第3章 无线局域网

第3章 无线局域网

3.1 概述

3.1.1 无线局域网的覆盖范围

3.1.2 无线局域网的特点

3.1.3 无线局域网的发展历程与相关标准化活动

3.1.4 无线局域网的分类与应用

3.1.1 无线局域网的覆盖范围

- 无线局域网是在局部区域内以无线媒体或介质进行通信的无线网络。
- 局部区域就是距离受限的区域，是相对广域而言。两者的区别主要在于数据传输的范围不同(但覆盖范围界限的区别并不十分明显)，从而引起网络设计和实现方面的一些区别。
- 介于广域网WAN和局域网LAN之间还有一种局部网络，称为城域网
- 比局域网覆盖范围更小的局部网络称为个(人区)域网。
- 广义的无线局域网还包含无线城域网(WMAN)和无线个域网(WPAN)。
- 无线网络也可以粗略分为无线广域网和无线局域网两种。

3.1.2 无线局域网的特点-优点

- 移动性：支持固定、半移动和慢速移动，支持数据链路层的越区切换或散步、以及网络层的漫游。
- 灵活性：组网方式灵活，通过基础节构接入或Adhoc组网
- 可伸缩性：通过添加AP及EP扩展
- 经济性：降低布线及人员费用

3.1.2 无线局域网的特点-局限性

- 可靠性(Reliability)
- 带宽与系统容量
- 兼容性(Compatibility)与共存性(Coexistence)
- 覆盖范围（引入蜂窝结构及采取桥接、中继等措施）
- 干扰（外界干扰、自干扰、网间干扰）
- 安全性（信息安全及人员安全）
- 节能管理
- 多业务与多媒体
- 移动性
- 小型化、低价格

3.1.3 无线局域网的发展历程与相关标准化活动

起源于Aloha Net，经历了四代:

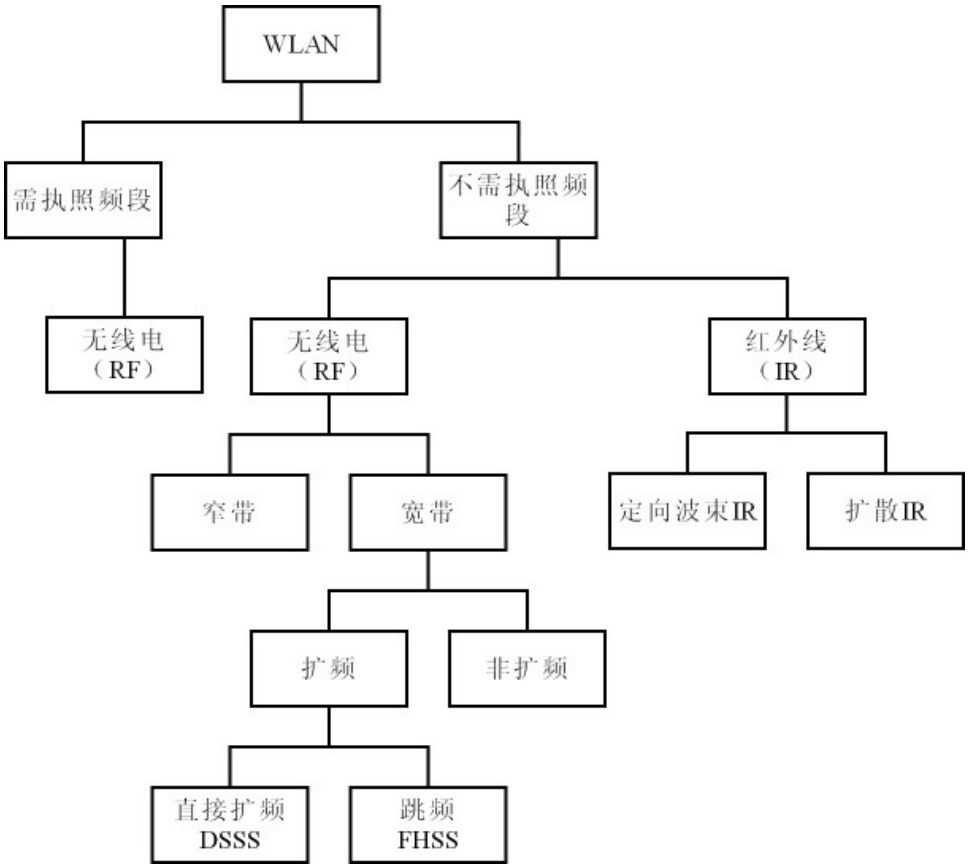
- 第一代:1985年，FCC颁布的电波法规为无线局域网的发展扫清了道路，分配专用频段1-2GHz以及ISM免许可频段。
- 第二代：基于HiperLAN1和IEEE 802.11标准的无线局域网。
- 第三代：符合IEEE 802.11b标准的产品已经较为普及，归为第三代无线局域网产品；
- 第四代：将符合IEEE 802.11a、HiperLAN2和IEEE 802.11g标准的产品称为第四代无线局域网产品。

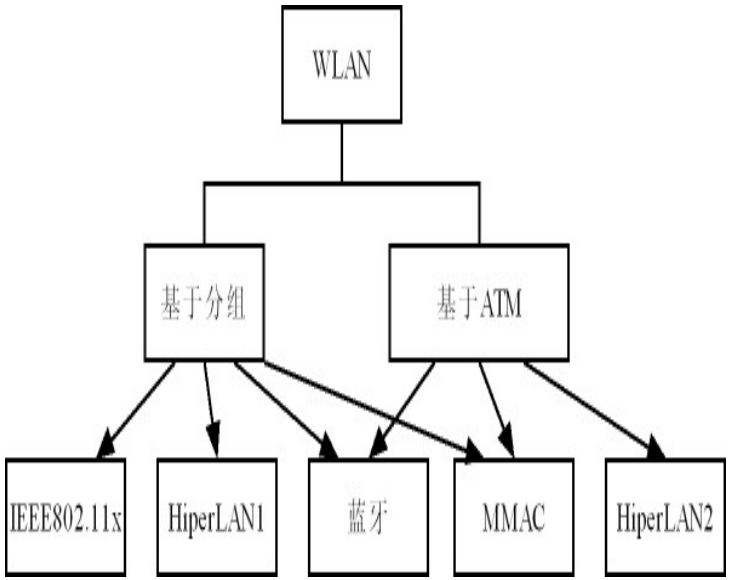
IEEE802.11下的任务组

任务组：	研究范围和目标	状　态
MAC组	为WLAN开发MAC机制	已完成，作为IEEE 802.11的一部分；被ISO/IEC接纳为8802-11：1999标准
PHY组	为WLAN开发三种PHY层机制：Infrared，DSSS和FHSS	已完成，作为IEEE 802.11的一部分，并被ISO/IEC接纳为8802-11：1999标准
TGa	开发适用于UNII频段的PHY规范	已完成，成为IEEE 802.1la标准，并被ISO/IEC接纳为8802-11：1999(E)标准
TGb	开发2.4 GHz频段的高速PHY规范	已完成，成为IEEE 802.11b标准
b-corl	纠正802.11b的MIB的不足和缺陷	进行中
TGc	向IEEE 802.1d标准提供所需要的信息，实现网桥和802.11MAC互操作	已完成，并作为IEEE 802.1d标准的一部分
TGd	为MIB定义新的PHY参数，并扩展802.11以适应一些国家的要求	进行中
TGe	增强MAC机制，改进QoS和CoS，增强认证和安全机制(已移至TGi)	进行中
TGf	制定IAPP协议	进行中
TGg	开发新的PHY规范，通过提高速率增强802.11b的性能和可用性	已完成，成为IEEE 802.11g标准
TGh	提高802.11MAC和802.11aPHY的网络管理和控制功能，提供动态信道选择和功率控制	进行中
TGi	增强MAC机制，提高安全和认证机制	进行中
TGn	利用智能天线技术提高传输速率、覆盖范围和系统容量	进行中
5GSG	和ETSI-BRAN合作，研究5GHz频段的全球化和协调	
Ad Hoc Publicity	通过研究应用和操作来推广802.11	
Ad Hoe Regulatory	跟踪各个国家的要求，确保802.11符合他们的要求	

3.1.4 无线局域网的分类与应用

- 无线局域网可根据不同的层次、业务、技术和标准以及应用等进行分类。

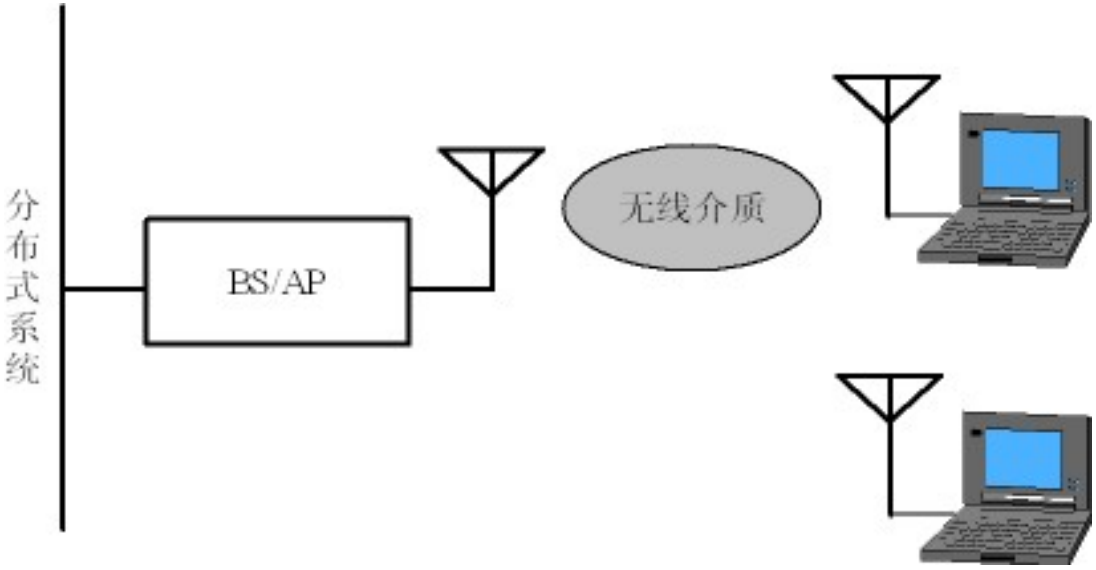




第3章 无线局域网

3.2　无线局域网的体系结构与服务

3.2.1 无线局域网的组成结构



1. 站STA(Station)

站也称主机或终端，是无线局域网的最基本组成单元,包括：

- 终端用户设备
- 无线网络接口:无线网卡或调制解调器
- 网络软件

移动站的分类	固定站	半移动站	移动站
开机使用的移动站	固定	固定	固定/移动
关机时的移动站	固定	固定/移动	固定/移动
举例	台式机	便携机	掌上机

站与站可以直接通信，也可以通过AP通信。

- 服务区域：无线局域网所能覆盖的区域
- 基本服务区：移动站的无线收发信机及地理环境所确定的通信覆盖区域
- 基本业务组：一个基本服务区内相互通信的主机集合

2．无线介质

- 无线介质是无线局域网中站与站之间、站与接入点之间通信的传输介质。空气是无线电波和红外线传播的良好介质。
- 无线局域网中的无线介质由无线局域网物理层标准定义。

3. 无线接入点

- 无线接入点类似蜂窝结构中的基站，是无线局域网的重要组成单元。是一种特殊的站，通常处于BSA（基本服务区）的中心，固定不动。
- 无线接入点具有无线网络接口，包括与分布式系统的接口、无线网络接口及相关软件。
- 无线接入点基本功能：

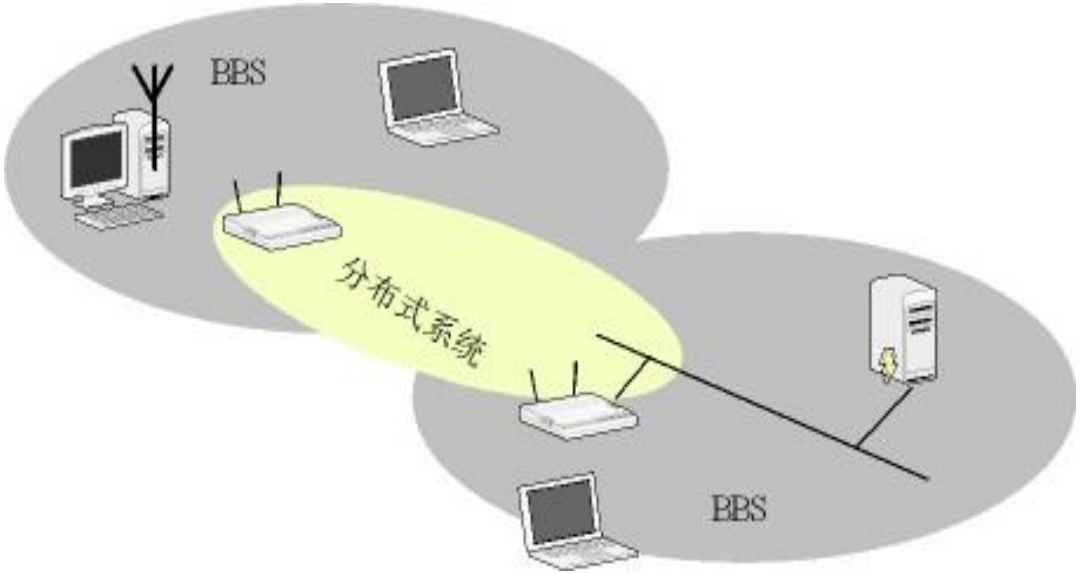
  (1)作为接入点，完成其他非AP的站对分布式系统的接入访问和同一BSS中的不同站间的通信联结。

  (2)作为无线网络和分布式系统的桥接点完成无线局域网与分布式系统间的桥接功能。

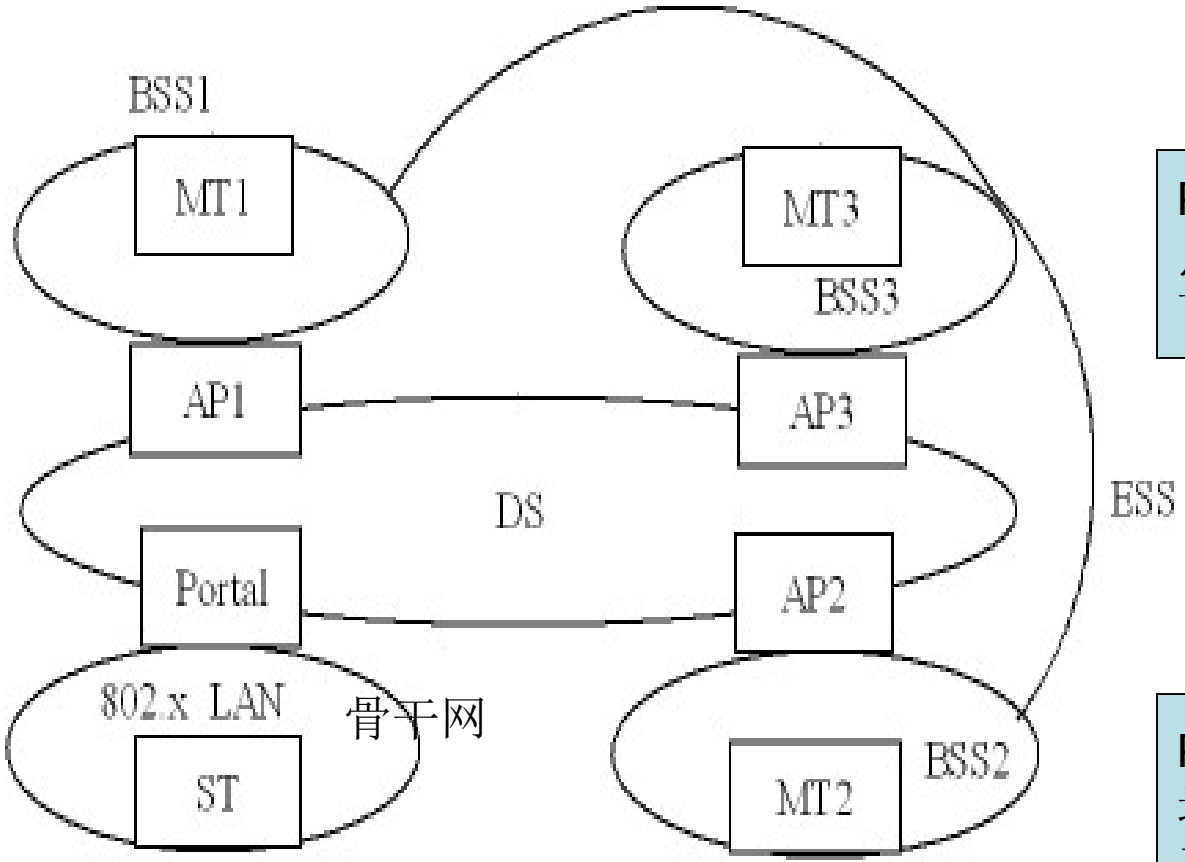
  (3)作为BSS的控制中心完成对其他非AP的站的控制和管理。

4．分布式系统DS

- 为了覆盖更大的区域，把多个BSA通过分布式系统连接起来，形成一个扩展业务区ESA，通过DS互相连接起来的属于同一个ESA的所有主机组成一个扩展业务组ESS。
- DS信道可以是有线或无线。



分布式系统通过入口(Portal)与骨干网相连



ST:固定终端；MT：移动终端；
接入点；Portal：入口

Portal是一个逻辑上的接入点，既可以是单一设备，也可以和AP共存于同一设备中

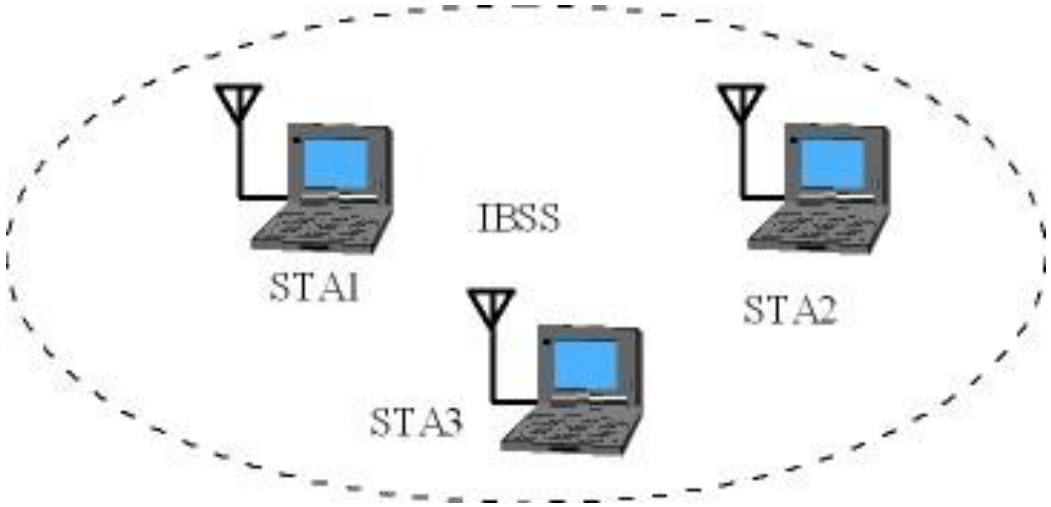
Portal必须能识别无线局域网的帧、DS上的帧、骨干网的帧，并能相互转换

3.2.2　无线局域网的拓扑结构

- 从物理拓扑分类看:单区网SCN和多区网MCN
- 从逻辑上看:对等式、基础结构式和线型、星型、环型
- 从控制方式方面来看:无中心分布式、有中心集中控制式
- 从与外网的连接性来看：独立WLAN和非独立WLAN

1．分布对等式拓扑

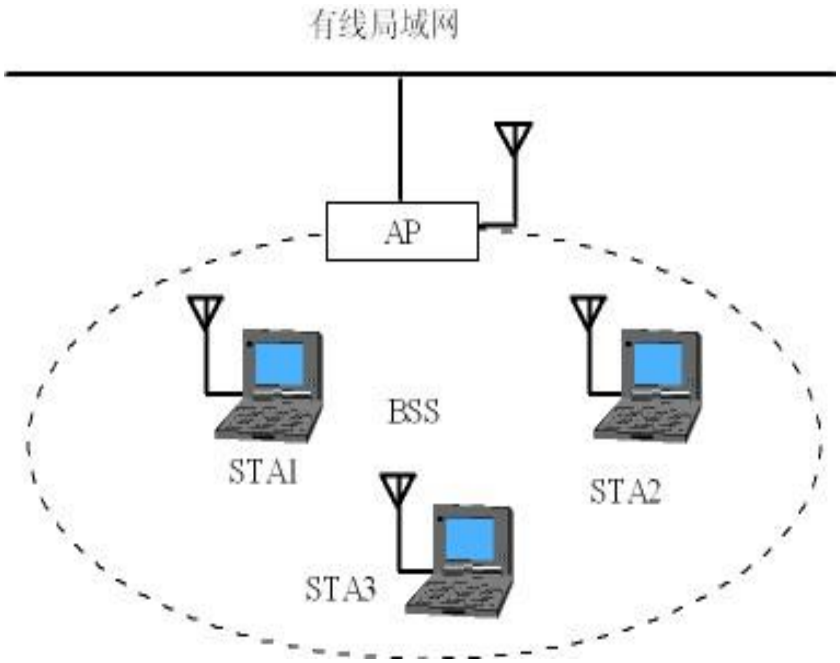
- 分布对等式网络是一种独立的BSS，它至少有两个站，是一种典型的、以自发方式构成的单区网。
- 该工作模式被称作特别网络或自组织网络(Ad Hoc Network)



- 只能直接通信
- 没有中继功能

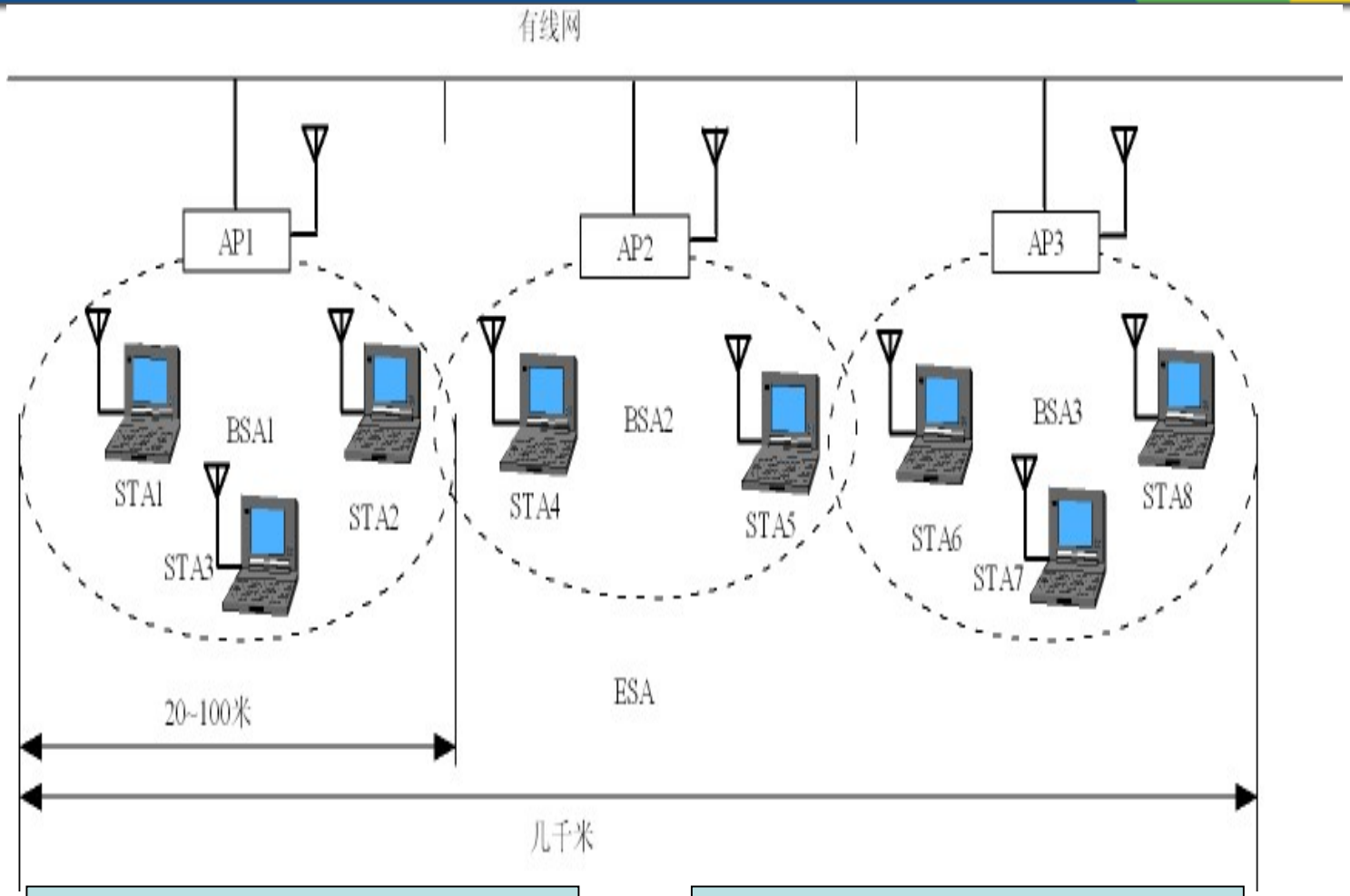
2．基础结构集中式拓扑

- 基础结构集中式式网络通过AP控制各站间的通信，抗毁性较差，AP复杂度较大。
- 但具有站点布局限制小、路由复杂性低、便于管理、易伸缩等优点。



- AP提供：
  - 到有线网络连接
  - 中继功能
- 站不能直接通信

3．ESS网络拓扑



BSA之间的移动称为散步或越区切换，是一种链路层的移动。

ESA之间的移动称为漫游，是一种网络层的移动。

4. 中继或桥接型网络拓扑

- 两个或多个网络(LAN或WLAN)或网段通过无线中继器、无线网桥或无线路由器等无线网络互连设备连接起来。
- 采用中继或桥接型网络拓扑是一种拓展WLAN覆盖范围的有效方法。

3.2.3 无线局域网的服务

- 与WLAN体系结构和工作原理密切相关的服务主要有两种类型:STA服务和分布式系统服务，这两种服务均由MAC层使用。
- IEEE 802.11标准中定义了九种服务，三种用来移动数据，其余六种是管理操作。

1. STA服务(SS)

- 由STA提供的服务被称为STA服务，存在于每个STA和AP中，包括：

Authentication

- 802.11支持多种认证模式，并允许对此进行扩充。
- 标准没有强制任何特定认证模式

De-authentication

- 一个原先已通过认证的站点离开网络时需要解除认证

Privacy

- 用来防止消息内容被非指定接收者阅读
- WEP（具体是RC4）

2. 分布式系统服务(DSS)

- 由DS提供的服务被称为分布式系统服务。在WLAN中，DSS通常由AP提供，包括：

关联(association)服务

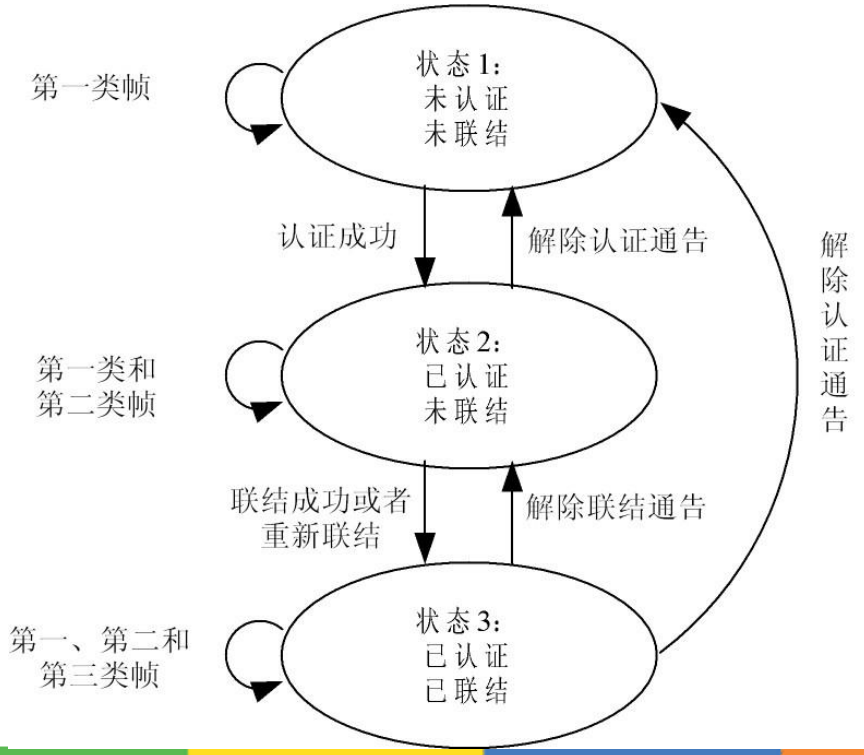
- Association
  - 站点必须与所在BSS的AP建立关联，AP才能将此信息通报给ESS内的其他AP，以便路由和帧的传递。
- Re-association
  - 关联可从一个AP转换到另为一个，允许站点从一个BSS移动到另一个。
- Disassociation
  - 去联通告可由AP或者与之关联的站点发出
  - MAC管理机制防止没通告的站点消失

分布式系统内的消息分发

- Distribution
  - 用在站点之间交换MAC帧
  - 从一个BSS的站点发送到另一个BSS的站点
- Integration
  - 当数据交换双方一个位于802.11LAN另一个位于非802.11LAN时
  - 涉及地址转换、传输介质变换逻辑和帧格式转换

3．服务之间的关系

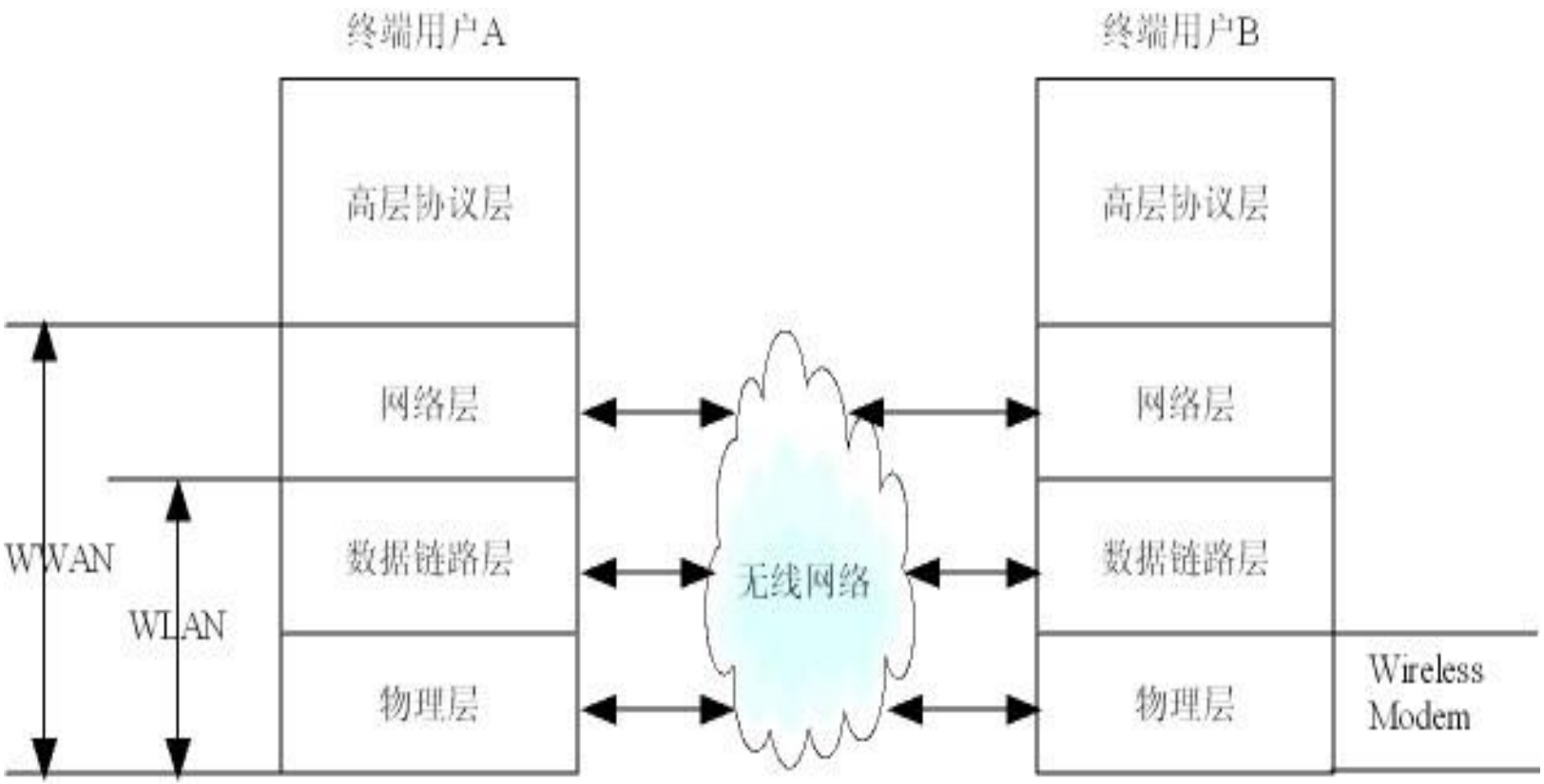
- 对于通过WM进行直接通信的STA均有认证状态(值为未被认证和已认证)和联结状态(值为未联结和已联结)两个状态变量。
- 这两个变量为每个远端STA建立了三种本地状态。



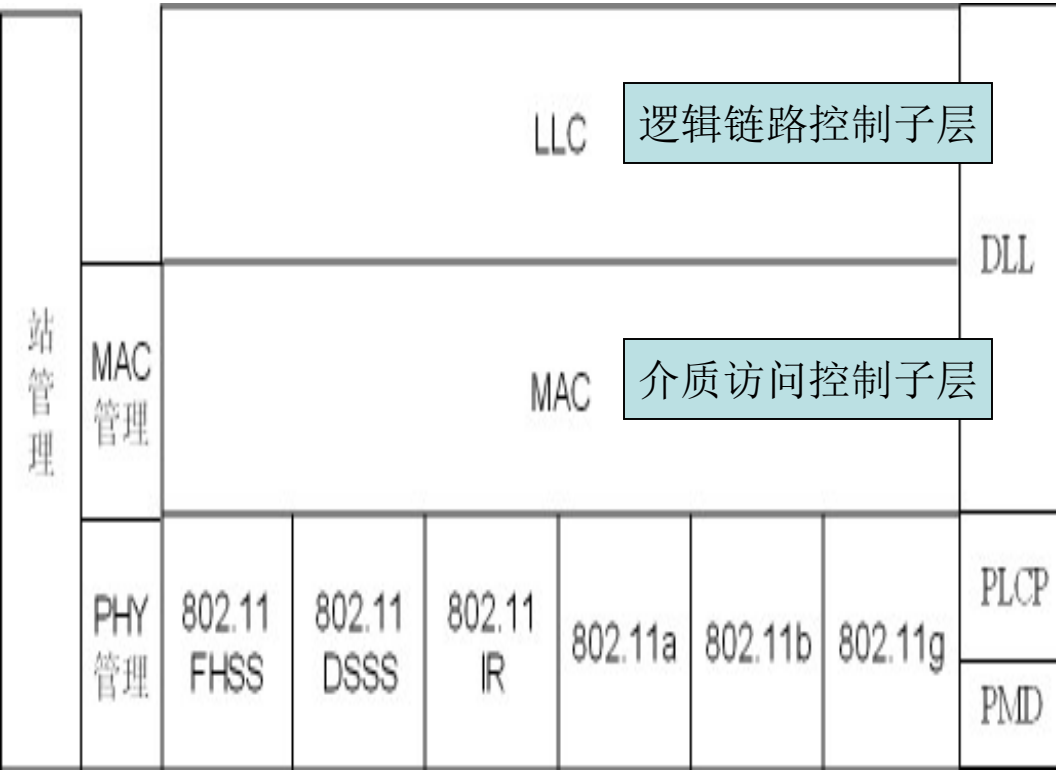
第3章 无线局域网

3.3 无线局域网的协议体系

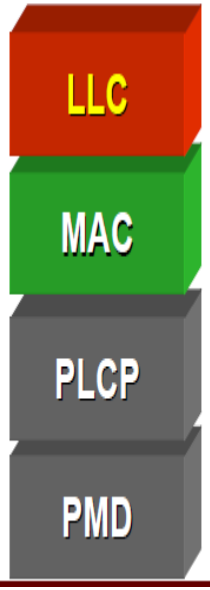
1. 无线网络逻辑结构



2. IEEE 802.11x无线局域网协议体系

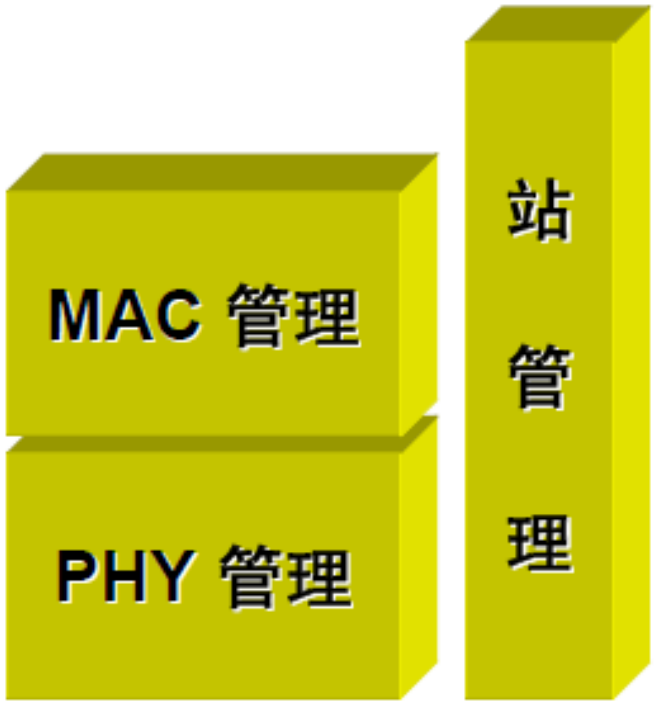


- 物理介质依赖子层（PMD）
  - 调制解调和编码/解码
- 物理层汇聚协议（PLCP）
  - 向上提供独立于传输技术的物理层访问点（SAP）
- 802.11介质访问控制层
  - 控制介质访问
  - 用户数据分段
  - 加密

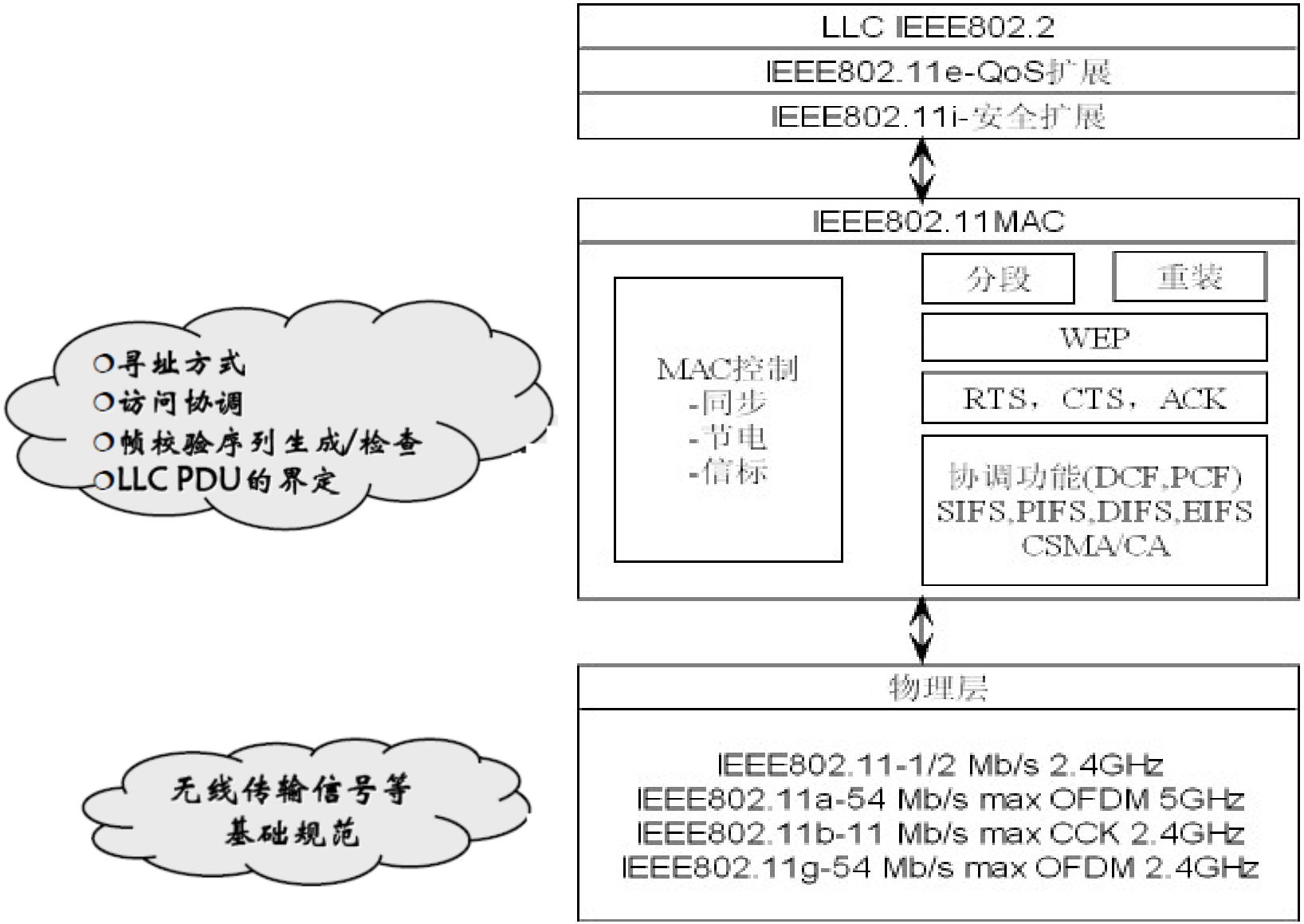


802.11 管理子层

- MAC管理
  - 站与AP的关联、站的漫游
  - 认证、加密、同步、能量管理
  - MAC管理信息库的维护
- PHY管理
  - 信道转换
  - 物理管理信息库的维护
- 站管理
  - 协同两个管理层
  - 高层功能

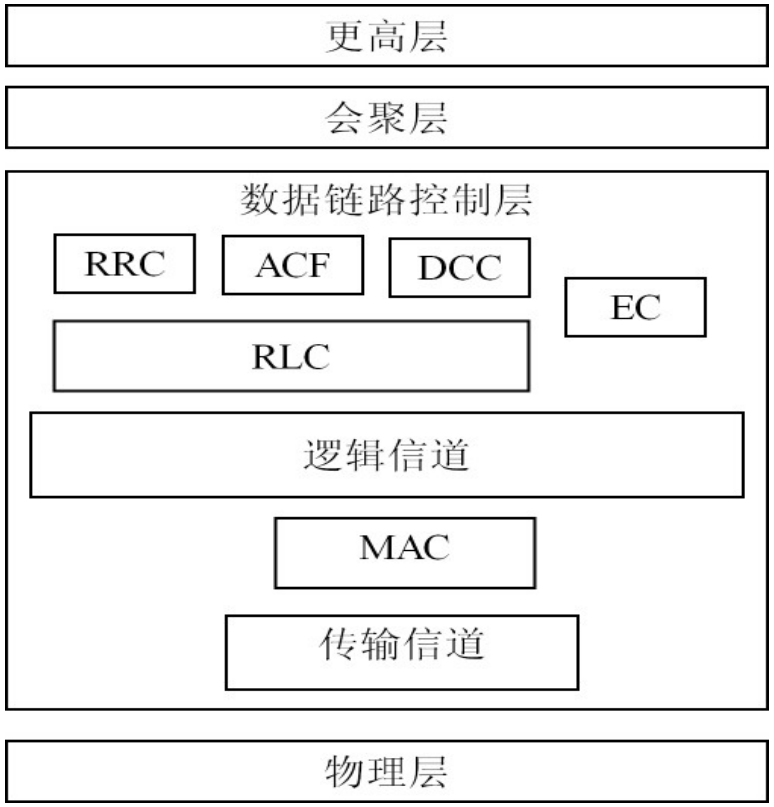


IEEE 802.11x标准较为完整的协议体系



3. HiperLAN协议体系

- 欧洲WLAN产业标准的代表是以HiperLAN为典型的宽带无线接入网(BRAN)，是以无线ATM(WATM)为基础的面向连接业务的标准。



无线链路控制协议（RLC）
无线资源控制：切换，频率，功率
联结控制功能：验证，密匙，联结
DLC连接控制：连接，多播，广播

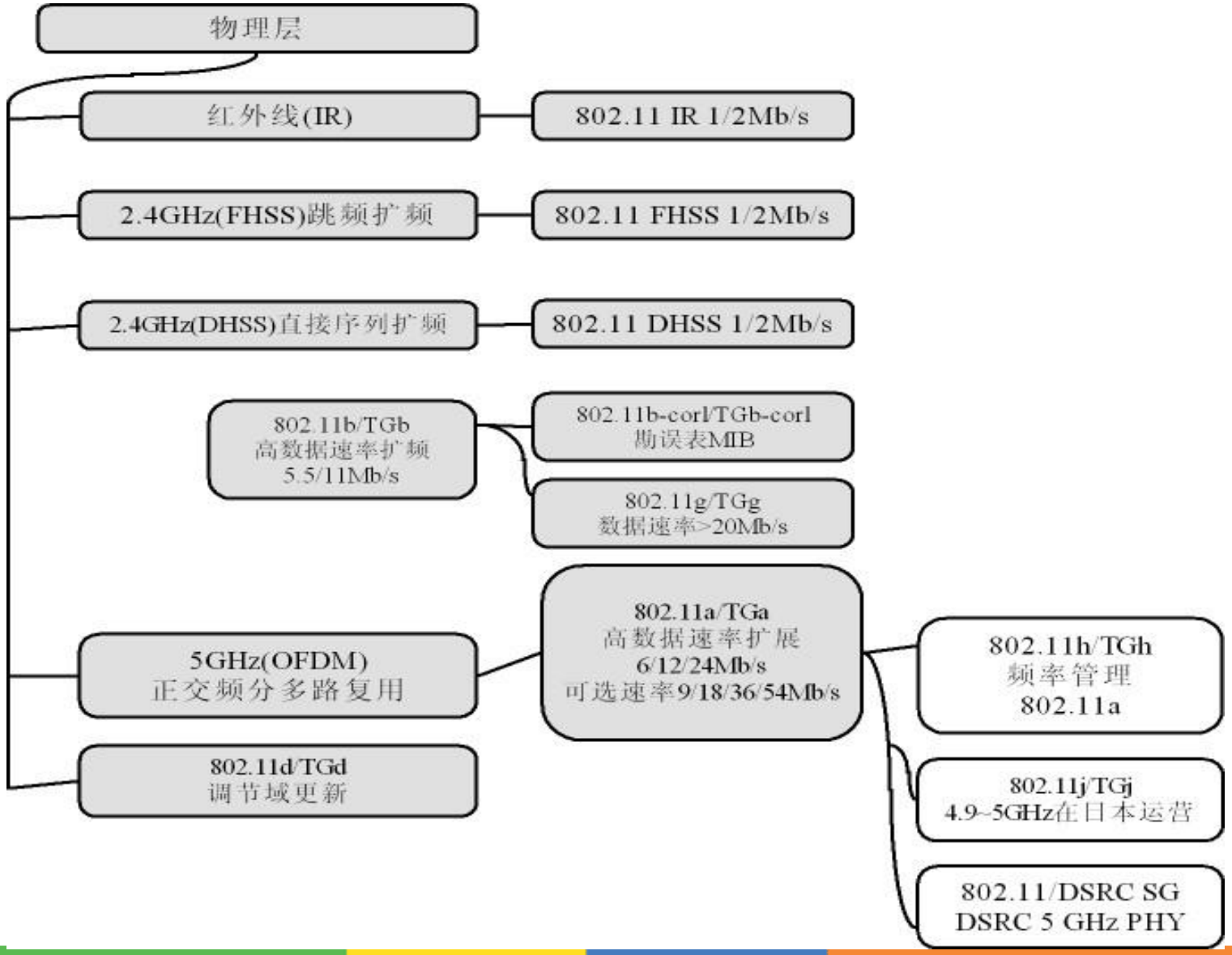
差错控制协议：选择重传ARQ
MAC协议：动态TDMA/TDD

4. Wi-Fi联盟的作用

- 在无线局域网标准的采纳和市场化推进中，Wi-Fi联盟(论坛)起到了主导作用。
- 无线以太兼容性联盟WECA1999年成立,后更名Wi-Fi联盟，建立了用于验证802.11b产品互操作能力的一套测试程序。
- 2004年起，验证的802.11b产品使用名称是Wi-Fi。
- Wi-Fi针对802.11a产品开发了一个认证过程，称为Wi-Fi5。
- Wi-Fi认证已扩展到802.11n。

第3章 无线局域网

3.4 IEEE802.11物理层



3.4.1 初始的IEEE 802.11物理层

- 工作在2.4GHz的ISM波段上的直接序列扩频，数据速率为1Mb/s和2Mb/s。
- 工作在2.4GHz的ISM波段上的跳频扩频，数据速率为1Mb/s和2Mb/s。
- 工作在波长介于850nm~950nm的红外波段上，其数据速率为1Mb/s和2Mb/s。

3.4.2 IEEE 802.11a

- 物理层
  - 采用OFDM（正交频分多路复用）技术
  - 工作频段是5GHz的ISM
  - 数据速率为54Mbps
  - 采用了54个频率
    - 48个用于数据
    - 4个用于同步控制

设计动机部分源于与欧洲的HiperLAN/2兼容

- MAC层与其他802.11标准相同

3.4.2 IEEE 802.11a信道结构

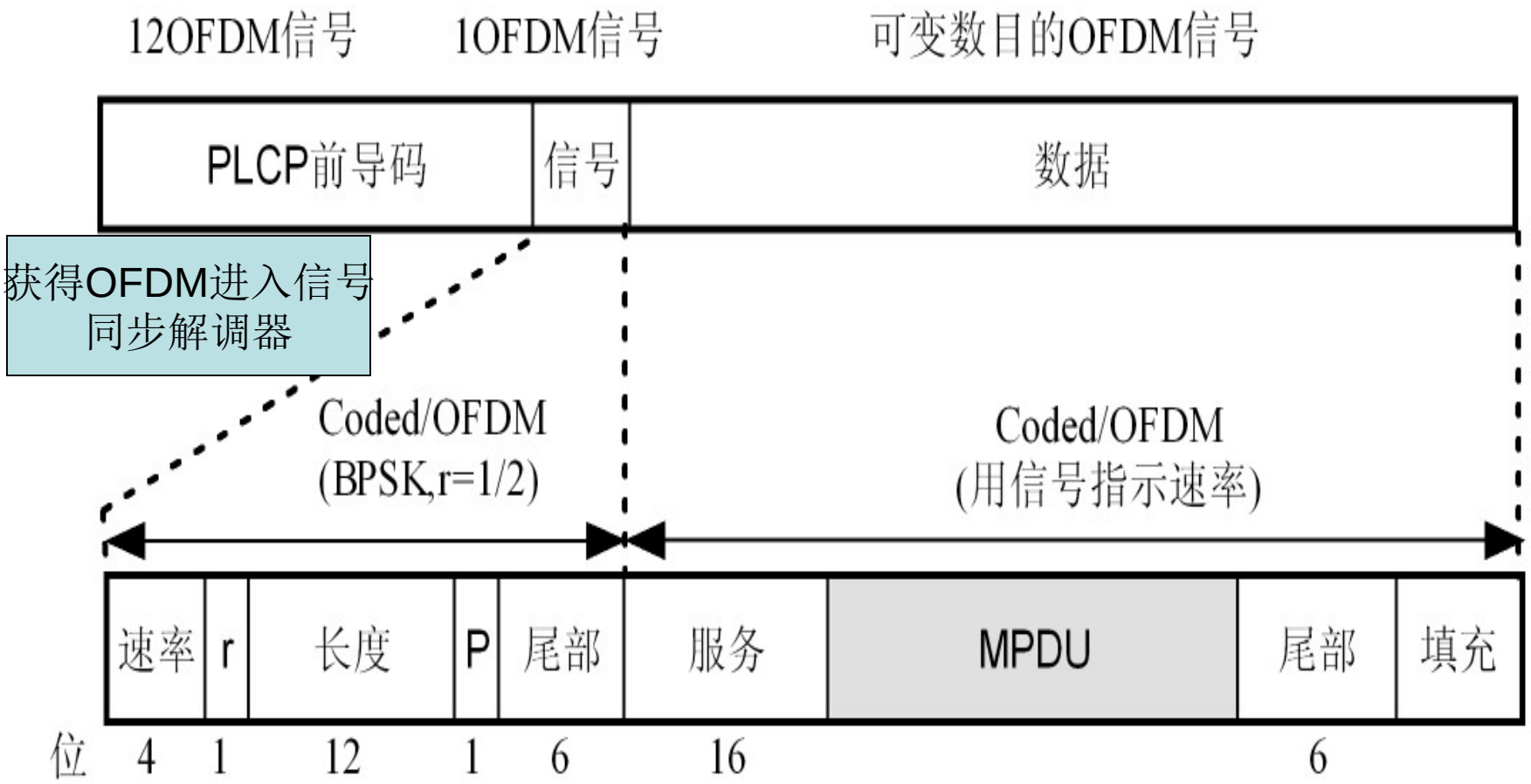
IEEE 802.11a使用非授权国家信息架构频段UNII。

- UNII-1频段(5.15~5.25GHz)用于室内；
- UNII-2频段(5.25~5.35GHz)用于室内或者室内；
- UNII-3频段(5.725~5.825GHz)用于室外。

3.4.2 IEEE 802.11a编码和调制

- IEEE 802.11a使用正交频分多路复用OFDM。
- OFDM也称多载波调制，在不同频率上使用多个载波信号，在每个信道上发送若干位，类似于FDM。
- 然而，在OFDM中，所有的子信道被指定给单个的数据源。

3.4.2 IEEE 802.11a帧结构



3.4.3 IEEE 802.11b

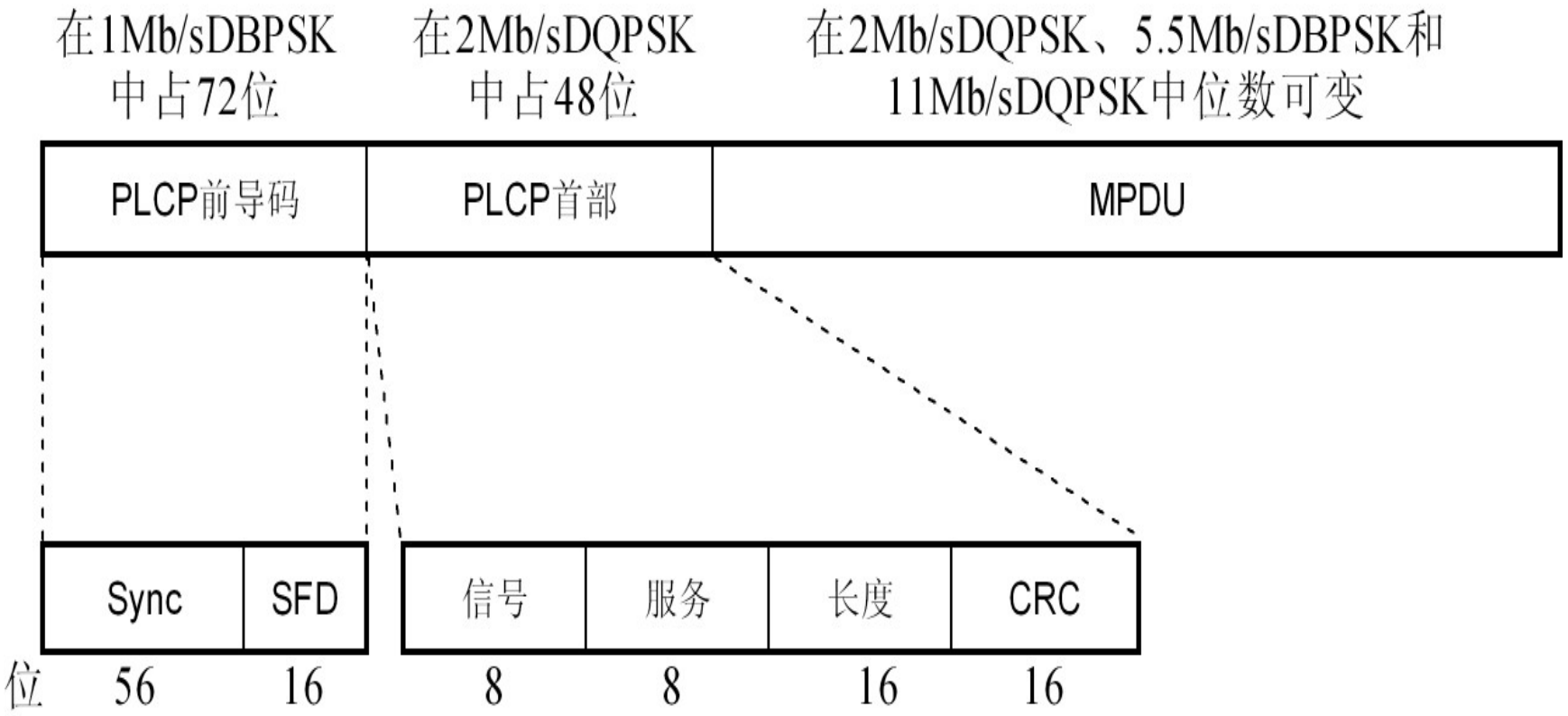
IEEE 802.11 DSSS模式的一个扩充

- 物理层
  - 采用HR-DSSS(高速率直接序列扩频)技术
  - 工作频段是2.4GHz
  - 数据速率为1、2、5.5Mbps/11Mbps
  - 覆盖范围是11a的7倍

使用补码键控(complementary code keying，CCK)调制模式，以获得可调整的数据速率

- 产品
  - 已经发展到第四或第五代
  - 大部分缺陷已经得到解决
  - 1~6Mbps的吞吐量能满足多种应用的需求

IEEE 802.11b物理层协议数据单元



3.4.4 IEEE 802.11g

- 2001被IEEE批准
- 2003正式发布

- 物理层
  - 采用OFDM（正交频分多路复用）技术
  - 工作频段是2.4GHz
  - 数据速率最大为54Mbps
- 兼备802.11a和802.11b的特点
- 比802.11a的功耗小、传输距离长、穿透力强

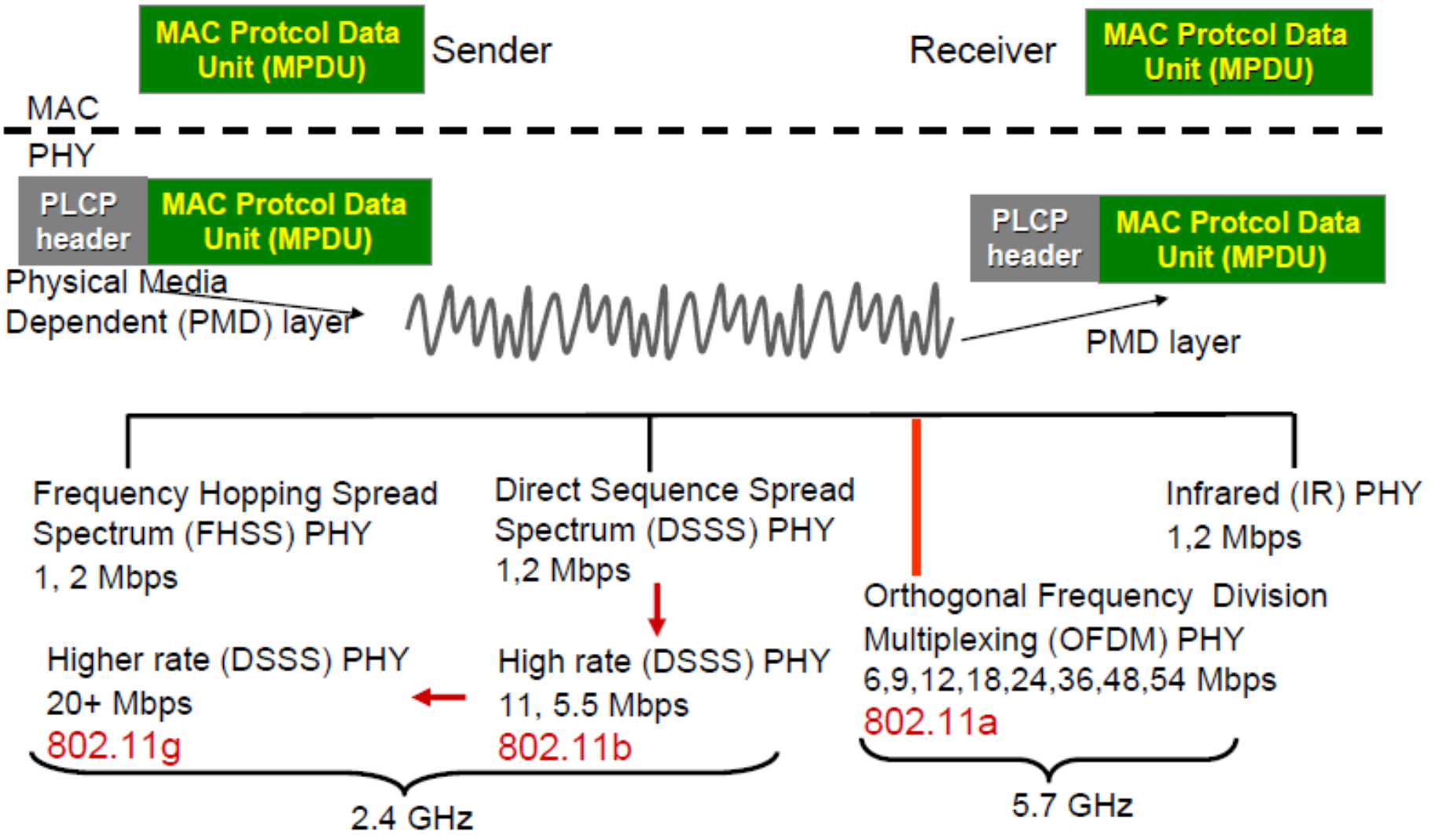
兼容802.11b，两者共存时
采取较低的802.11b传输速率

IEEE802.11g支持多种模式

数据率(Mb/s)	调制模式	数据率(Mb/s)	调制模式
1	DSSS	18	ERP-OFDM
2	DSSS	22	ERP-PBCC
5．5	CCK或PBCC	24	ERP-OFDM
6	ERP-OFDM	33	ERP-PBCC
9	ERP-OFDM	36	ERP-OFDM
11	CCK或PBCC	48	ERP-OFDM
12	ERP-OFDM	54	ERP-OFDM

3.4.5 IEEE 802.11n

- 工作于2.4GHz，5GHz
- 要求物理层数据率达到200Mbps
- 关键技术：MIMO，OFDM
- 2005年9月发布第一个标准


MAC Protcol Data Unit (MPDU)
Sender
Receiver
MAC Protcol Data Unit (MPDU)
MAC
PHY
PLCP header
MAC Protcol Data Unit (MPDU)
PLCP header
MAC Protcol Data Unit (MPDU)
Physical Media Dependent (PMD) layer
PMD layer
Frequency Hopping Spread Spectrum (FHSS) PHY
1, 2 Mbps
Direct Sequence Spread Spectrum (DSSS) PHY
1,2 Mbps
Infrared (IR) PHY
1,2 Mbps
Orthogonal Frequency Division Multiplexing (OFDM) PHY
6,9,12,18,24,36,48,54 Mbps
802.11a
Higher rate (DSSS) PHY
20+ Mbps
802.11g
High rate (DSSS) PHY
11, 5.5 Mbps
802.11b
2.4 GHz
5.7 GHz

第3章 无线局域网

802.11 MAC 设计目标及功能

- 802.11MAC设计目标
  - 单个MAC支持多个PHY
  - 抗干扰能力强
  - 处理隐藏节点问题
  - 支持限时服务、QoS
  - 重载下可扩展并且稳定
  - 提供节能模式
  - 提供私密性和访问控制

三大功能

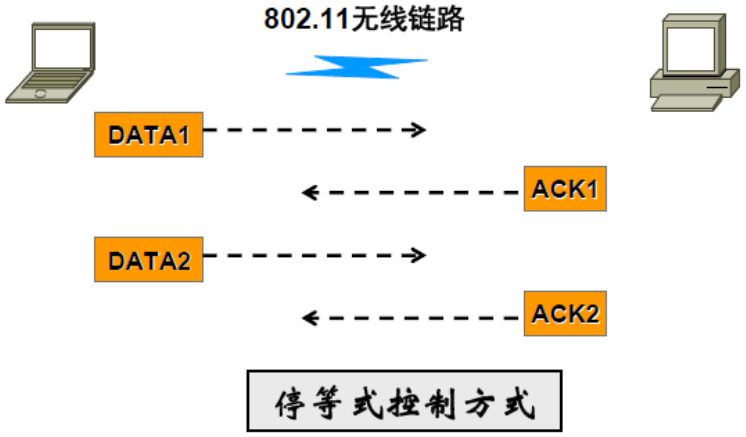
可靠数据传递

访问控制

安全

3.5.1 可靠的数据传送

- IEEE 802.11使用帧交换协议。当一个站点收到从另一个站点发来的数据帧时，它向源站点返回一个确认(ACK)帧。此交换被作为一个原子单元处理，它不会被其他站点发出的传送打断。如果因为数据帧被损坏或因为返回的ACK被损坏，源站点在一个短的时间周期中没有收到ACK，它会重发帧。
- 为了更进一步地增强可靠性，可以使用四帧交换。（RTS/CTS）



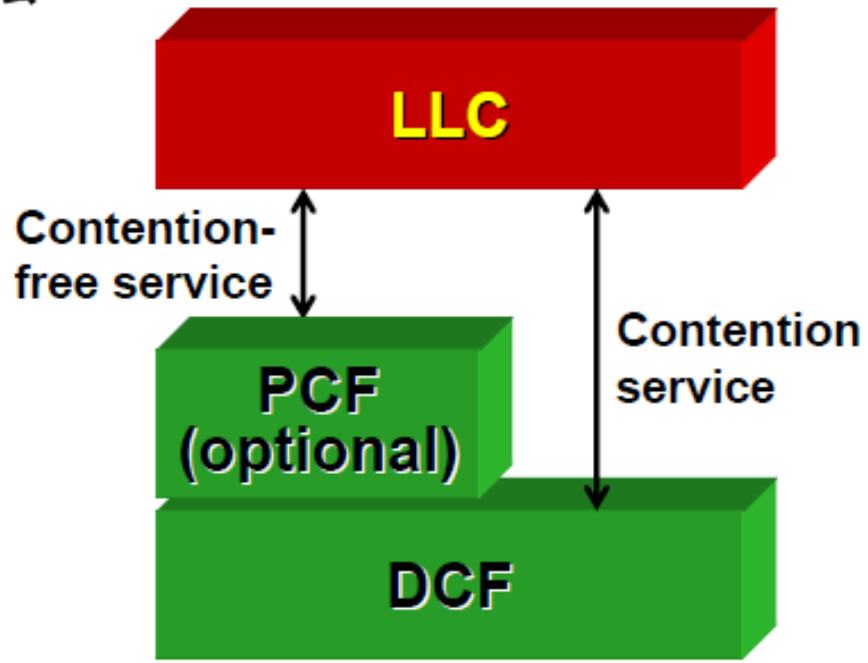
3.5.2 接入控制

- 基于CSMA/CA的强制基本功能
- 避免隐藏终端问题的可选功能

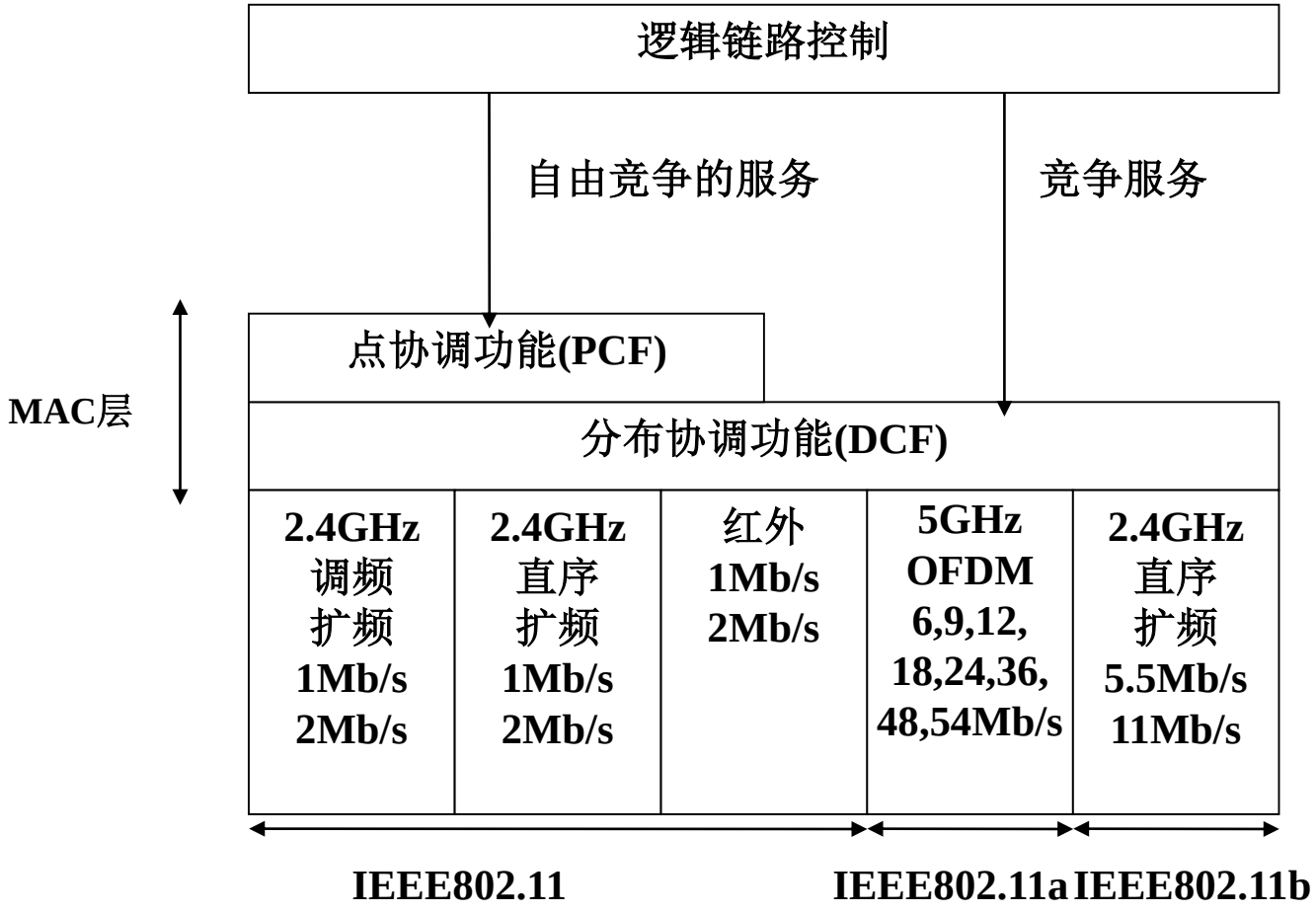
→ 分布式协调功能
异步传输服务

- 时限服务的无冲突polling方法

点协调功能
○异步传输服务
○时限服务



IEEE 802.11的协议体系结构



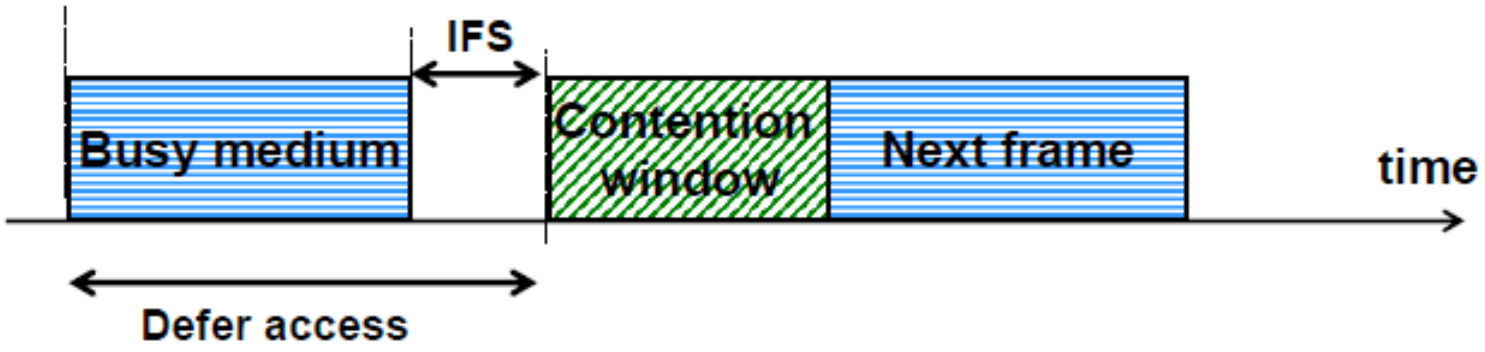
1. 分布协调功能

- DCF子层利用一个简单的载波监听多点接入CSMA算法：如果一个站点有一个MAC帧要发送，它监听媒体。如果媒体空闲，站点可以发送，否则，该站点必须等到当前发送已完成才能发送。

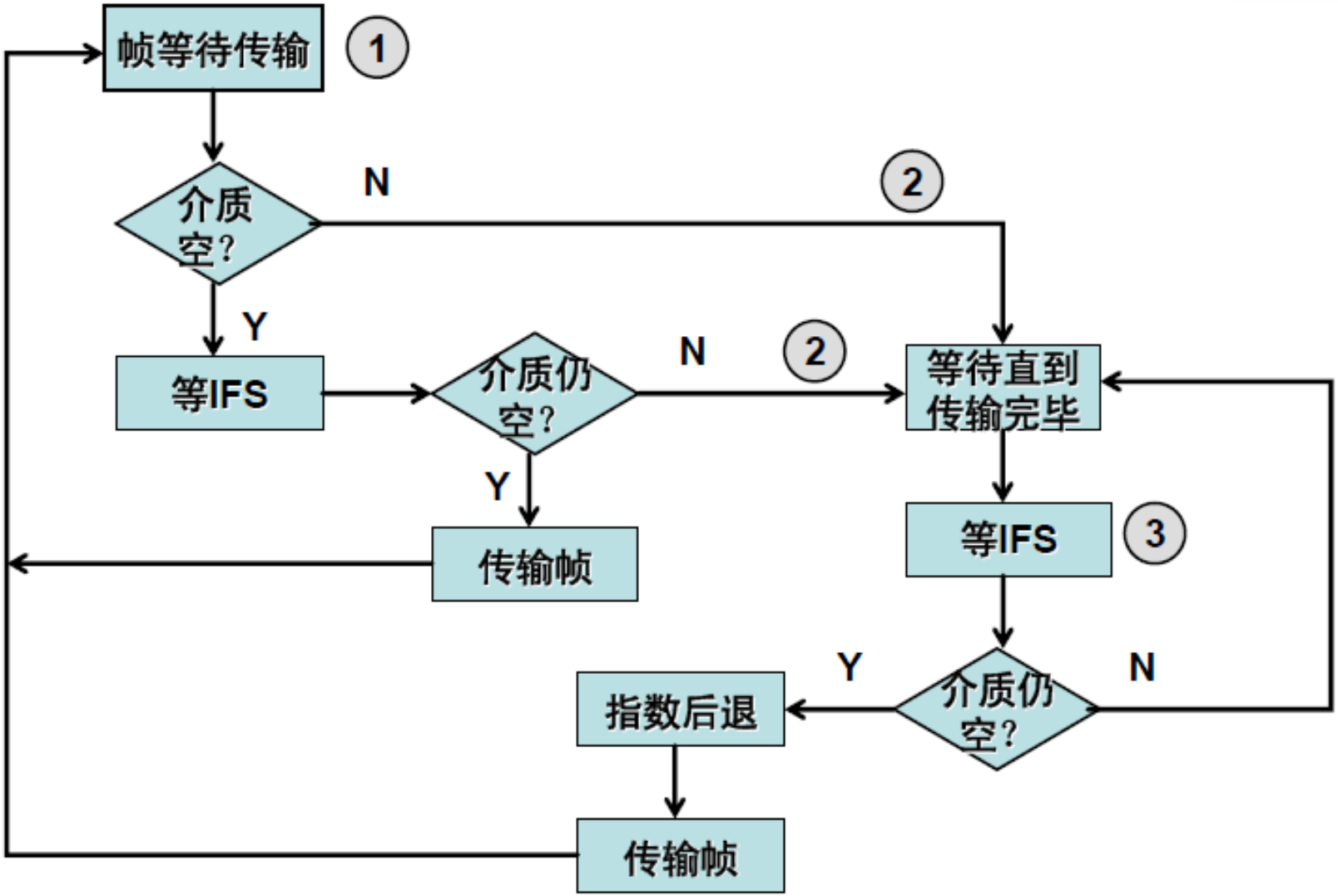
- 为确保此算法起到平滑和公平的作用，DCF包括一套相当于优先级模式的时延，用帧间间隔IFS实现。

CSMA/CA

- 载波侦听（CSMA）
  - 如果介质为空，则节点传输帧；
  - 如果介质为忙，则等待直到当前传输完全结束。
  - 上述规则并不总是适合（如：RTS/CTS）
- 冲突避免（Collision Avoidance）
  - 随机后退算法
  - 优先级确认协议



CSMA/CA 算法


帧等待传输
1
介质空?
N
2
Y
等IFS
介质仍空?
N
2
等待直到传输完毕
Y
传输帧
等IFS
3
Y
介质仍空?
N
指数后退
传输帧

退避过程（Backoff）

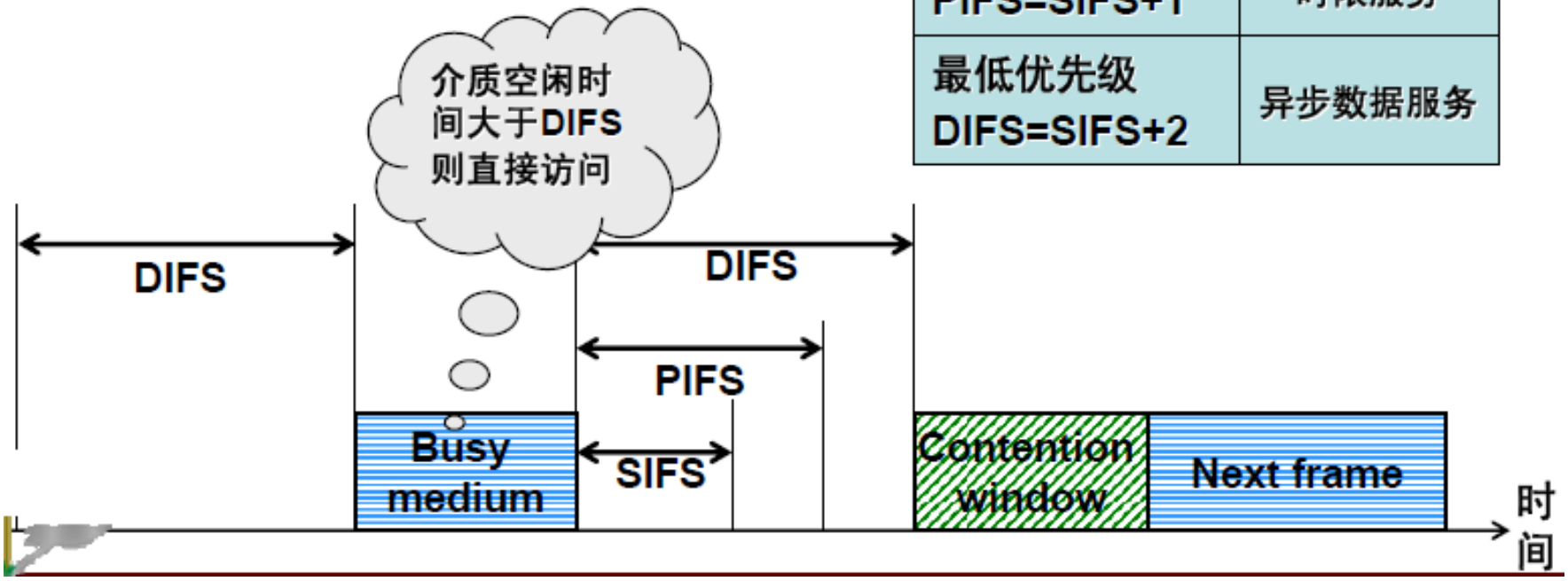
- 当空闲时间≥ IFS，立即传输
- 当介质忙，延迟直到当前传输结束 + IFS时间
- 开始随机后退过程
  - 选择一个随机数 (0, Cwindow)
  - 使用侦听确定每个时间槽是否有活动
  - 如果没有活动则减少 backoff时间
- 后退过程中介质为忙时挂起backoff过程
- 在当前帧传输结束后恢复后退过程

使用后退过程延迟发送的目的在于避免多个站点同时传输引起的冲突

三种IFS-控制等待时间的参数

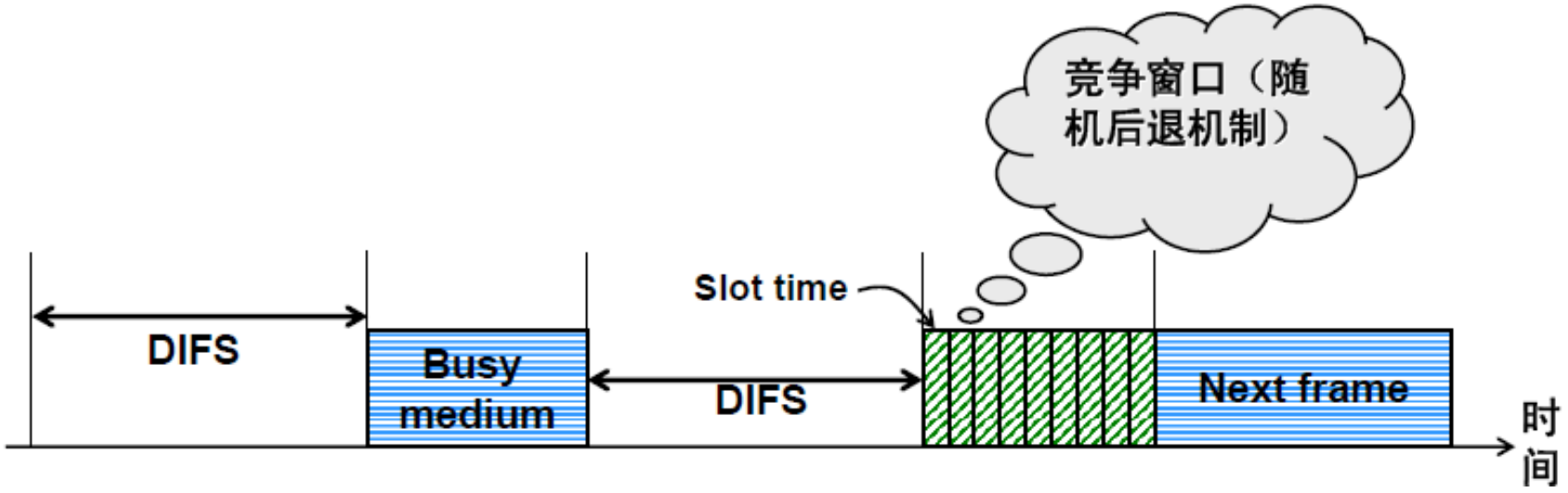
- 用不同的帧间隔来定义优先级
  - SIFS (Short IFS)
  - PIFS (PCF IFS)
  - DIFS (DCF IFS)

优先级	用途
最高优先级 SIFS	✧ACK ✧CTS ✧轮询响应
中等优先级 PIFS=SIFS+1	使用PCF 时限服务
最低优先级 DIFS=SIFS+2	异步数据服务



使用CSMA/CA的基本DCF

- 如果介质持续为空的时间大于DIFS，则节点可以立即访问介质。
  - 网络负载较轻时可缩短访问延迟
  - 网络规模增大时需要其他机制的协助
- 如果介质为忙，则等待一段随机时间。



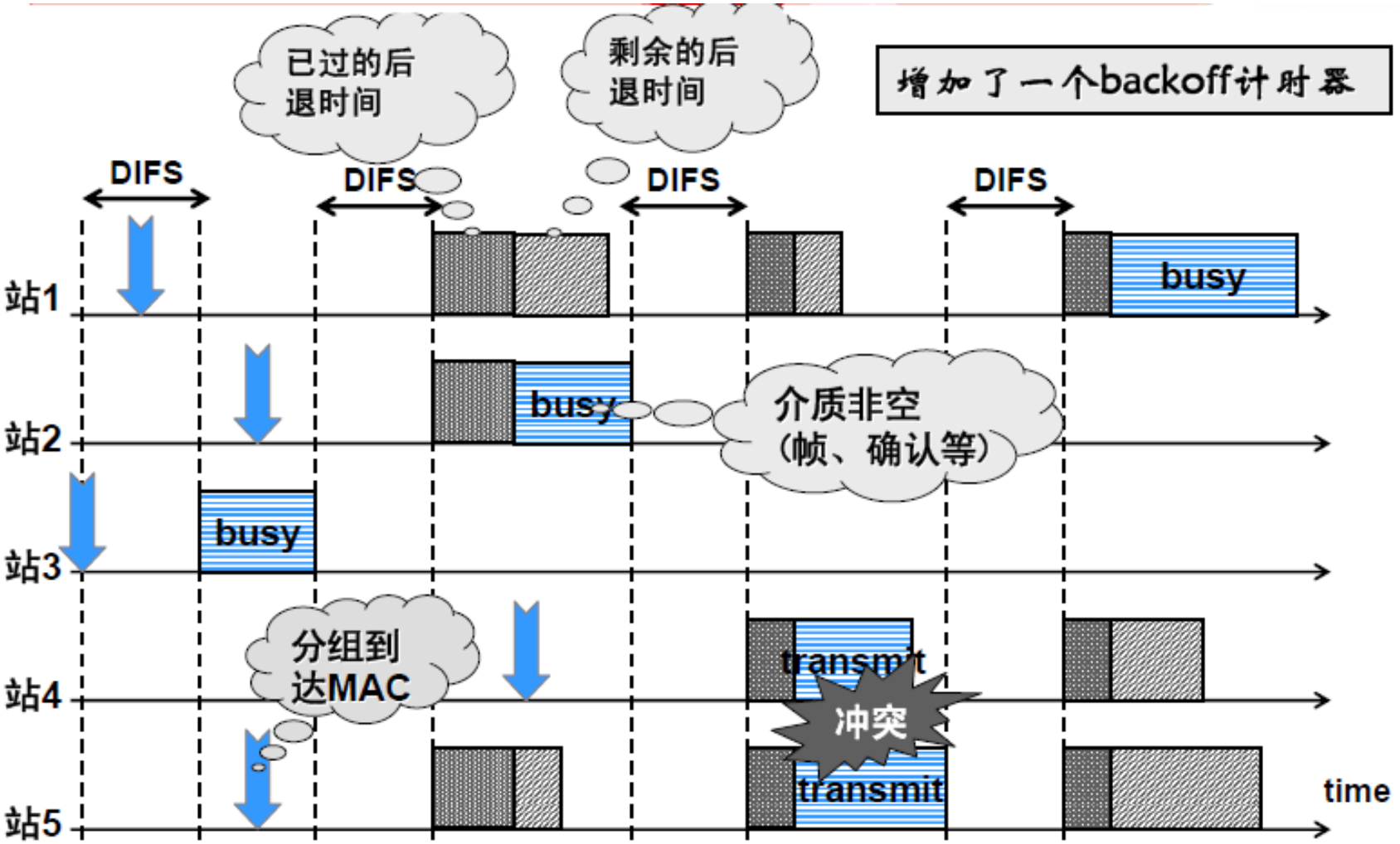
CSMA/CA公平性

- 如果介质忙，则节点必须等待DIFS，然后进入竞争阶段；
- 每个节点在竞争窗口中选择一个随机backoff时间，延迟这段时间访问介质；
- 如果随机等待时间过后，介质仍然为空，则节点可立即访问介质；
- 如果介质为忙？

那些已经等待过的节点：

- 重新开始下一轮竞争
- 每个节点在下一次竞争时具有同样的发送数据机会

802.11对CSMA/CA的改进



基本DCF特性

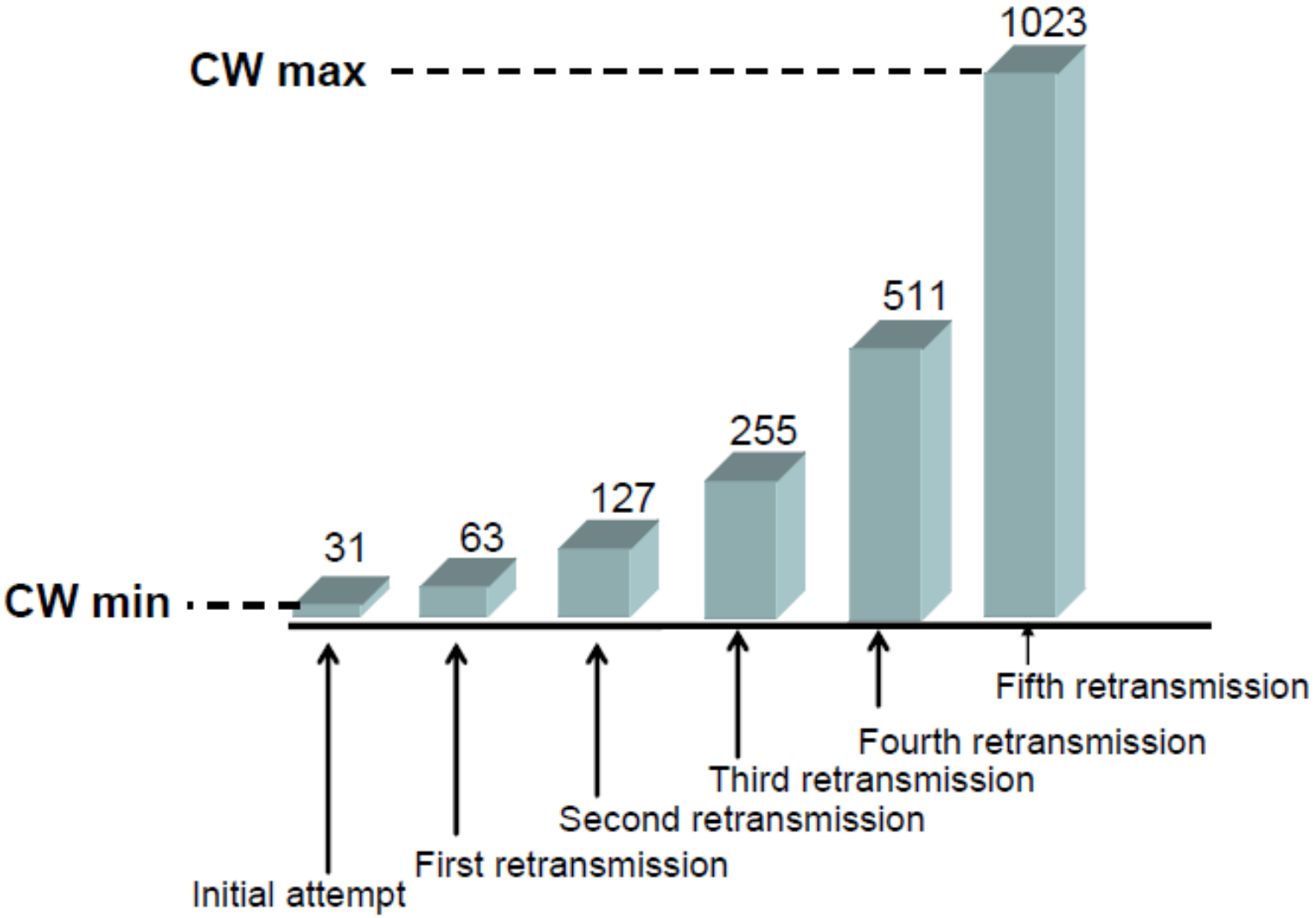
- 当网络负载大时
  - 竞争窗口越小，站点选择的随机值越接近。

    导致太多的冲突
- 当网络负载轻时
  - 竞争窗口越大，站点等待时间越长。

    导致不必要的延迟
- 指数后退算法
  - 竞争窗口初始化为某个最小值，发生冲突时加大窗口。直到达到最大值。

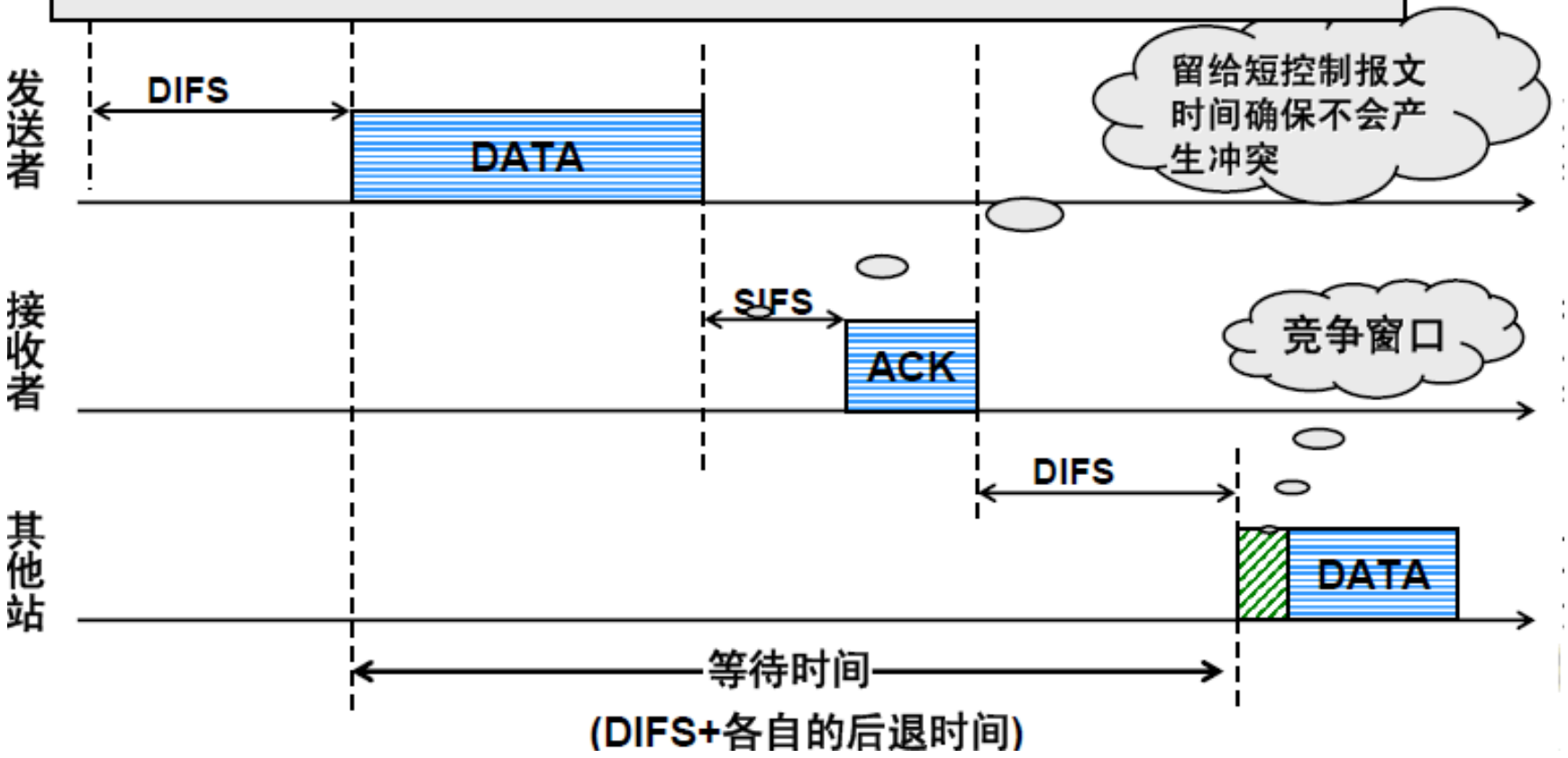
系统应该自我适应当前想发送的站点数目

竞争窗口


CW max
1023
CW min
31
63
127
255
511
Initial attempt
First retransmission
Second retransmission
Third retransmission
Fourth retransmission
Fifth retransmission

单播数据传送

- CSMA/CA + ACK
  - 接收方在CRC正确时立即返回ACK
  - 没有收到ACK则在随机后退时间后重传数据帧



带有RTS/CTS的扩展DCF

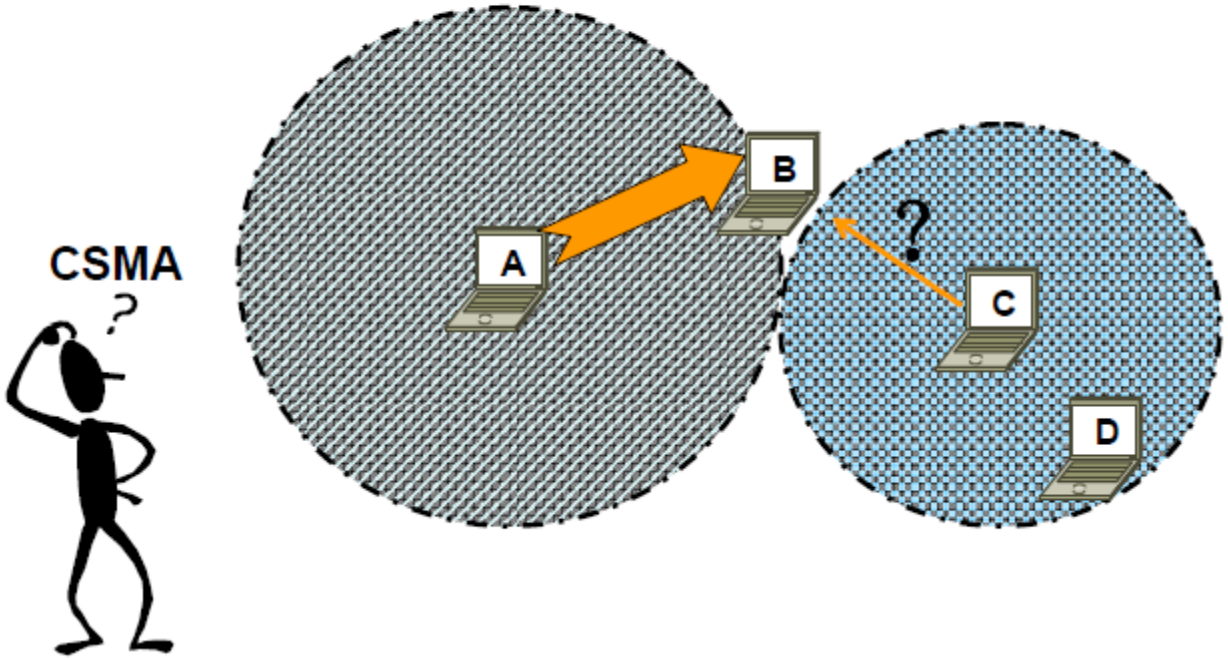
针对“隐藏节点”问题

- RTS/CTS机制
  - 机制的使用是可选的
  - 每个802.11节点必须实现该功能
- 明确预留信道
  - 发送者发送短的RTS（请求发送）
  - 接收者用短的CTS（清楚发送）
  - CTS为发送者预留了带宽同时通告所有的站点（包括隐藏的）
  - RTS和CTS长度很短，冲突的概率减少
- 避免“隐藏”终端冲突

- 接受者地址
- 发送数据帧时间
- 发送ACK时间

隐藏终端

假设：A正在向B传输数据，C也要向B发送数据。



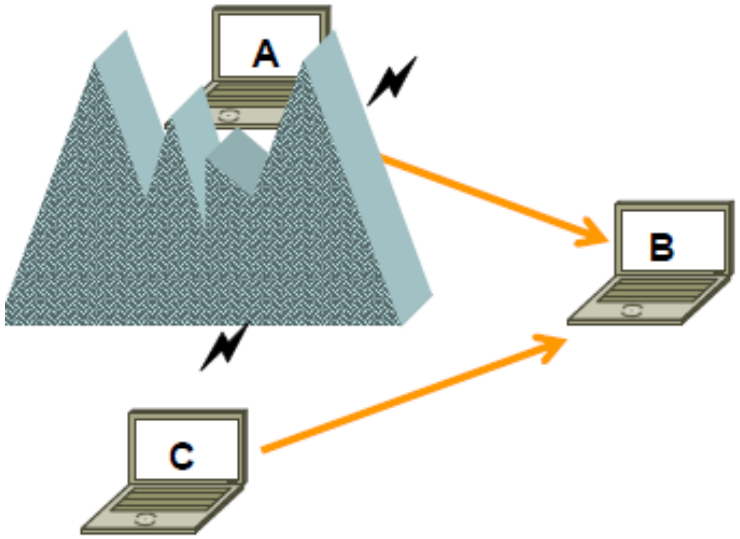
由于距离太远而导致一个站点无法检测到介质竞争对手的存在。

隐藏节点能够干扰接收端但不能侦听到发送端。

如何解决隐藏节点问题

- 隐藏终端： A和C互不知道
  - 障碍物导致信号衰减
  - 如果多于两个节点同时发送将在B处冲突

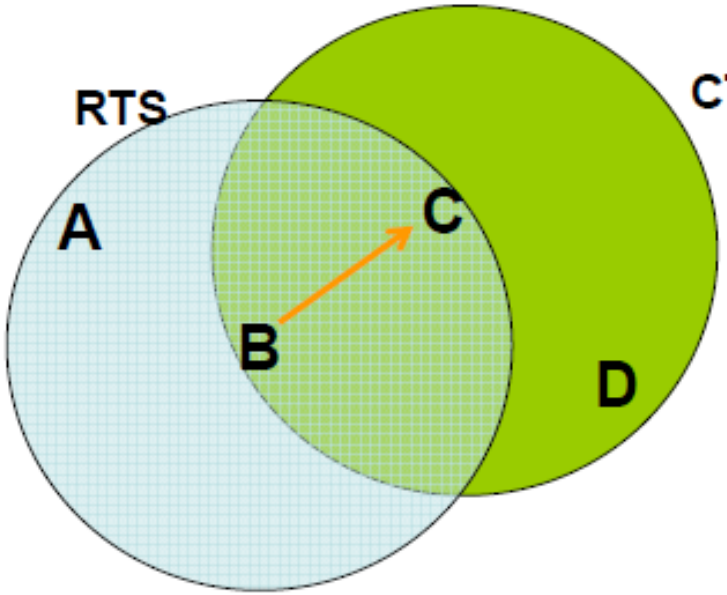
A和C发送长报文冲突将导致带宽的浪费



解决办法：通过短的控制分组预留带宽

用RTS/CTS解决隐藏节点问题

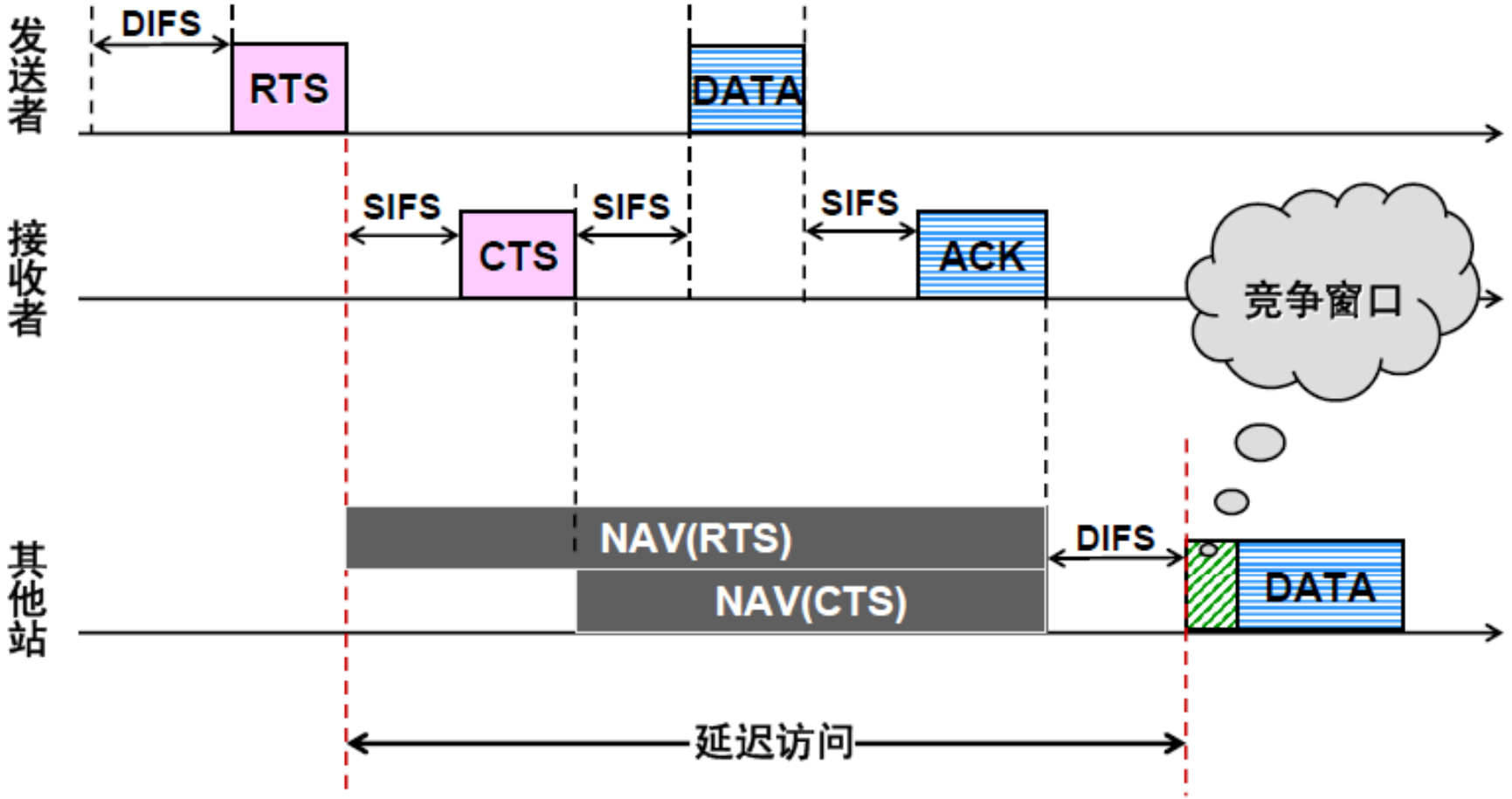
- ✧侦听RTS
- ✧等待足够长时间
- ✧被请求的站点以CTS响应



- ✧侦听CTS
- ✧等待足够长时间

侦听到RTS➔发送者在附近
侦听到CTS ➔ 接收者在附近

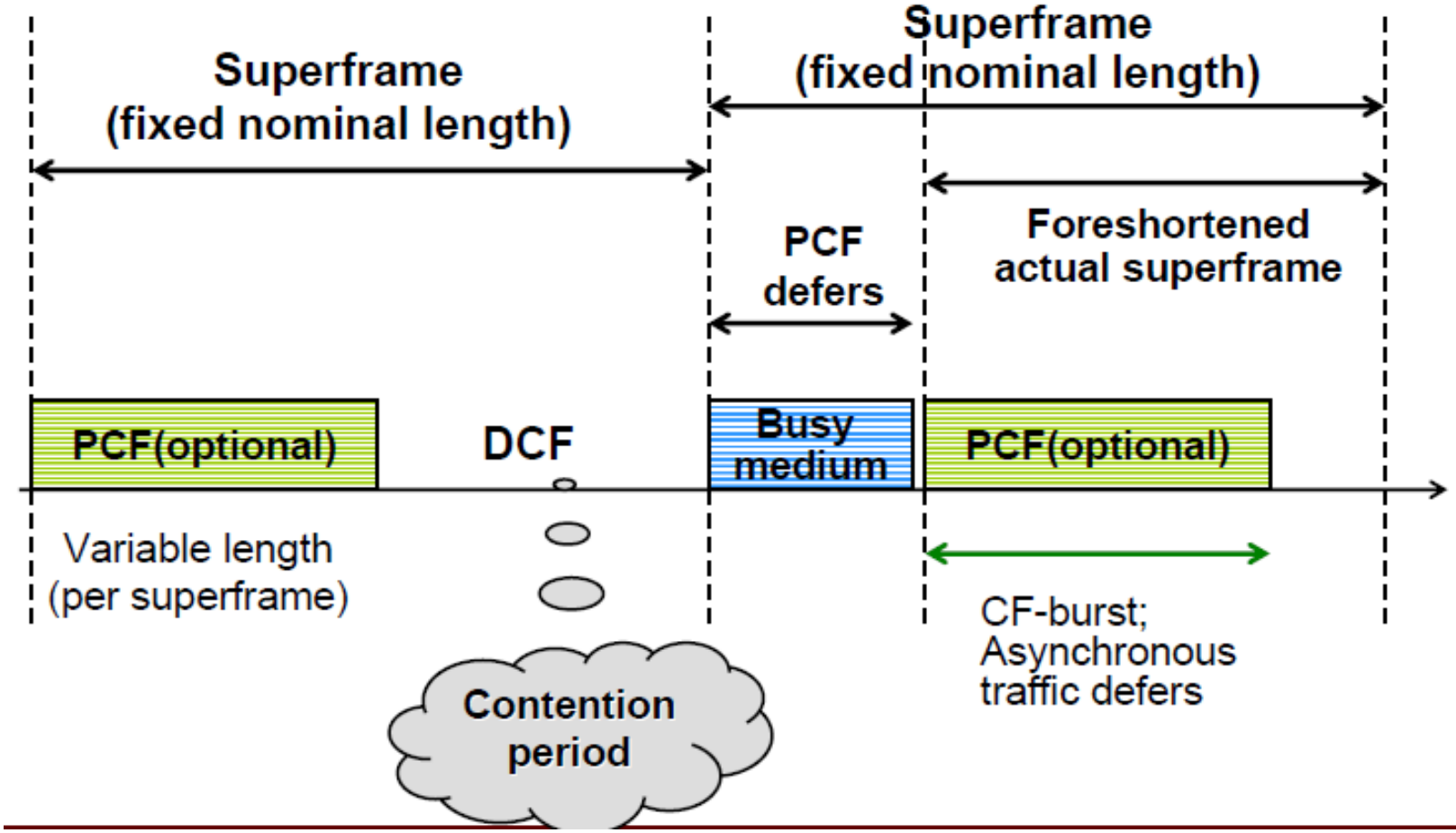
用RTS/CTS解决隐藏节点问题



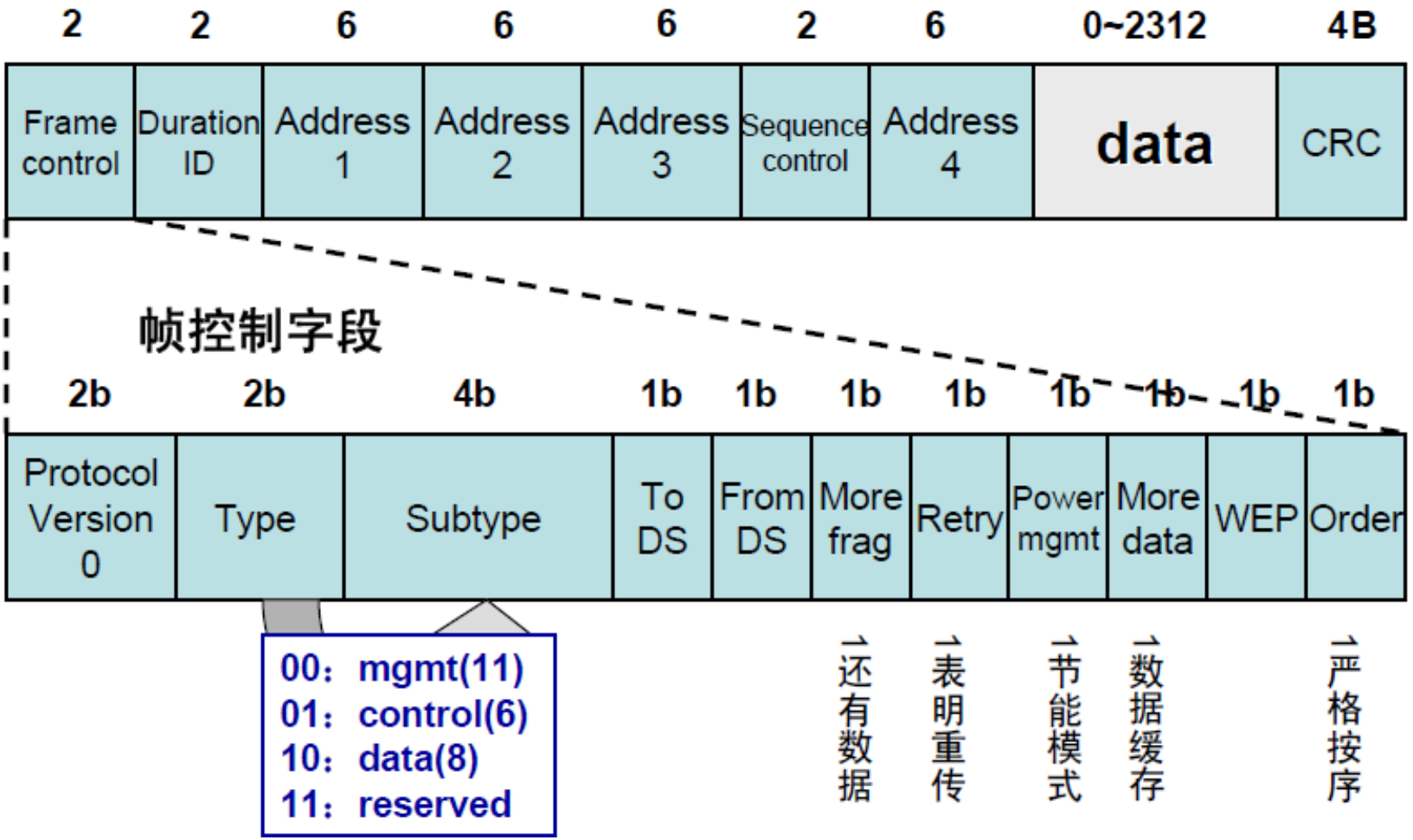
2. 点协调功能

- PCF是一个在DFC之上实现的替代接入方式。该操作由中央轮询主机(点协调者)的轮询组成。
- 点协调者在发布轮询时使用PIFS。由于PIFS小于DIFS，点协调者能获得媒体，并在发布轮询及接收响应期间，锁住所有的非同步通信。

超帧


Superframe
(fixed nominal length)
Superframe
(fixed nominal length)
PCF
defers
Foreshortened
actual superframe
PCF(optional)
DCF
Busy
medium
PCF(optional)
Variable length
(per superframe)
CF-burst;
Asynchronous
traffic defers
Contention
period

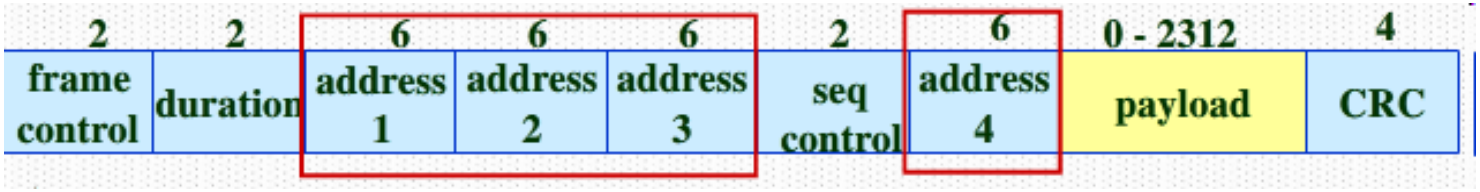
3.5.3 MAC帧

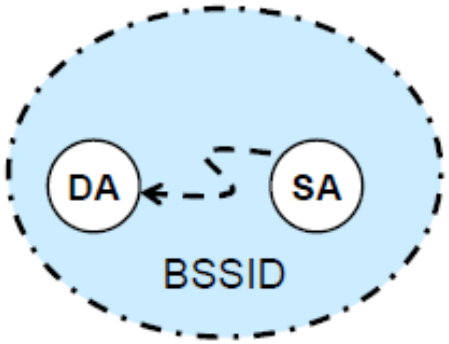

2 2 6 6 6 2 6 0~2312 4B
Frame control
Duration ID
Address 1
Address 2
Address 3
Sequence control
Address 4
data
CRC
MAC帧
帧控制字段
2b 2b 4b 1b 1b 1b 1b 1b 1b 1b 1b
Protocol Version 0
Type
Subtype
To DS
From DS
More frag
Retry
Power mgmt
More data
WEP
Order
帧控制域
00：mgmt(11)
01：control(6)
10：data(8)
11：reserved
还有数据
表明重传
节能模式
数据缓存
严格按序

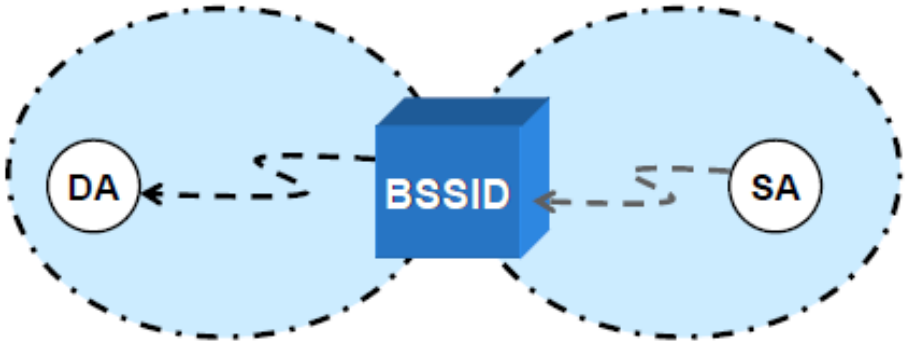
MAC帧基本字段

- Frame control
  - 两个字节的控制字段具有多种用途。
- Duration/ID
  - 表示下一个要发送的帧可能要持续的时间。
- Address 1~4
  - 每个地址的含义由Frame control中的DS解释。
- Sequence control
  - 序列号用来过滤掉重复帧。
- Data
  - 包含任意长度的数据（0~2312字节）。
- Checksum
  - 802.11采用4个字节的校验码。

地址字段







	to DS	from DS	Address1	Address2	Address3	Address4
Ad hoc	0	0	DA	SA	BSSID	--
接收自AP	0	1	DA	BSSID	SA	--
发送至AP	1	0	BSSID	SA	DA	--
DS内部	1	1	RAP	TAP	DA	SA
			物理接收者	物理发送者	逻辑发送者	逻辑接收者

MAC帧控制字段

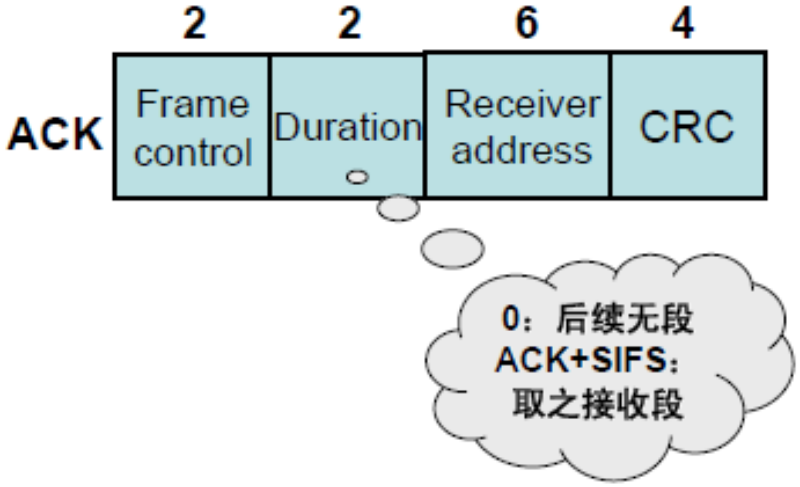
- More fragments
  - 1表示在当前的MSDU后面还有另一个fragment。
- Retry
  - 1表明当前帧是以前帧的重传。
- Power management
  - 表明站的模式：1表示节能；0表示活跃。
- More data
  - 一般来说该字段指示接受者发送者还有帧要传来。
- Wired equivalent privacy (WEP)
  - 该字段表明采用802.11标准的安全机制。
- Order
  - 1指示接受者必须严格按照顺序处理该帧。

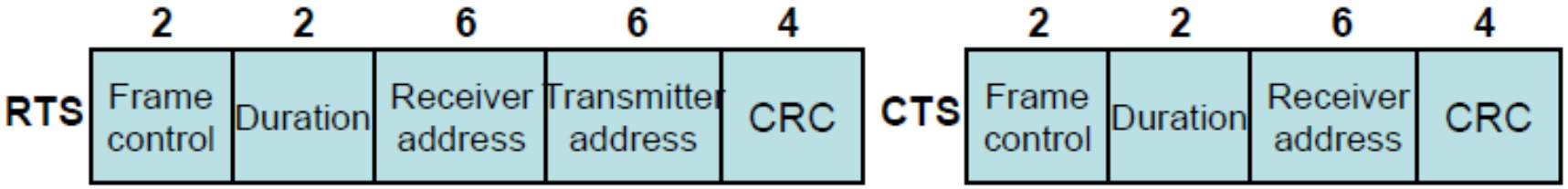
不同的MAC帧类型

1. 控制帧：6种子类型
2. 数据帧：8种子类型
3. 管理帧：11种子类型

控制帧

- ACK
  - 来自接收端的立即确认
  - 正确的数据帧
  - 管理帧
  - Poll帧
- RTS/CTS
  - 4次交换的前两个帧
  - 通知发送端和接收端附近的节点





控制帧（续）

- Power save-poll
  - 发自某个站
  - 请求一个缓存帧
- CF-end
  - 通告无竞争阶段的结束
- CF-end + CF-ack
  - 确认CF-end

- 节能模式
  - AP可以指示一个移动站进入睡眠状态，直到由AP或者用户显式唤醒为止
  - 在移动站睡眠期间，AP必须负责把所有发给该站点的帧全部缓存起来

数据帧

- 第一类：携带用户数据（4）
  - Data
    - 最简单的数据帧。用于无竞争/有竞争阶段
  - Data + CF-ack
    - 仅用于无竞争阶段。除了携带数据外，该帧还携带对刚收到数据的确认。
  - Data + CF-poll
    - 被AP用来传递数据给移动站，也可用于请求移动站点发送一个可能被缓存的数据帧。
  - Data + CF-ack + CF-poll
    - 把上述功能结合在一个帧中

数据帧（续）

- 第二类：没有任何数据（4）
  - Null function（no data）
    - 携带能量管理帧中由AP指示站点进入节能状态
  - CF-ack （no data）
  - CF-poll （no data）
  - CF-ack + CF-poll （no data）

} 意义同前

管理帧

- 基本功能
  - 处理移动站点与AP之间的通信—控制移动环境所需要的机制
    - Synchronization：支持寻找一个无线站点、同步内部时钟、产生beacon信号。
    - Power management：为power conservation而不丢失帧控制发送器活动，例如定期睡眠、缓存、
    - Roaming： 加入一个网络（关联），改变接入点、扫描接入点。

管理帧-关联操作帧

- Association request
  - 移动站点向BSS内的AP请求关联
- Association response
  - AP接受移动站点的关联请求
- Re-association request
  - 当移动站点离开当前BSS而进入另一个BSS时必须向新BSS的AP请求关联
  - 新AP据此和老AP协商数据帧的转发
- Re-association response
  - 新AP接受移动站点的关联请求
- dissociation

✧是否加密
✧是否轮询

管理帧-获取BSS及站点信息帧

- Probe request
  - 用来获取AP或者其他站点的信息
- Probe response
  - 对上述请求的响应

- BSSID
- 时间戳（用于同步）
- 流量指示图（sleep模式）
- 能量管理和漫游

- Beacon
  - AP建立时序同步功能 而准定期发送的管理帧
- Announcement traffic indication message
  - 通知其他站点有缓存的数据

管理帧-安全管理帧

- 802.11提供了两类认证
  - Open system authentication
    - 双方同意交换数据，没有任何安全保障；只需要交换各自身份
  - Shared key authentication
    - 需要双方共享密钥；该密钥用来确保双方的身份
- 安全帧
  - Authentication
    - 站点之间交换信息和采用多种模式
  - De-authentication
    - 通知其他站点终止当前的安全通信。

第3章 无线局域网

3.6 其他IEEE802.11标准

- IEEE 802.11c关注桥操作，连接两个具有类似或相同MAC协议的局域网设备。
- IEEE 802.11d是作为管理范畴(regulatory domain)更新被提及。
- IEEE 802.11e对MAC层作了一些修正以改进服务质量并解决了一些安全问题，并用包括优先级的HCF替代PCF和DCF。
- IEEE 802.11f致力于解决在来自多个厂商的接入点(AP)之间的互操作能力问题。
- IEEE 802.11h处理频谱和功率管理问题，特别是欧洲5GHz频带部分为军用。

其他IEEE802.11标准(续)

- IEEE 802.11i定义了MAC层的安全和认证机制，解决WEP缺陷。
- IEEE 802.11k定义了无线资源测量，增强了其功能，为较高层提供了无线和网络测量的机制，包括AP质量位置报告，信道信息，信道接入统计信息。
- IEEE 802.11m是一个纠正标准中编辑的和技术问题的工作组正在进行着的活动。
- IEEE 802.11n正研究对物理层和MAC层的增强范围，以改进信息流通量。

第3章 无线局域网

3.7.1 安全威胁War-Xing

- WLAN传输信号可以被覆盖范围内任意接收机收到
- War-Driving：通过驾驶车辆在目标区域往返进行AP探测
- War-Biking：通过骑车等方式在目标区域往返进行AP探测
- War-Walking：通过徒步等方式在目标区域往返进行AP探测
- 钓鱼Wi-Fi

3.7.2 IEEE 802.11 安全标准-WEP

初始标准使用连线对等保密(WEP)

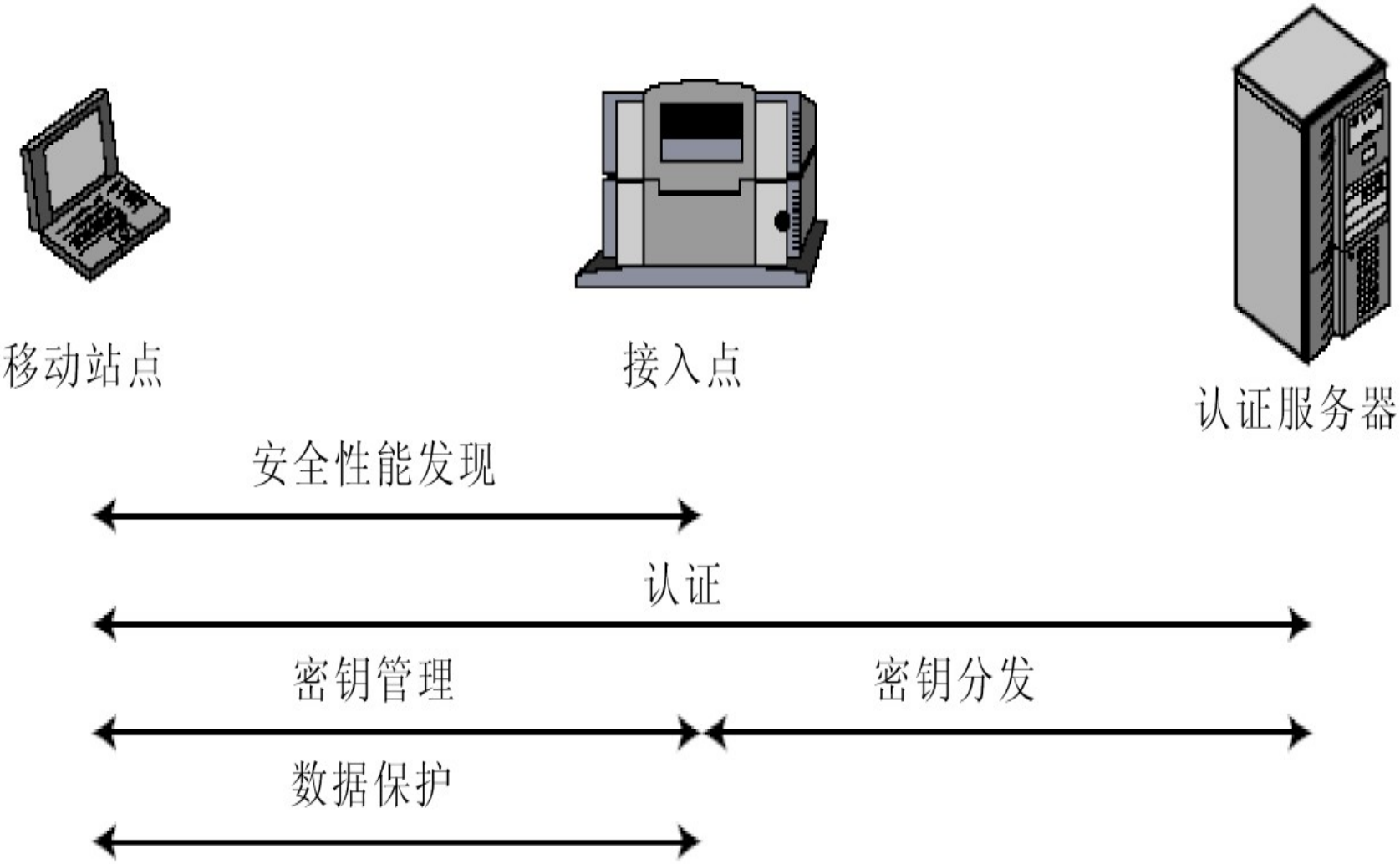
- 在链路层采用RC4对称加密技术
- 提供了40位和104位长度的密钥机制
- 钥匙是静态的，要手工维护，扩展能力差
- 易受攻击，缺乏密匙管理而大量重复使用

3.7.2 IEEE 802.11 安全标准—WPA

IEEE 802.11i定义Wi-Fi保护接入（WPA）

- 继承了WEP基本原理，又解决了WEP缺点。
- 包含了认证、加密和数据完整性校验三个组成部分，是一个完整的安全性方案。
- 要求使用认证服务器AS并定义了一个更为健壮的认证协议。

802.11i的各操作阶段



第3章作业（作业3）

1 简述无线局域网分布式系统的概念和作用。

2 IEEE 802.11定义了哪几种服务？并作简单介绍。

3 无线局域网AP承担哪几类角色？各自具有什么功能？

4 说明IEEE 802.11 a/b/g/n物理层技术的区别。

5 IEEE 802.11 MAC层提供哪两类接入控制？两者区别是什么？

6 说明IEEE 802.11如何解决隐藏节点问题。

7 简述IEEE 802.11CSMA/CA算法过程。

8 IEEE 802.11提供哪几种帧间隔？各自具有什么作用？

End