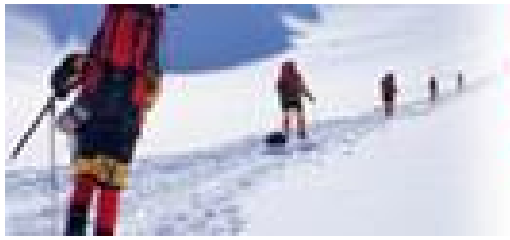


Data Communications and Networking Fourth Edition

Forouzan

第14章

无线局域网

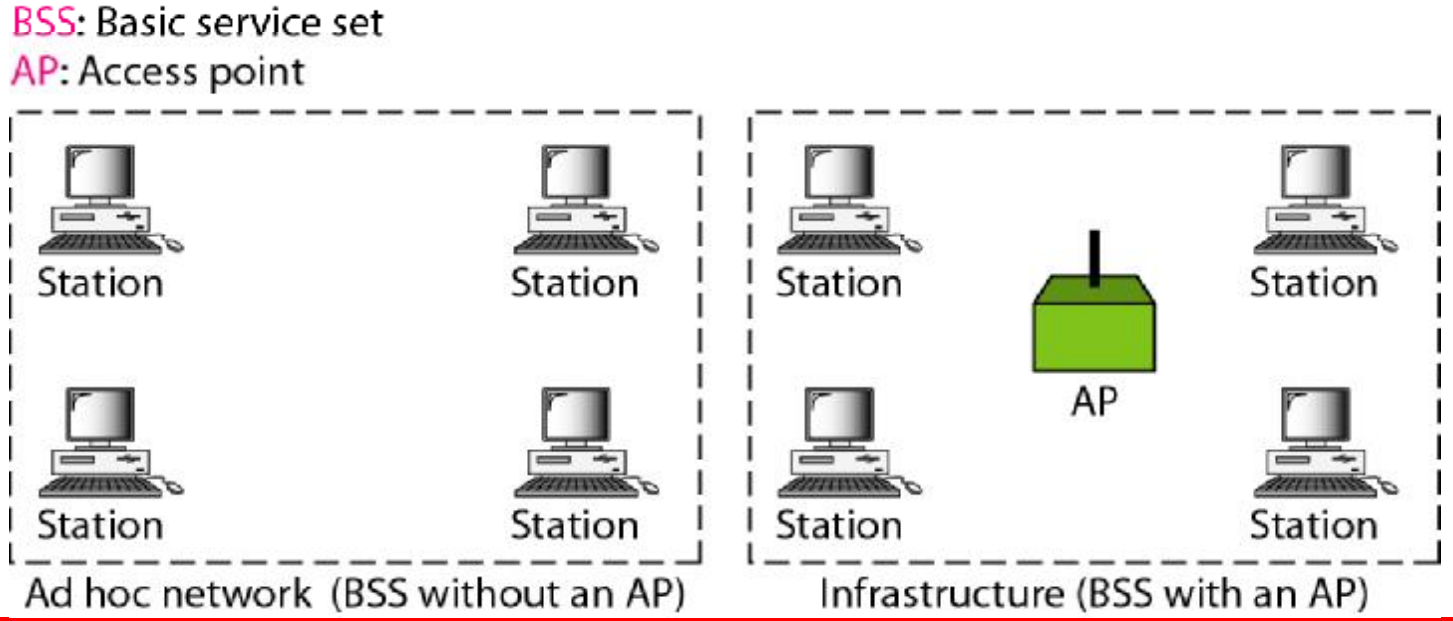
14-1 IEEE 802.11

- 由IEEE定义的无线局域网规范称做IEEE 802.11（有时也称为无线以太网），该规范涵盖了物理层和数据链路层；
- 标准定义了两种类型的服务：基本服务集（BSS）和扩展服务集（ESS）

图14.1 基本服务集(BSS)

p 由固定的或移动的无线站点和一个可选的、称为访问点AP的中央基站组成；

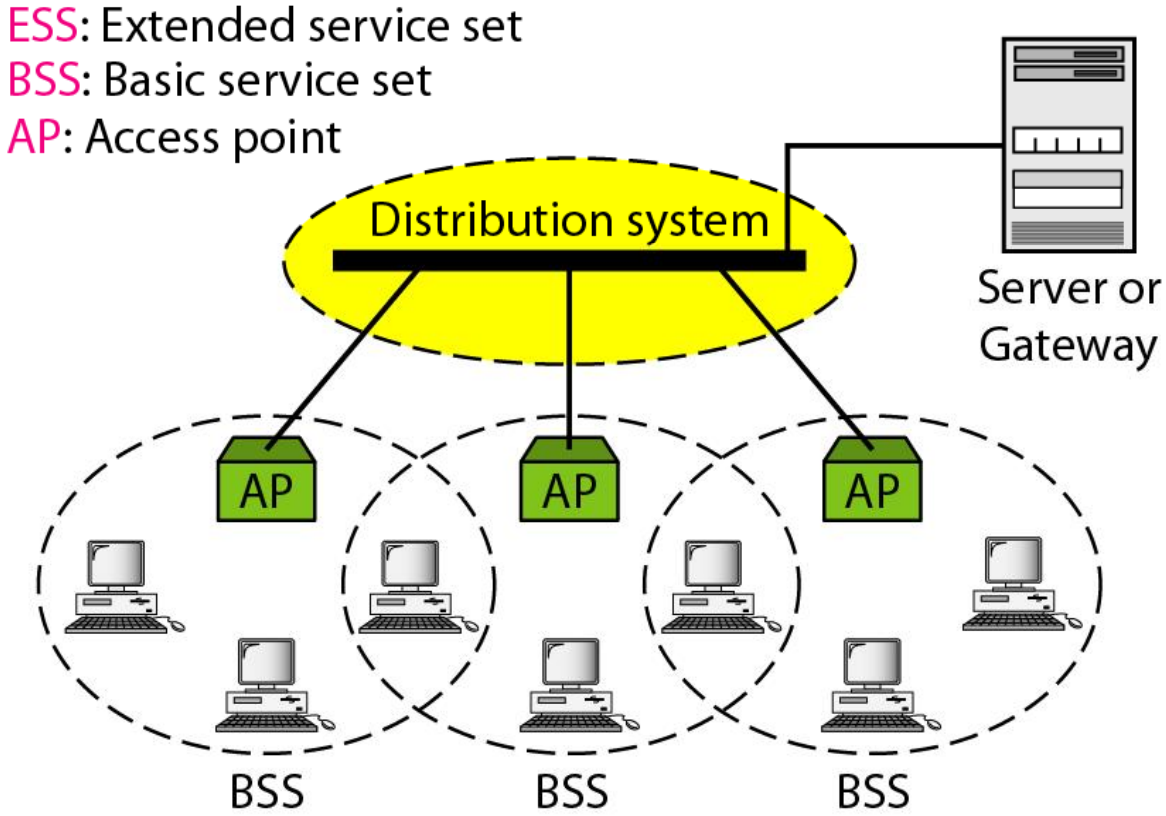
p 不带AP的BSS是一个独立网络，它不能向其他BSS发送数据，站点能够构成网络而不需要AP，它们能够相互定位并允诺是BSS的一部分（自组织）



不带AP的BSS称为ad hoc网络；
带AP的BSS称为基础（infrastructure）网络

图14.2 扩展服务集(ESS)

- 由两个或更多个带有AP的BSS组成，通过一个分布式系统（通常是有线局域网）将各个BSS（的AP）连接在一起；
- 使用两种类型的站点：移动的和固定的；移动站点指BSS内的普通站点，而固定站点则是一个属于有线局域网一部分的AP站；
- 连接BSS时，互相可达站点之间可以相互通信而不使用AP，但是两个不同BSS的站点间通信一般要跨过两个AP。

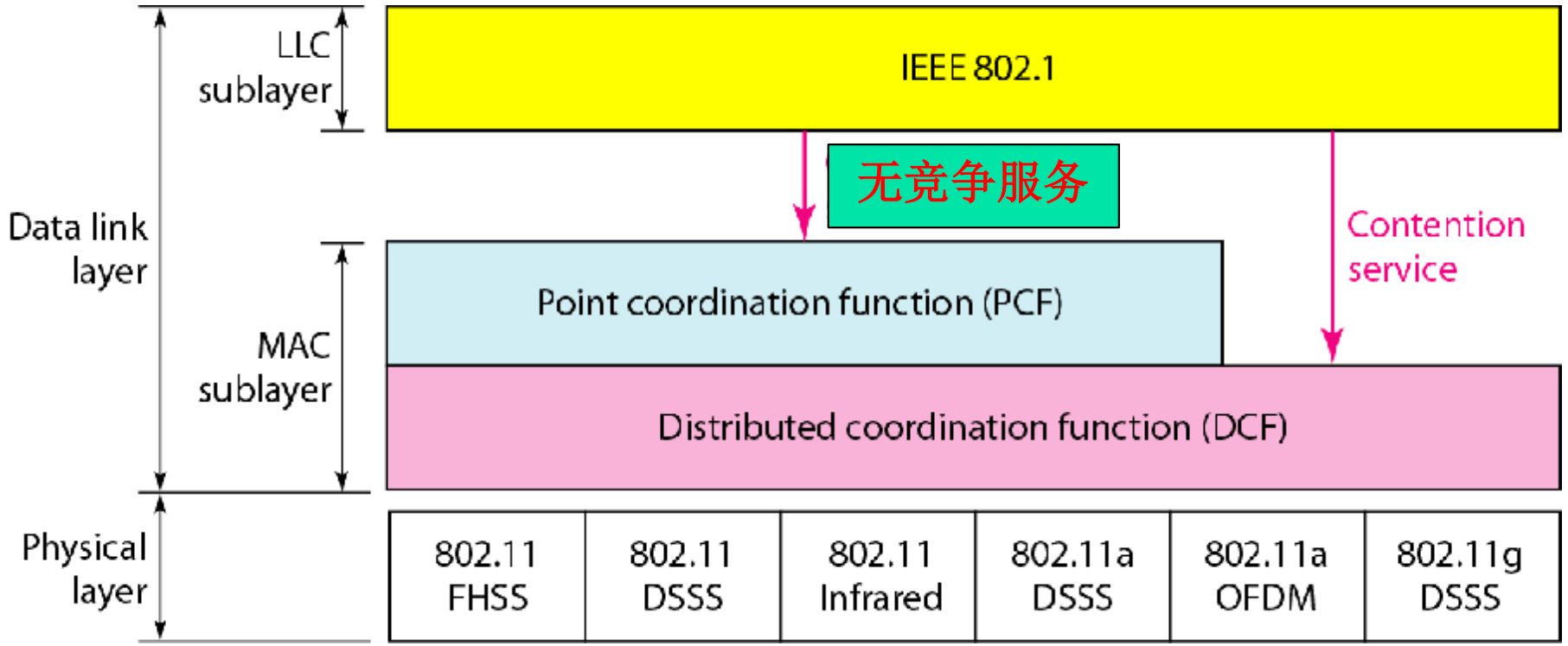


IEEE 802.11站点类型

- 根据站点在无线局域网中的移动性，分为三种类型：不迁移、BSS迁移和ESS迁移；
- 不迁移站点或者是一个固定（不移动）的，或者是仅在BSS内部移动的站点；
- BSS迁移站点可以从一个BSS移动到另一个BSS，但其移动被限制在一个ESS之内；
- ESS迁移站点可以从一个ESS移动到另一个ESS，但是IEEE 802.11不能保证通信在移动中是连续的。

图14.3 IEEE 802.11标准中的MAC层

p IEEE 802.11定义了两个MAC子层：分布式协调功能DCF和点协调功能PCF



分布式协调功能

- DCF使用CSMA/CA作为介质访问协议；
- 无线局域网因为三个原因不能实现CSMA/CD：
  - Ø1.为了冲突检测，站点必须能够同时发送数据和接收冲突信号，这就意味着建立站点的费用很高，并且增加了带宽需求；
    - Q：802.11半双工？-时分双工TDD-什么时候冲突？
  - Ø2. 因为隐藏的站点问题，可能检测不到冲突；
  - Ø3. 站点间的距离可以很大，信号衰减会使得一端的站点很难侦听到另一端的冲突。

图14.4 CSMA/CA流程图

p 1.发送帧前，源站点通过检测载波频率的能量级来侦听介质

Ø a. 在通道空闲之前，通道使用带有补偿的持续策略；

Ø b. 站点发现通道空闲之后，它等待DIFS，然后发送“请求发送RTS”控制帧（未画出竞争窗口机制？）

p 2.收到RTS并等待SIFS的短暂时间后，目的站点向源站点发送“清除发送”CTS控制帧，表示目的站点准备接收数据；

p 3.等待SIFS后，源站点发送数据；

p 4.等待SIFS后，目的站点发送确认说明已经接收到帧；在这个协议中，由于没有任何方法检查它的数据是否已经成功地到达目的站点，所以确认还是需要的（而在CSMA/CD中，没有冲突就是向源站点表示数据已经到达）。

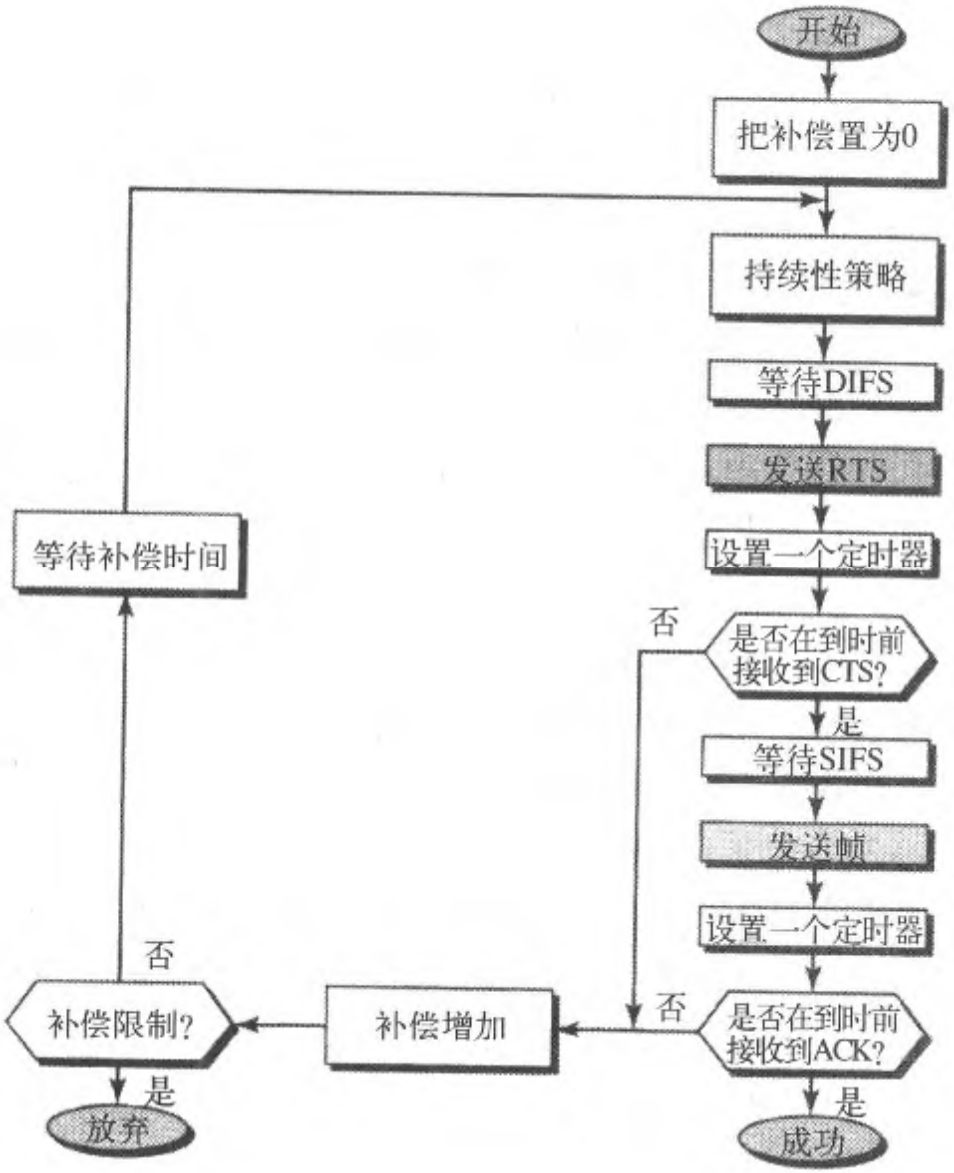
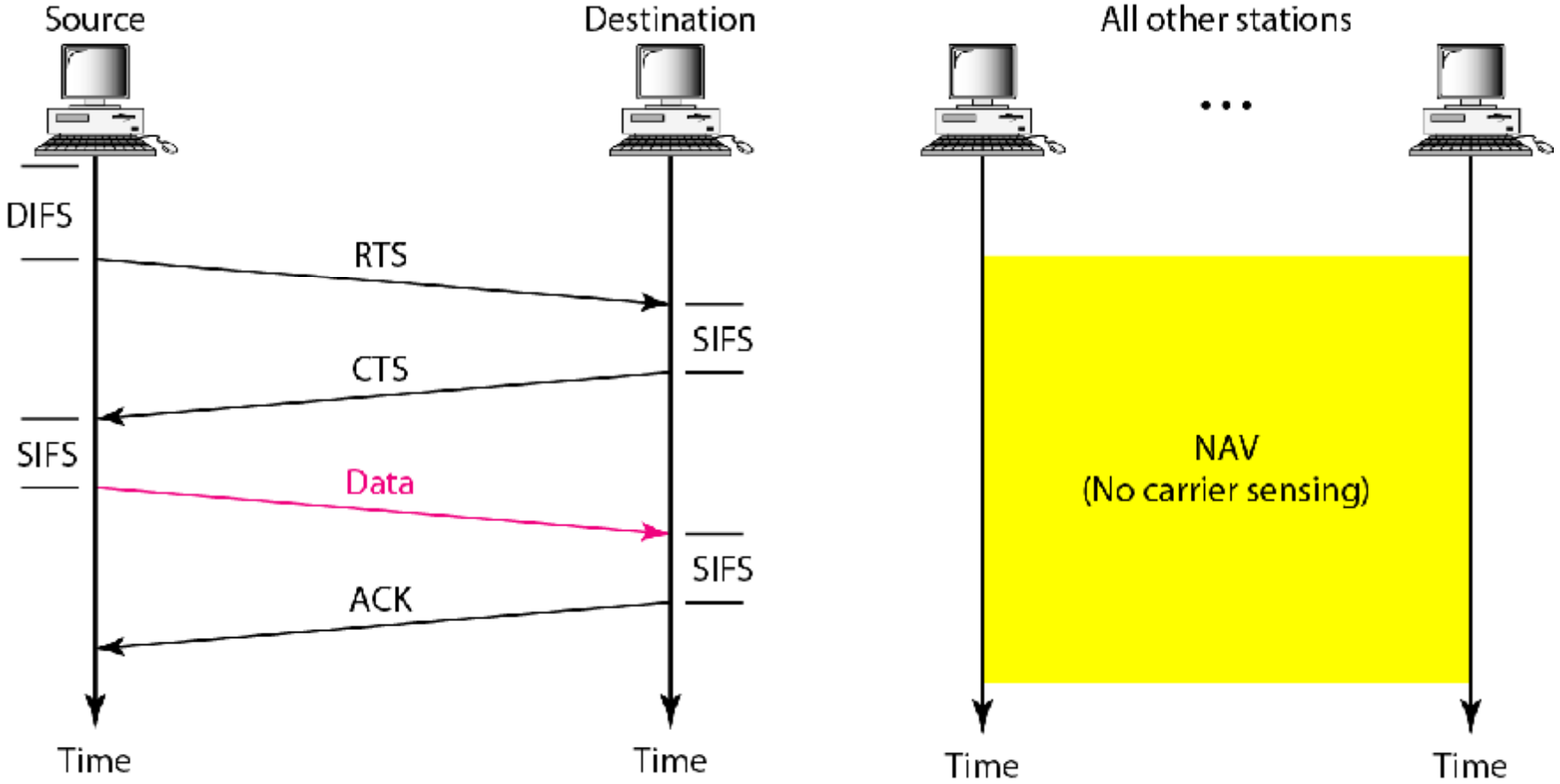


图14.5 CSMA/CA和NAV（Network Allocation Vector）

p若一个站点获得访问权，那么其他站点如何推迟发送数据的时间呢？即如何实现冲突避免呢？关键是一个叫做NAV的特性。



p RTS帧包含了需要占据通道的时间，受影响的站点会建立一个叫做网络分配矢量NAV的定时器，指出在允许这些站点检测通道是否空闲之前还必须要经过多长时间；

p 每当一个站点访问系统并且发送RTS帧时，其他站点就启动它们的NAV；换句话说，对任何一个站点，在检查物理介质是否空闲之前，首先要检查它的NAV是否过期；

p 在RTS或CTS发送期间（叫做握手周期），若两个或更多站点同一时刻试图发送RTS帧，这些控制帧可能会相互冲突，但由于没有检测冲突的机制，因此发送方在它没有收到CTS时就以为产生了冲突，于是采取补偿策略并重新发送。

点协调功能PCF

- 一种可以在基础设施网络中（不在Ad hoc网络中）实现的可选访问方式；
- 它在DCF之上实现，主要用于对时间敏感的传输；
- PCF是集中式的、无竞争的轮询访问方式，AP对那些可以被轮询的站点进行轮询，站点依次被轮询，将数据发送给AP；
- 为了给予PCF高于DCF的优先级，定义了另一套帧间间隔：PIFS和SIFS；
- SIFS与DCF中的一样，但是PIFS（PCF IFS）比DIFS短，这意味着如果同时一个站点想只使用DCF，而一个AP想使用PCF，那么AP有优先权。

- 由于PCF的优先级高于DCF，只使用DCF的站点可能得不到对介质的访问；
- 为避免此问题，设计了重复间隔来覆盖无竞争（PCF）和基于竞争（DCF）的通信；
- 重复间隔会持续地重复，开始于一个称为信号帧（beacon frame）的特殊控制帧；当站点听到信号帧时，在重复间隔的无竞争周期内它们开始它们的NAV；
- 重复间隔中，PC（点控制方）可以发送轮询帧、接收数据、发送ACK、接收ACK或者做任何这些动作（802.11 使用捎带）的组合；
- 在无竞争周期结束时，PC发送CF结束（无竞争）帧允许基于竞争的站点使用介质。

图14.6 重复间隔的例子

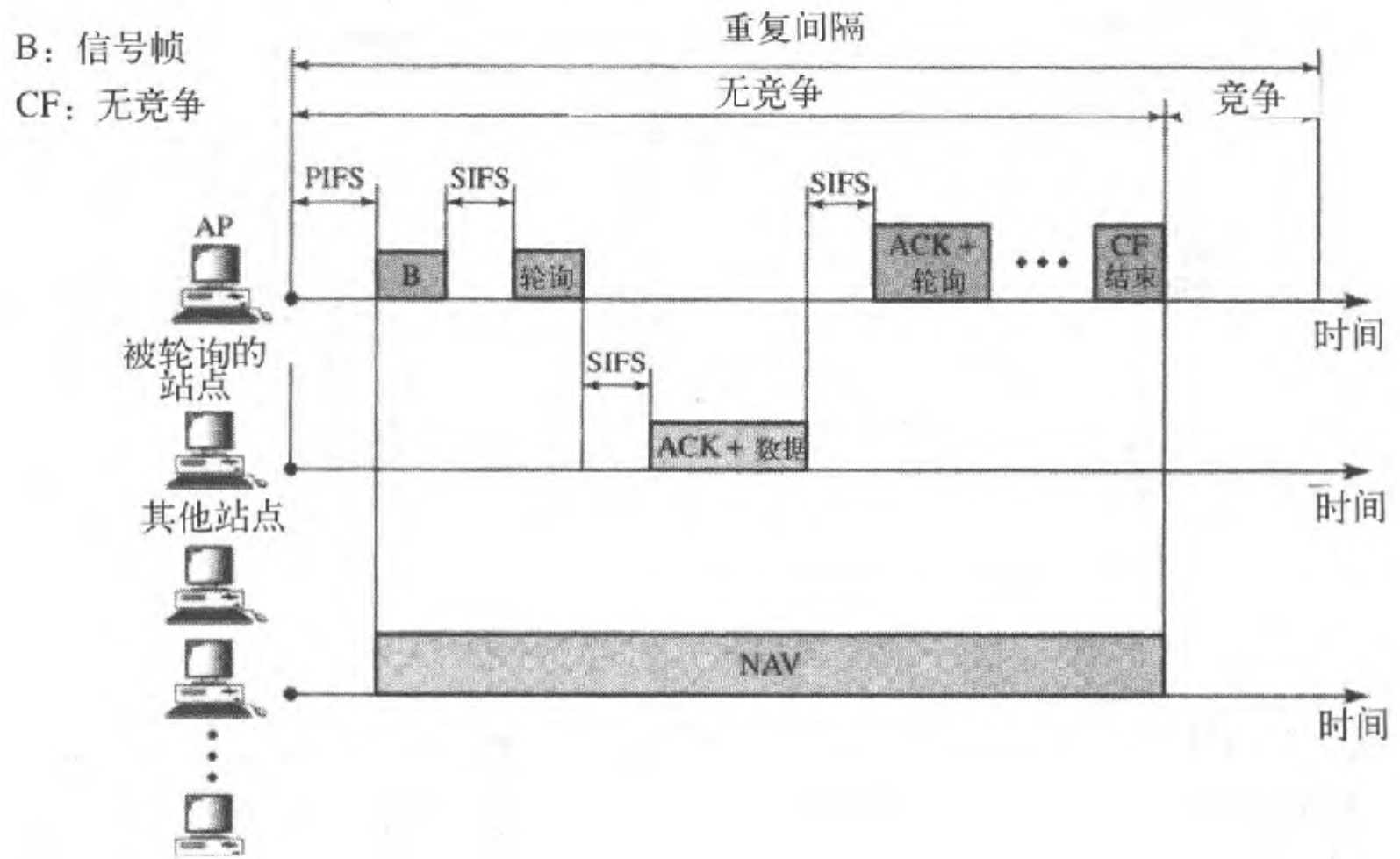


图14.7 帧格式

- 帧控制FC：2 字节，定义了帧的类型（控制、管理和数据）和一些控制信息（如分片、私密等）；
- D：设置NAV值的传输间隔时间，或帧ID（某些控制帧中）；
- 地址：4个6字节地址字段，字段含义取决于to DS和from DS子字段的值；
- 序列控制：定义帧的序列号，用于流量控制；
- 帧主体：0-2312字节，包含了具体信息；
- FCS：4字节CRC差错检测序列

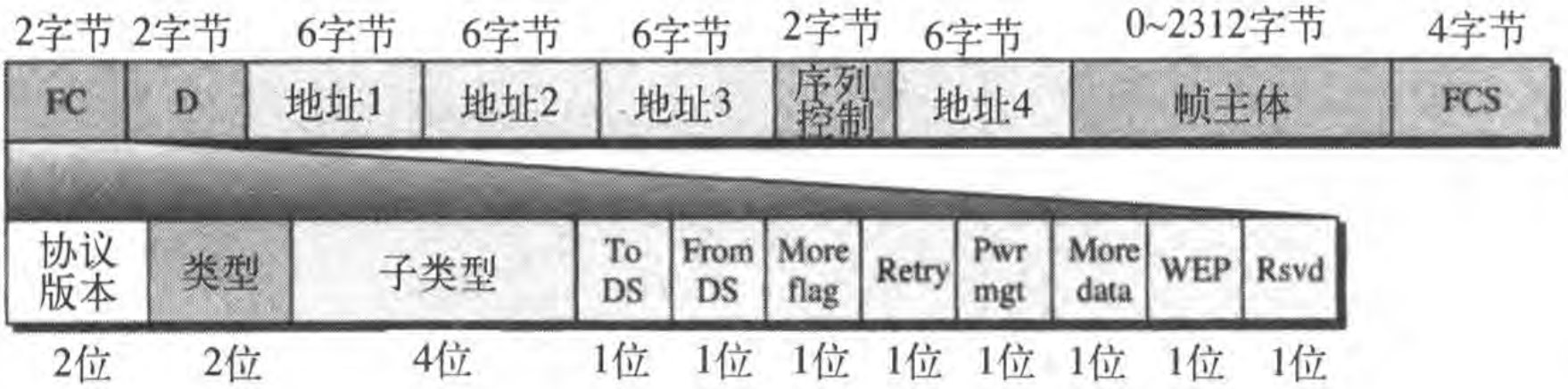
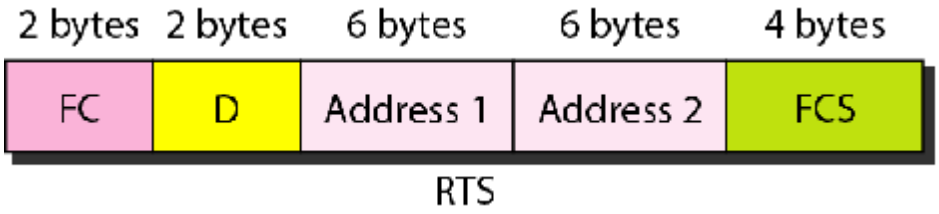


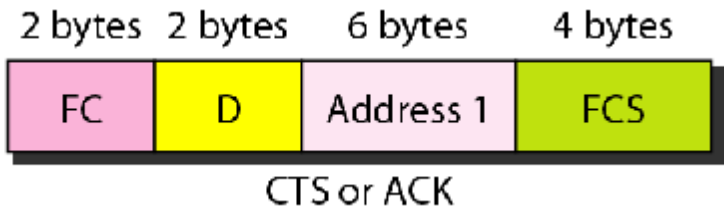
表14.1 FC字段中的子字段

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

帧类型

- IEEE 802.11定义了三种类型的帧：管理帧、控制帧和数据帧；
- 管理帧用于在站点和AP之间初始化通信，包括关联的管理（请求、响应、重关联、取消关联以及鉴别等）；
- 控制帧用于访问通道和对帧的确认，主要包括RTS、CTS和ACK（其实共6小类，还包括节电轮询、无争用结束、无争用结束加无争用确认）；
- 数据帧用于携带数据与控制信息





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

寻址机制

p00：帧既不是发往也不是来自一个分布式系统中，它是从BSS中的一个站点到另一个站点，而不经过分布式系统；

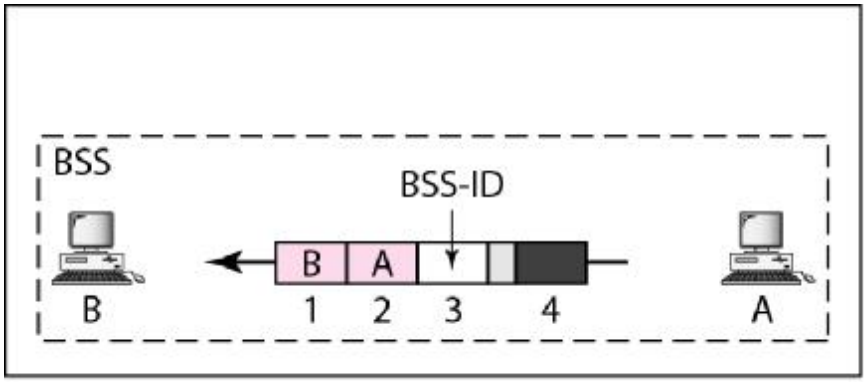
p01：帧从一个分布式系统中来；帧从一个AP来，到一个站点去，地址3包含帧的原始发送方地址（在另外的BSS中）；

p10：帧要发送到一个分布式系统中去，帧是从一个站点发往AP，地址3包含帧的最终目的地址（在另外的BSS中）；；

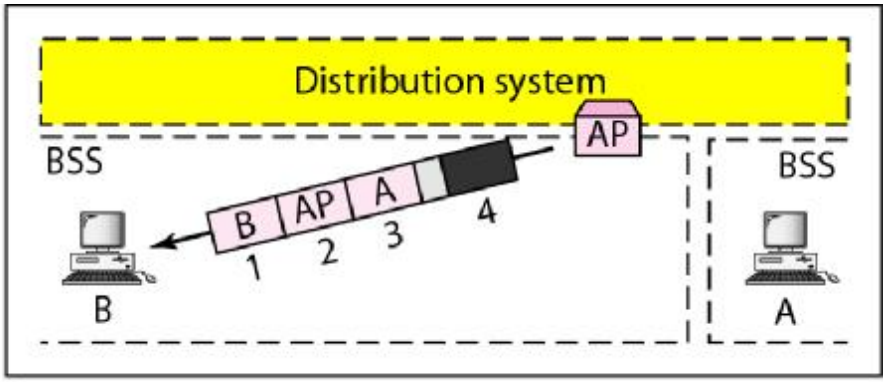
p11：说明分布式系统也是无线的，帧在一个无线分布式系统中从一个AP发送到另一个AP。

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

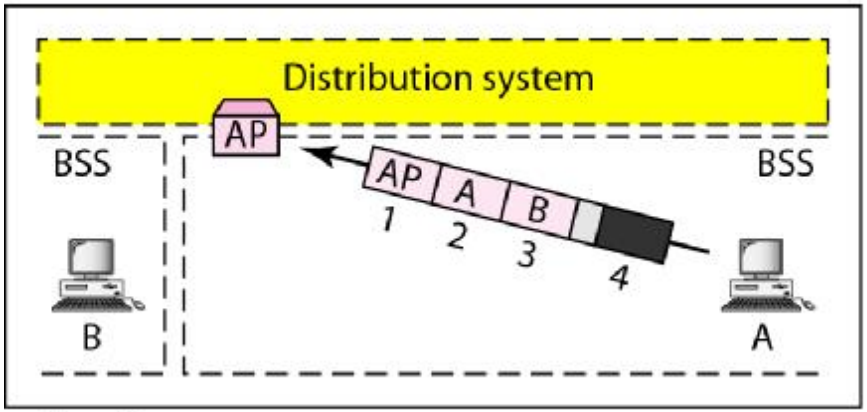
图14.9 寻址机制



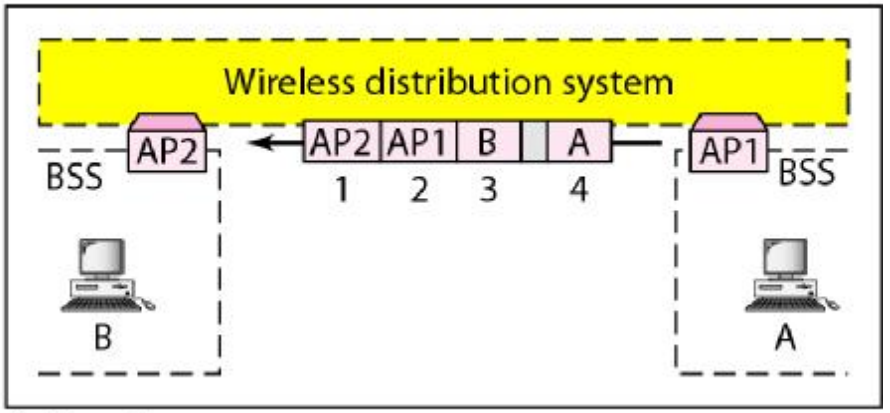
a. Case 1



b. Case 2



c. Case 3



d. Case 4

图14.10 隐藏站点问题

- 假设B和C都要发数据给A，由于B在C的范围之外且C在B的范围之外，它们都认为介质是空闲的，产生了冲突，此时，说站点B和C对于A来说是互相隐藏的；
- 因为冲突的可能性，隐藏站点降低了网络的能力

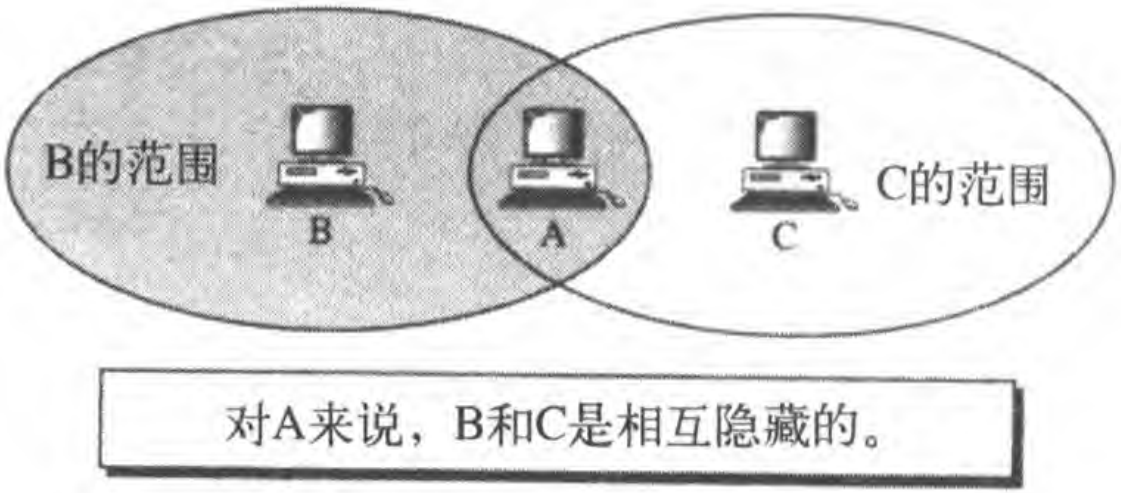


图14.11 握手的使用来避免隐藏站点问题

pCSMA/CA握手中的CTS帧可以避免来自隐藏站点的冲突，因为A的CTS可以同时到达B和C，C知道一些隐藏站点正使用通道，就限制传输直到这个期间结束

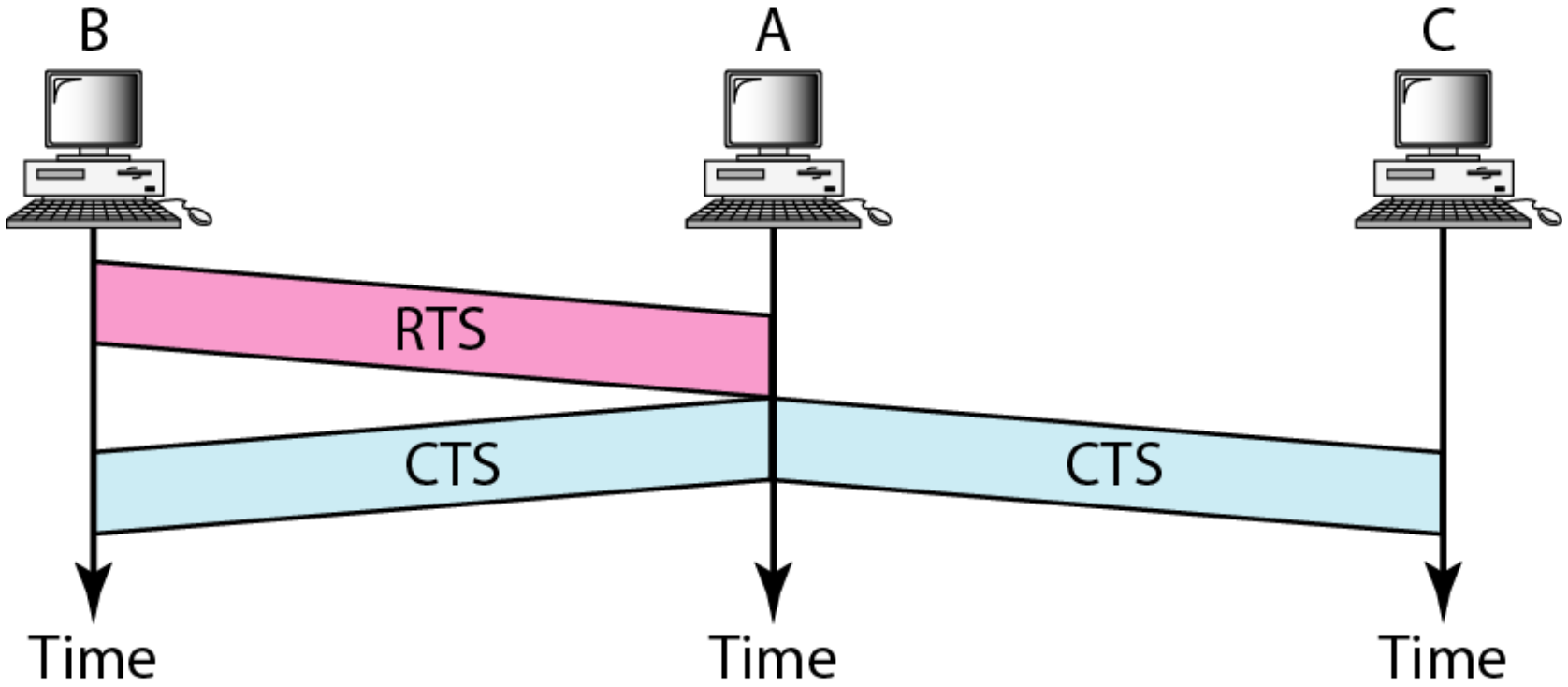


图14.12 暴露站点问题

p站点被限制使用通道，尽管通道是可用的；

pA向B传送，C有一些数据要发送给D，这应该可以发送而不会干扰到从A到B的传输；

p但是，C暴露给了A的传送，它听到A在发送，这样被限制了发送；换句话说， C太保守，浪费了通道的能力。

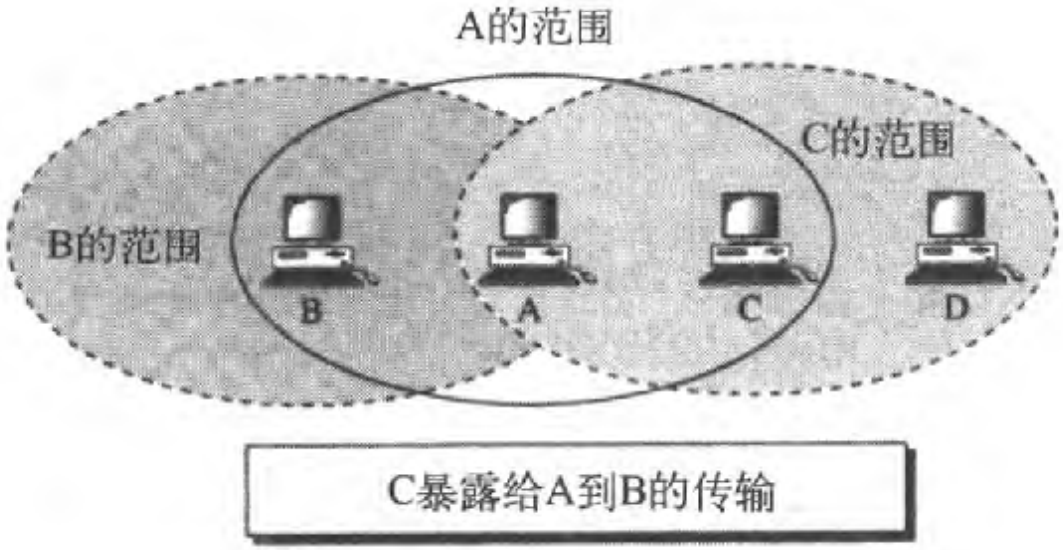


图14.13 暴露站点问题中握手的使用（P288：后两个B->D）

pC由于冲突不能接收到来自D的CTS，它会保持暴露直到A结束它的数据发送

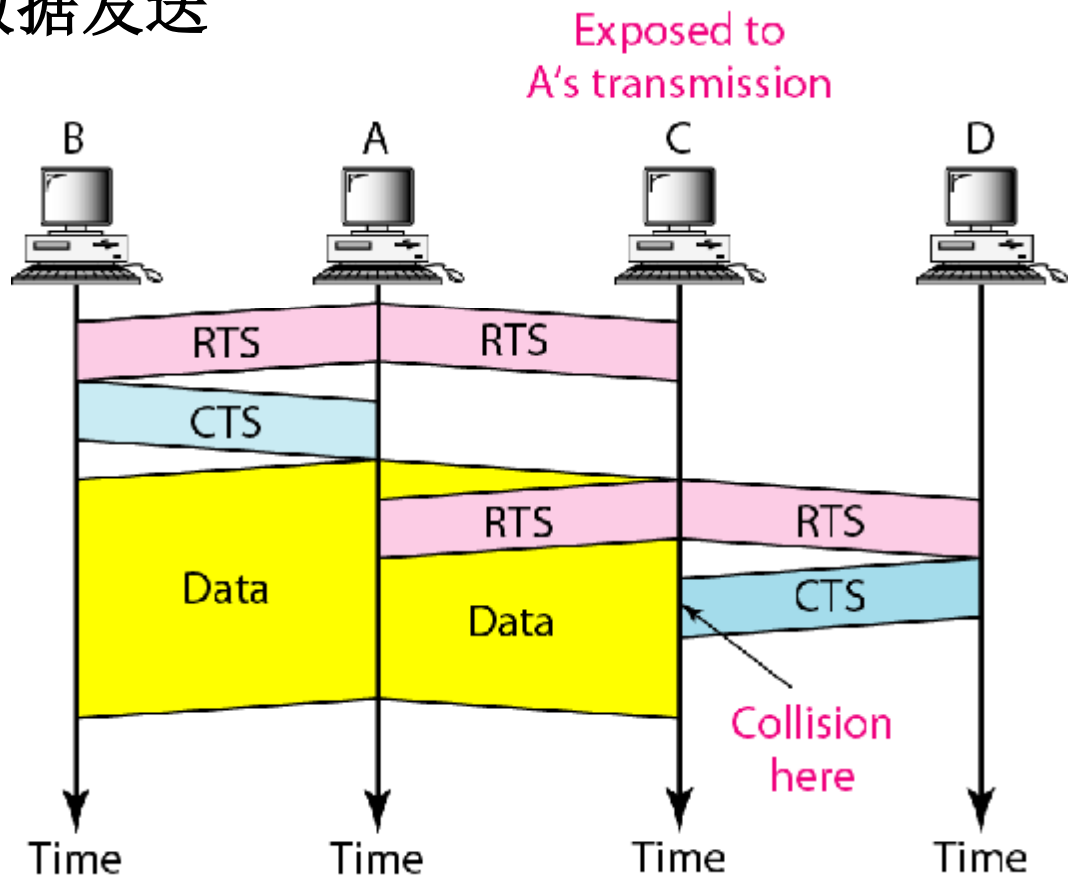


表14.4 物理层规范

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

图14.14 工业的、科学的和医学（ISM）的频带-不需要许可证

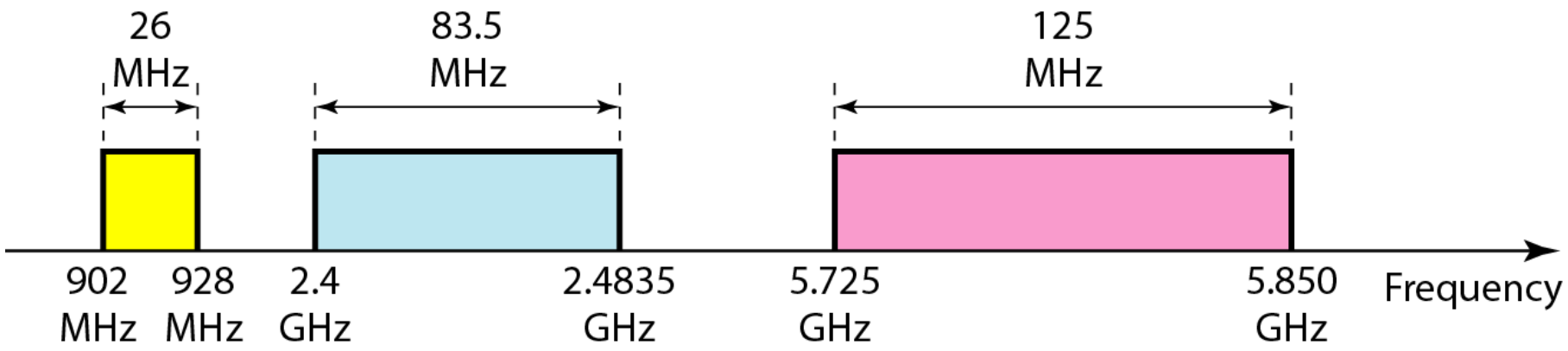


图14.15 IEEE 802.11 FHSS的物理层

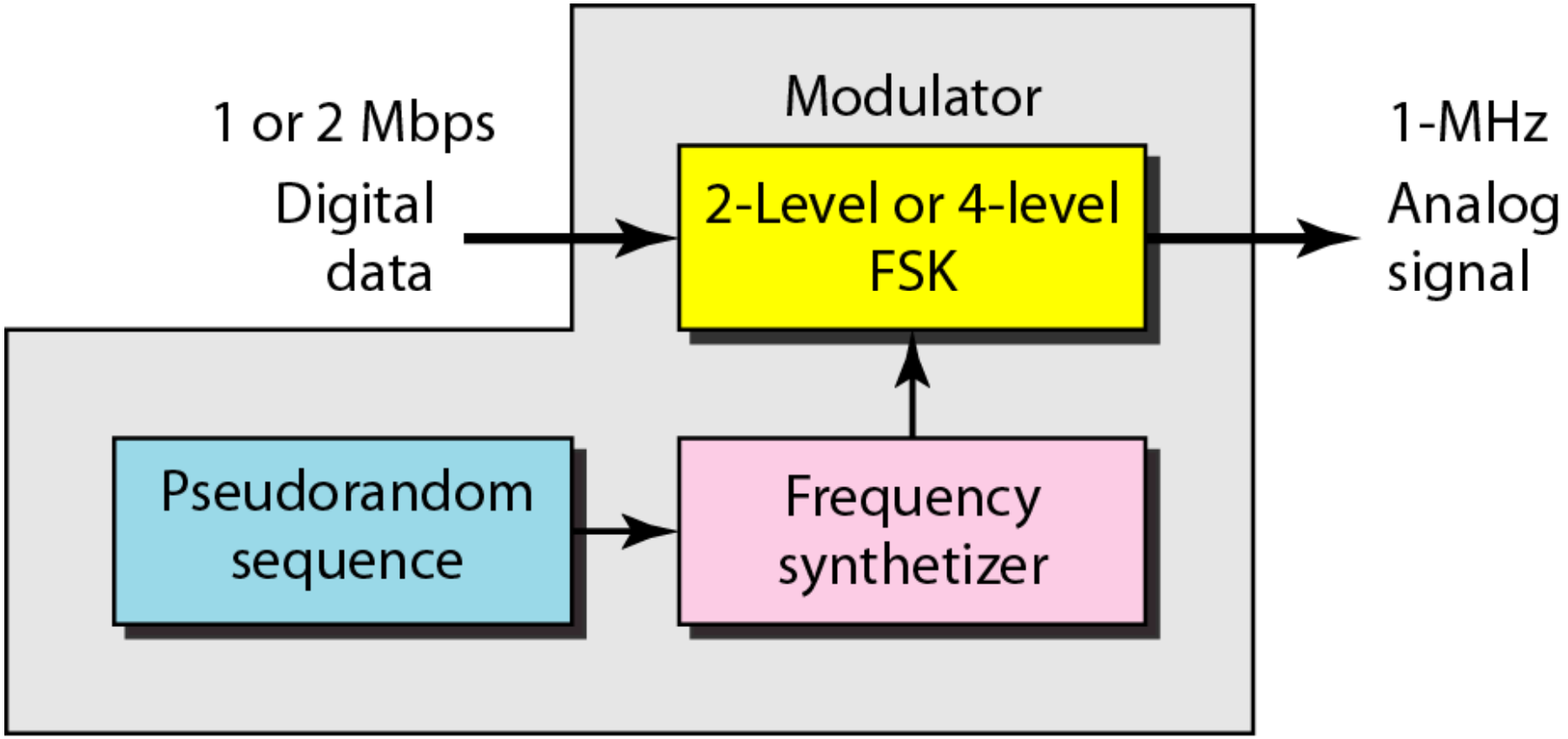


图14.16 IEEE 802.11 DSSS的物理层

图14.17 IEEE 802.11红外线的物理层

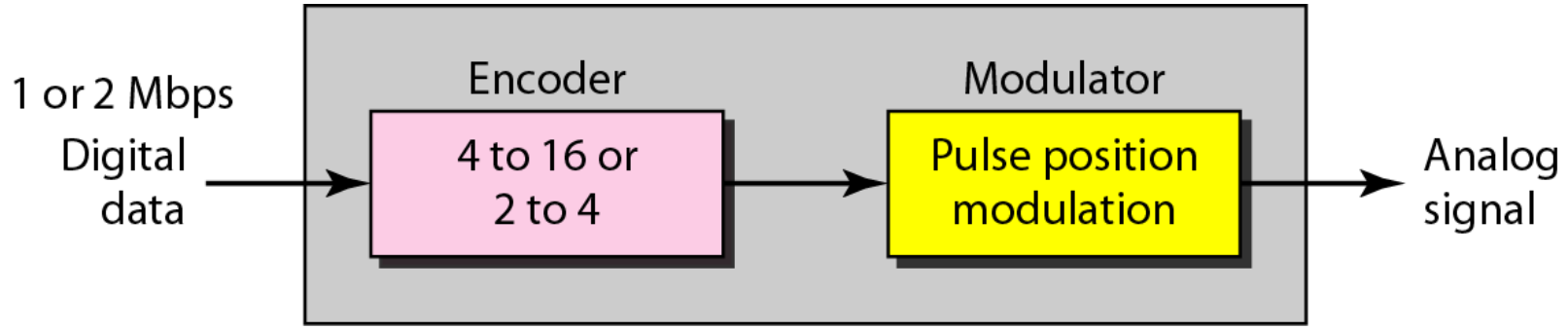


图14.18 IEEE 802.11b的物理层