无线局域网的结构与实现

陈美娜

厦门联创微电子股份有限公司

WLAN相比有线局域网的优点

- 移动性好。在服务区域，无线局域网用户可以随时地访问信息
- 设备安装快速，简单，灵活：无线局域网消除了布线地繁琐工作，网络可遍及有线不能到达的地方
- 减少投资。无线局域网减少了布线的费用，应用在频繁移动和变化的动态环境中，投资回报高
- 扩展能力强。无线局域网可以组成多种拓扑结构，容易从少数用户的对等网络模式扩展到上千用户的结构化

WLAN与有线网络的区别

- 有线网络

传输媒体一般有双绞线，同轴电缆，光缆

其中的以太网采用的标准是IEEE802.3（CSMA/CD总线式媒体访问控制协议及相关的物理层规范）

n WLAN

传输媒体主要有无线电波和红外线，实现技术：DSSS和FHSS

现在通常有四种商业无线局域网方案供人们选择

1）802.11WLAN：被设计称大概在300英尺的范围内提供无线连接服务。

2) HomeRF:主要针对家庭无线局域网，支持语音和数据。

3）蓝牙技术：一种短距离无线通讯技术，以低成本的短距离无线连接为基础。

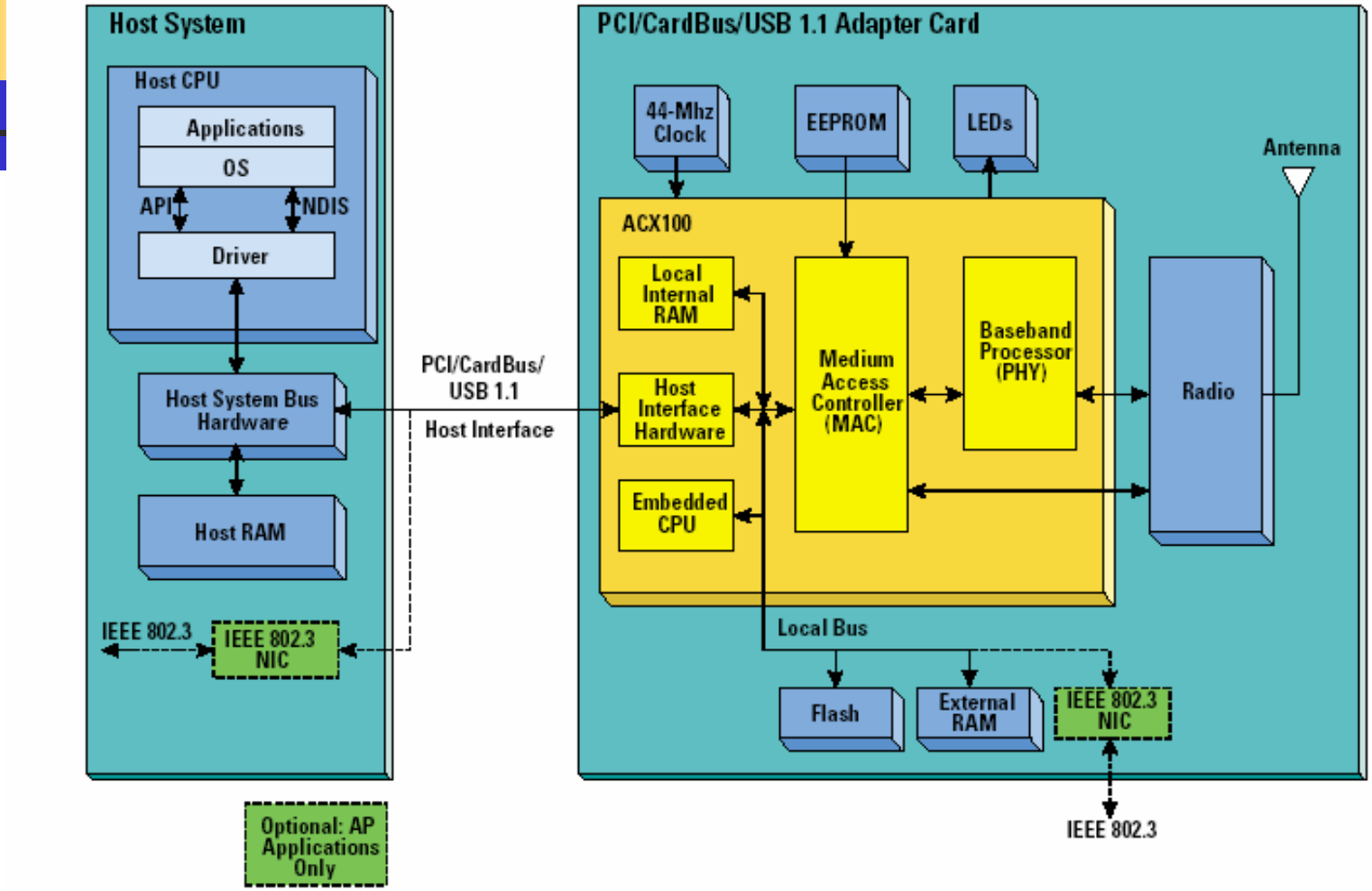
4）HiperLAN:为集团消费者，公共和家庭环境提供无线接入到因特网和实时视频服务。

其中的IEEE802.11即 **CSMA/CA**媒体访问控制协议及相应的物理层规范 ）

IEEE802协议体系

802.11只定义了**OSI**（**Open System Interconnection**）中的物理层和数据链路层中的媒体访问控制层。

就是说在协议体系中，只有物理层及MAC层是由网卡的硬件及软件完成，而LLC层以上各层均有计算机软件来实现。



MAC协议处理芯片的要完成的功能

- MAC协议控制芯片基于802.11标准系列的，它要符合802.11g这一混合标准，要能将从射频模块接收来的信号处理成送入主机所需的数据格式。作为无线局域网的一块应用芯片，它要能处理无线环境下的各种工作方式和进行低功率运行管理，安全管理（即加密）等工作。
- MAC协议处理芯片要有灵活的总线接口，协议方式和物理支持，是多种产品的设计能用同一个芯片。该芯片能完成所有MAC层所要实现的功能，用户在使用时只要加上memory和相应的物理层来完成一个完整的WLAN的连接就可以了。

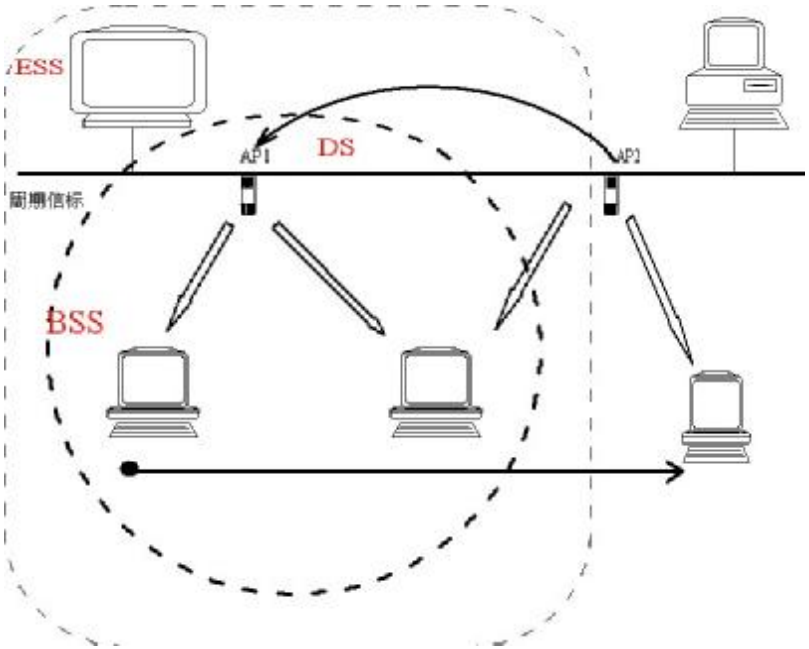
- IEEE802.11 WLAN的设计大致可分为RF设计和基带(baseband)设计和MAC设计。一个WLAN产品，如用于笔记本电脑的无线PC卡或用于连接无线客户端和有线网络的接入点(access point)，主要由调制解调、RF/IF转换、功率放大、基带处理和MAC控制组成。在RF部分，已有现成的符合IEEE802.11 WLAN标准的IC供应，如Harris的PRISM II芯片组和Lucent的WaveLAN模块。再配上MAC控制器和存储器、驱动软件等即可构成一个完整的无线系统前端。

几大公司产品

	Agere system	Atheros	intersil	TI	Euvara	Broadcom
采用标准	802.11a/b/g multimode module					
Chips set	W154040(RF)+WL60040(MAC) +WL64040(Baseband)	AR5002AR2X AR5002AR1X 等七组	ISL3890 ISL3893	ACX100 TNETW 1130 （单片多模）	WiND502 WiND512（单片多模	
上市时间	2003 年第二季	2003.6.3.	2003 年第二季	2003 年四月	2003 年第一季	
采用工艺	Bicmos	0.25umcmos	SiGe	0.13umcmos		0.18umcmos
加密				ASE（高级加密标准）WEP WAP	WEP WAP	
支持接口	PCMCIA CardBus PCI mini-PCI USB					
备注	Techknowledge 预测:802.11g 芯片组将达 9.68 美元，去年是 18 美元。					

WLAN参考模型和术语

- AP（access point):是访问接入点，通过无线的介质访问分布式系统提供服务.
- BSS(Basic service set）：基本业务集,一个接入点所控制的所有的移动台
- DS(Distributed system）：分布系统,是指固定（或有线）的基础结构.
- ESS （ Extended service set）：扩展业务集,用DS连接的一组BSS.



WLAN的工作过程（一）

- 同步搜索：为了得到WLAN提供的服务，工作站在进入到WLAN的服务区域时，需进行同步搜索以定位AP，获取相关信息
- 验证和关联

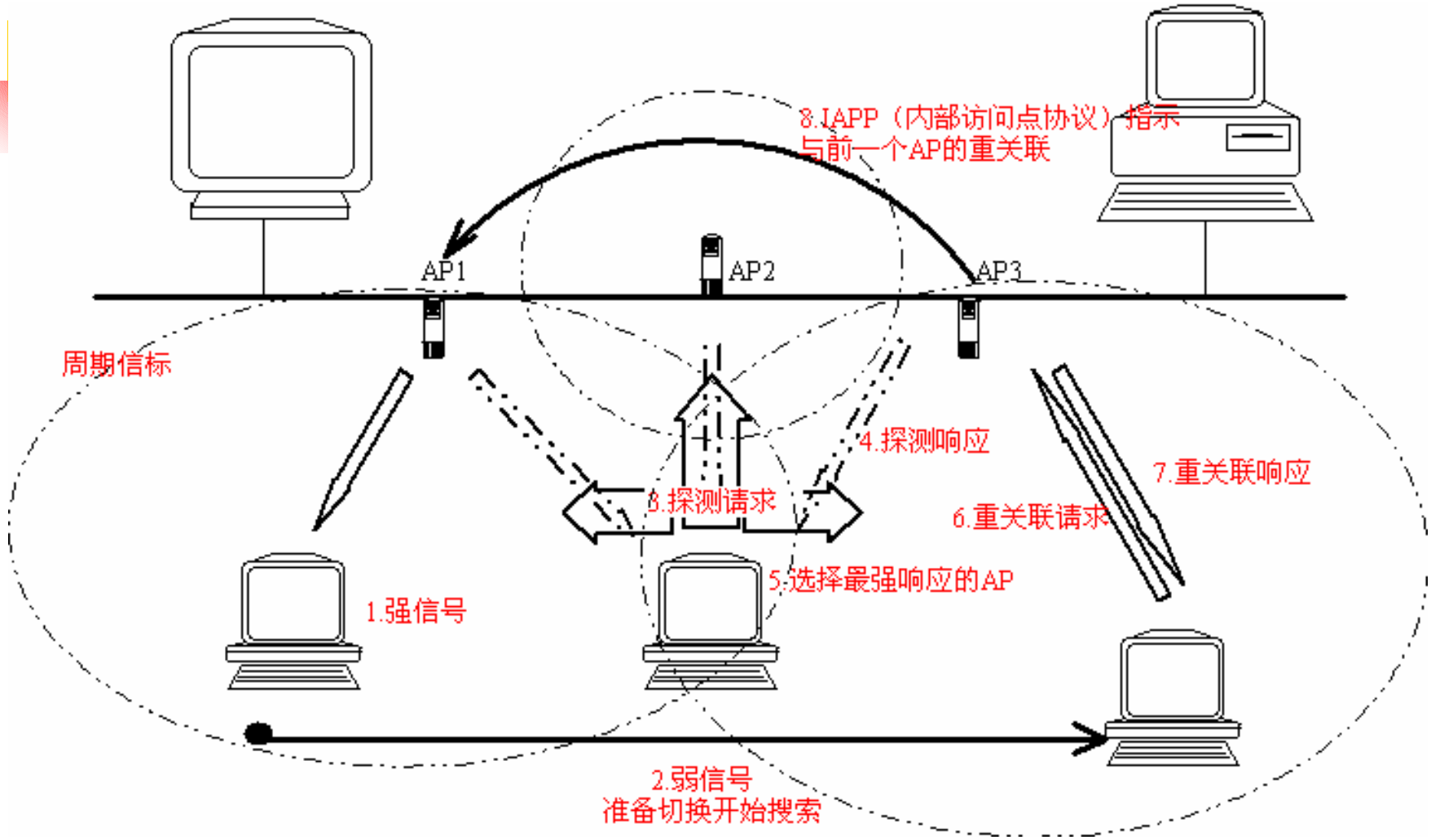
验证：工作站在获得了同步信息并定位了AP后，它就开始了验证的过程，验证过程包括AP对工作站的身份的确认和共享秘匙的认证等。

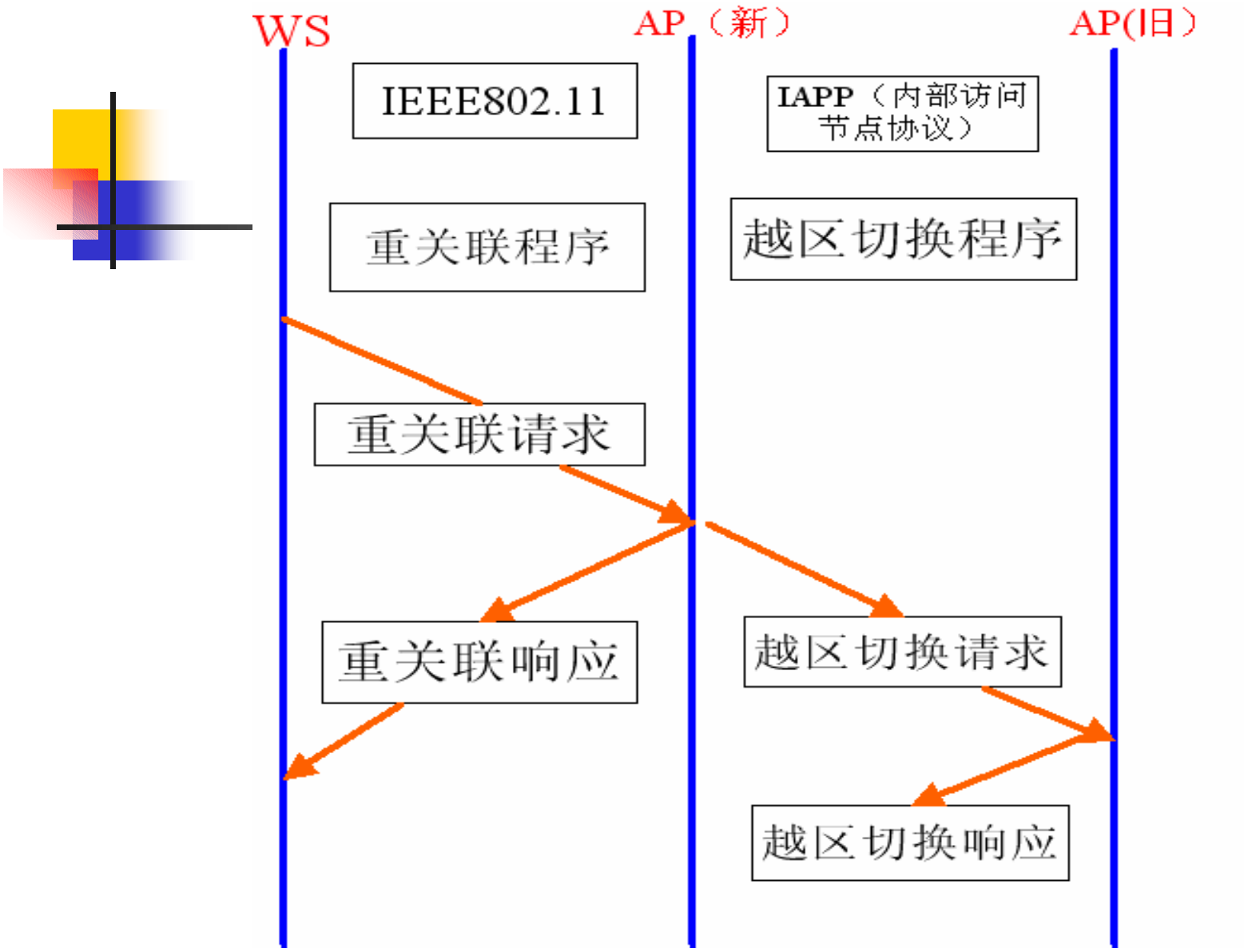
WLAN的工作过程（二）

关联：验证过程结束后，就开始关联过程，关联过程包括：工作站和AP交换信息，在DS中建立了工作站和AP的映象关系，DS将根据该映象关系来实现相同BSS及不同BSS用户间的信息传送。在关联过程结束后，工作站就能够得到该BSS提供的服务了。

WLAN的工作过程（三）

- 漫游：当工作站开始漫游并逐渐远离原AP时，它对原AP的接收信号将变差，于是，工作站&启动扫描功能，重新定位AP，一旦定位了新的AP，工作站随即发射重新连接请求给新的AP，新的AP将该工作站重新连接请求通知分布系统（DS），DS随即更改该工作站与AP的映象关系，并通知原AP，不再与该工作站关联，然后，新的向该站发射重新连接响应，至此，完成漫游过程。如果工作站没有收到重新连接响应，它将重启扫描功能，定位其他AP，重复上述过程，直到连上新的AP。

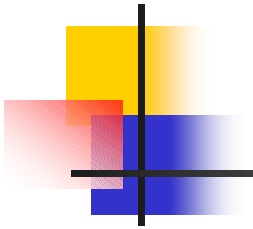




802.11a/b/g在使用上的不同

- **802.11b**是目前普及最广的无线**LAN**规格

  802.11b使用**2.4GHz**频带的电波，可以在相距**50**～**100**米的较长距离内实现设备间的通讯，另外，它还有的抗障碍物的能力较强，可以在公众**WLAN**接入服务中使用低廉产品的出现等优点。但其最大数据传输速度只有**11Mbps**，这虽然与原有的无线**WLAN**相比，速度快了不少，但是要想收发送动态图象等今后将趋普及的大容量尚心有余而力不足。但由于其设备的发展及制造都简单，已经有超过**2000**万的使用者。



- **802.11a是802.11b的后续规格**

  802.11a规格最大数据传输速度为54Mbps，通信速度快，但由于使用5GHz频带的电波，传输损失大，具有未经许无法在户外使用，很难通过墙壁以及无法与普及的802.11b兼容等缺点。802.11a不能与802.11b兼容将成为它发展的一个瓶颈，要将下现有的802.11b网络过渡到802.11a网络，如果改变接入点（主机），就必须更换所有的客户设备的无线WLAN卡（子机），更换的成本很高。

- **802.11g将是WLAN的发展方向**

  802.11g其实是一个兼容标准，它既能适应传统的**802.11b**标准，在**2.4GHz**频率下提供每秒**11Mbps**的数据传输率，业符合**802.11a**标准在**5GHz**频率下提供**54Mbps**数据传输率。

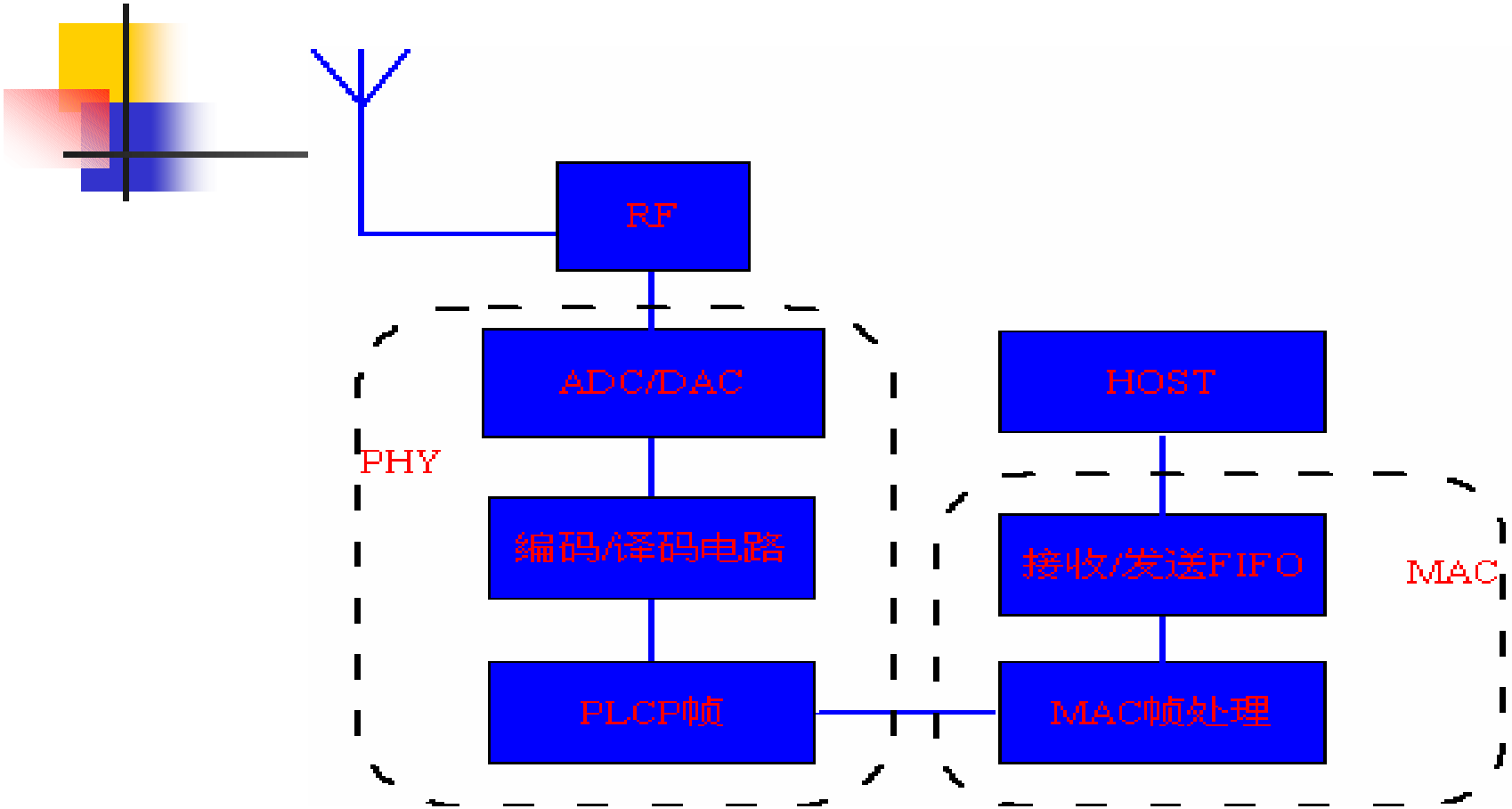
  可以说集**802.11b**和**802.11a**的优点于一身的**802.11g**，将是今后**WLAN**发展的方向。

802.11a/b/g的不同

- **802.11b**：工作在**2.4GHz**频段，物理调制方式为**CCK** 编码的**DSSS**，正常速率**11Mbps**。
- **802.11a:**该物理层使用**5GHz**的频带 **,**采用**OFDM**（正交频分复用）编码技术来传输数据
- **802.11g**：采用的调制方式包括**IEEE802.11a**中采用的**OFDM**（正交频分复用）与**IEEE802.11b**中采用的**CCK**（补码键控）

802.11分层体系结构

- MAC子层主要负责访问机制的实现和分组的拆分和重组。
- MAC的管理子层主要负责ESS漫游管理，电源管理，还有登记过程中的关联，去关联以及要求重新关联等过程管理。
- PLCP主要进行载波侦听的分析和针对不同的物理层形成相应格式的分组。
- PMD子层用于识别相关介质传输的信号所使用的调制和编码技术。
- 物理层管理子层为不同的物理层进行信道选择和调协。

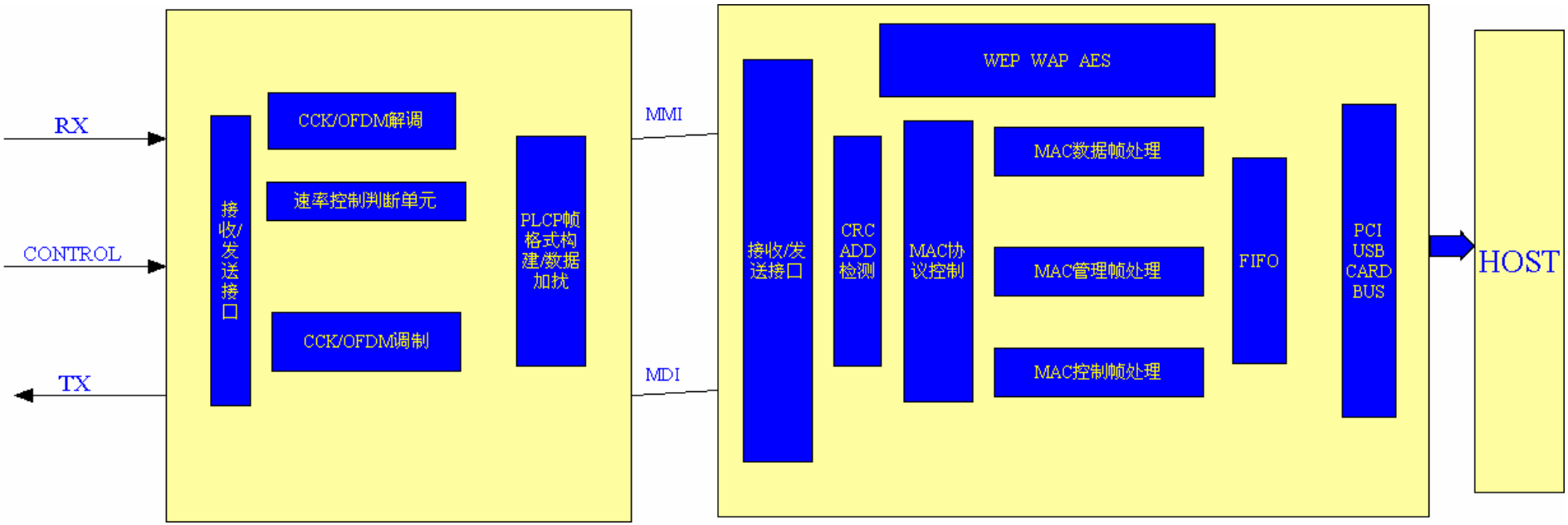


802.11网卡实现原理框图（一）

- 当MAC层有分组需要发送时，无线局域网通过物理和虚拟载波机制监听信道是否空闲，如果虚拟载波发现信道繁忙，就在MAC产生一个随机退让时间进行等待。并继续对信道的侦听。如果发现信道时空闲时，在等待DIFS（基于竞争中使用的一种等待周期）后就开始进行数据传输。此时如果是发送，则PLCP在收到MAC层的发送请求后，就将PMD转换到传输模式，同时MAC层将该请求一道发送数据和速率指示。并且PMD通过天线发送帧前同步码。

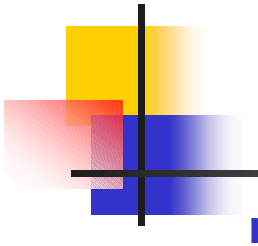
- 接收：接收网络接收传过来的数据帧。如果载波侦听检测介质忙，同时有合法的即将到来的帧的同步码。PLCP开始监视该帧的适配头，如果PLCP测定适配头无误，接收地址是本地址，它将向MAC层通知帧的到来和一些帧适配头的信息。

802.11网卡实现原理框图（二）

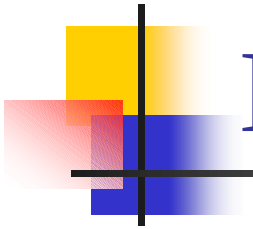


帧版本控制单元

- 完成将所收到的帧进行辨别，是何种帧，并送入相应的处理单元。并且能对STA进行功率管理，即它要能处理STA接收到声明信标帧时，能在规定的时间内让STA苏醒过来，扫描有欲传到本站的数据。在ＳＴＡ要进入睡眠模式时，通知AP。



- 在移动通讯中，一个很重要的问题就是功率保持问题，即在空闲状态保持关掉电源又保持会话。在802.11无线局域网中，利用TSF（timing synchronization function）时间同步帧，将所有的STA在同一时间唤醒以监听信标。STA使用帧控制字段中的功率管理位来表明自己当前是处于睡眠还是唤醒状态。随着信标一起发送的还有一个业务指示表TIM（Traffic indicaton map），它是在AP总有缓存信息的移动台的列表。STA通过检查信标和TIM来了解自己是否有缓存信息。有缓存信息的STA发送节能轮询帧给AP。如果处在活动模式时，AP就向其发送缓存的分组。

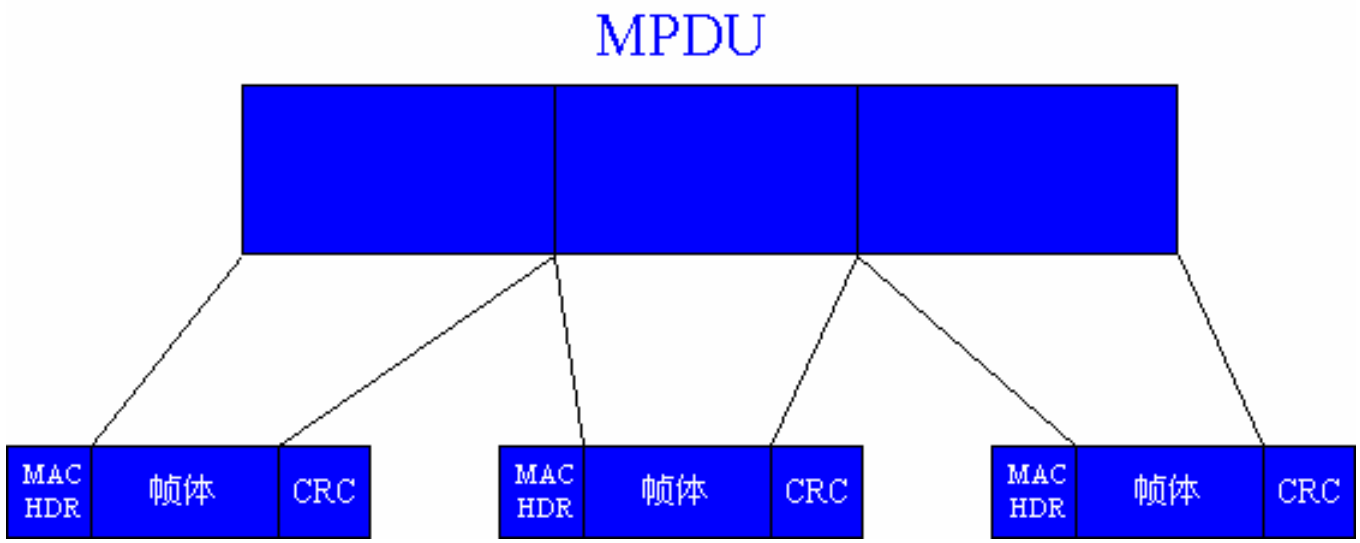


MAC控制帧单元

- 主要用来处理MAC层控制帧的一些功能。例如发送RTS/CTS，ACK等一些查询和控制响应帧。

MAC数据帧控制单元：

- 在将收到的数据帧去掉帧头，并和加密单元一起将接收到的数据进行解密，还原出数据原来的格式，送给FIFO单元。
- 在发送时，先验证发送请求的有效性。再通过信道检测单元检测信道的环境，如果是在一个充满干扰和噪声的环境中，较长的帧就根据此时信息管理库MIB定义的分割阈值长度在此分成较短的帧进行传递。即将较长的数据分成几段，再分进行加上数据帧帧头处理。



ADD，CRC校验单元

- 当数据送入MAC层时，该单元首先对数据进行ADD检查确认，如果地址不符，将不再往下进行处理，如果地址正确，将数据送入帧版本控制单元进行处理，同时进行CRC校验。
- 在进行ADD检查时，工作站在决定要不要收一个数据讯框时是依据Address的内容来判断的。如果Address的内容与自己的地址相同则可接收。如果Address的内容是一个群体地址，则BSSID也要一并检查，以确定该广播或群播讯框是来自相同的BSS。

- CRC校验：CRC就是块数据的计算值，它的全称是“Cyclic Redundancy Check”，“CRC校验”就是“循环冗余校验”。
- CRC校验采用多项式编码方法。被处理的数据块可以看作是一个n阶的二进制多项式，由。如一个8位二进制数10110101可以表示为：。多项式乘除法运算过程与普通代数多项式的乘除法相同。多项式的加减法运算以2为模，加减时不进，错位，和逻辑异或运算一致。
- 采用CRC校验时，发送方和接收方用同一个生成多项式g（x）,并且g（x）的首位和最后一位的系数必须为1。CRC的处理方法是：发送方以g（x）去除t（x），得到余数作为CRC校验码。校验时，以计算的校正结果是否为0为据，判断数据帧是否出错。

MAC管理帧单元

- 包含有一个MIB（MAC信息管理库），能对MAC层的操作进行配置，测量，并进行调整。例如在一个STA准备加入一个BSS时所进行的请求和关联等工作进行管理，发送相应的帧进行请求。

MAC接收/发送单元

- 该单元要完成MAC与PHY之间请求和应答信号的交流。在接收状态时，要对接收来的数据的SFD进行判别，判断出其地址单元，然后送入ADD/CRC单元进行地址检验。同时接收发送单元还要实现虚拟载波监听的功能

速率接收控制单元

- 在接收数据时，数据要经过该单元，进行数据的速率判断，确定其采用的编码技术，然后选择不同的译码单元。

PLCP帧格式构建/数据加扰

- 发送时，有ＭＰＤＵ数据到达该单元时，该处理单元会为MPDU加上ＰＨY的信息，如CRC校验，同步序列和前导信息序列等。经过该单元的MPDU（介质协议数据单元）就包含了物理层接收和发送所需的信息，这个合成帧为PLCP协议数据处理单元（PPDU）。在接收时，则要处理所接收的数据单元的PLCP的帧头。
- 在802.11g产品中，同时支持CCK和OFDM两种编码技术。两种不同的编码技术在PLCP分组帧格式上是不同的。

- DSSS和FHSS的SFD格式是一致的，但是代码的内容是不一样的。
- FHSS中的PSF字段和DSSS中的Signal字段表示的都是数据速率
- FHSS中不存在在DSSS中位Service的保留字段
- DSSS中的FCS和FHSS中的CRC字段的功能是相似的

802.11中FHSS方式的PLCP帧格式

SYNC（80比特）	SFD（16比特）	PLW（12比特）	PSF（4比特）	CRC（16比特）	白化MPDU（<4096字节）

SYNC:0或1　SFD：0000110010111101　PLW：分组长宽　PSF：采用500kbps步长的数据速率　CRC:PLCP帧头编码

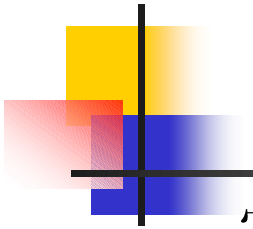
802.11中DSSS方式的PLCP帧格式

SYNC(128比特)	SFD（16比特）	Signal(8比特)	Service(8比特)	Length(16比特)	FCS（8比特）	MPDU

SYNC：0或1　SFD：1111001110100000　Signal:100kbps步长的数据速率　Service:保留将来使用
LengthLMPDU的长度　FCS：PLCP帧头编码

信道检测单元

- 通过空中接口地实际侦听来发出信道评价信号CCA（Clear channel assignment）。在通过在空中接口侦听检测地比特，或者载波的收信号的度RSS（Receive signal strength）超过阈值，该单元向MAC发出CCA信号。

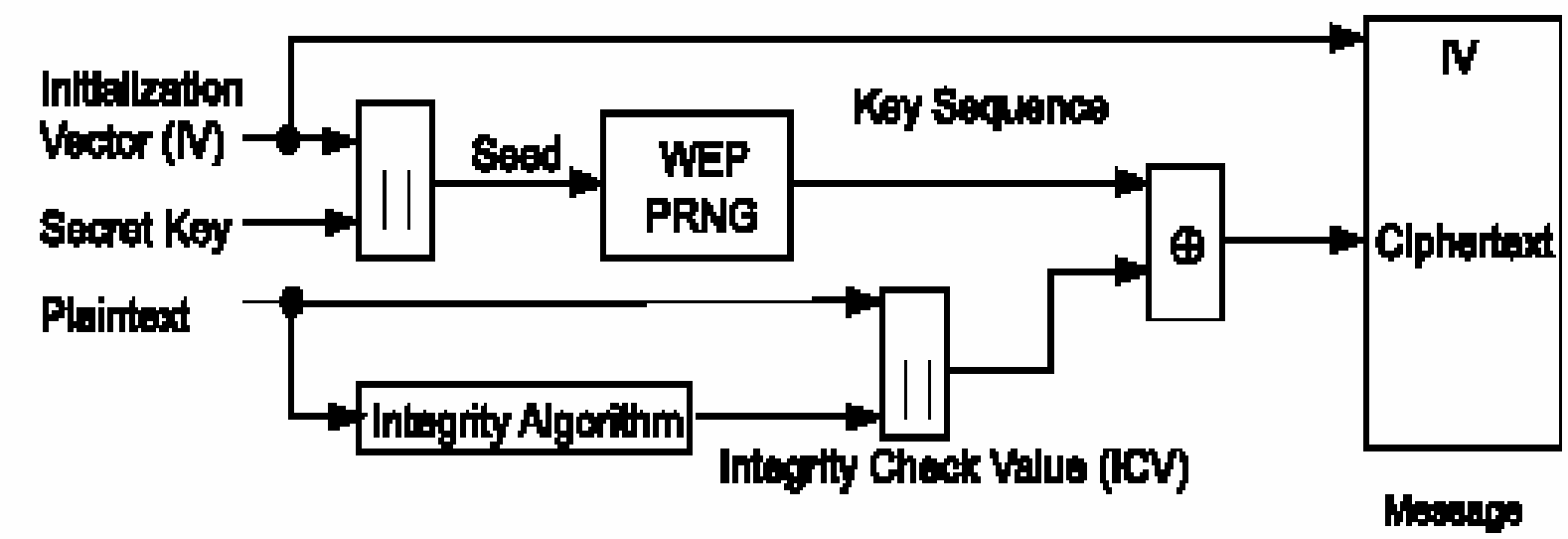


它和MAC层中由RTS/CTS(发送请求/清除发送)和PCF（集中控制方式）支持地网络配置矢量NAV一起分别完成对信道地物理和虚拟载波侦听。采用CSMA/CA（Carrier sense multiple access with collision avoidance）协议进行访问时，只要MAC层有分组要发送，就要利用物理和虚拟载波侦听机制侦听信道是否空闲。如果虚拟载波侦听发现NAV信号存在，则表示信道繁忙，就会将操作延时，继续保持侦听直到NAV信号消失，当虚拟载波侦听发现NAV＝0，即信道空闲，MAC层就侦听信道的物理条件，如果此时信道空闲，STA等待DIFS（DCF inter－frame spacing）就开始发送信息。如果此时信道忙，则MAC层利用随机让时间控制机制，产生一个随机数作为退让时间进行等待。

WEP加密单元

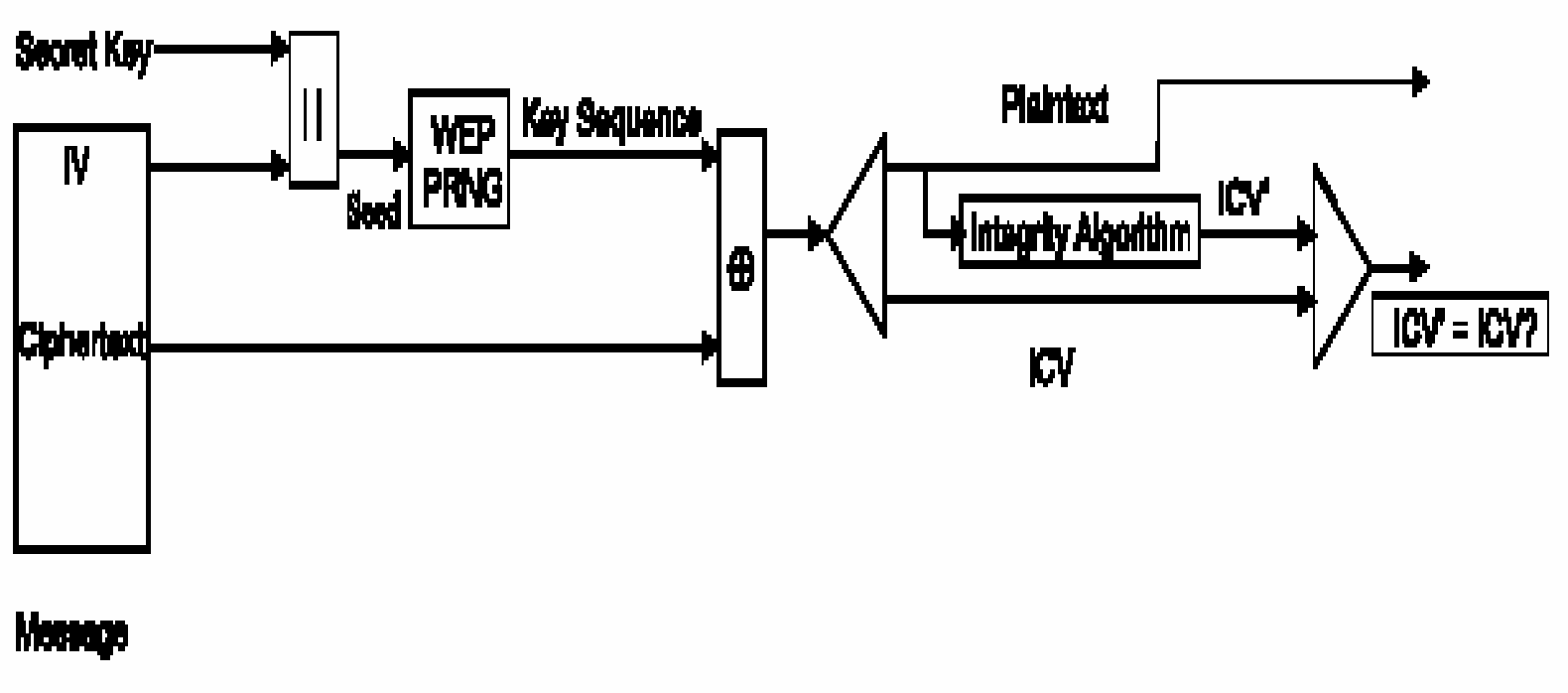
- 用来对MPDU(MAC Protocol data unit)进行WEP算法加密和对接收的数据单元进行解密的单元。
- WEP（Wireled Equivalency Privacy）有线等价保密是被定义用来防止非授权用户的“意外偷听”，提供了手段用来加密位于移动单元和基站之间的无线通信完网络的连接。

WEP加密过程



- 把密钥和一个初始化向量串联在一起，并且得到地种子被输入到伪随机数生成器（PRNG，Pseudorandom Number Generator）里。PRNG使用RC4流加密算法，输出与被发送数据八位组数字等长的伪随机八位组密钥序列。在试图防止未经授权修改数据的时候，对未加密报文执行一个完整性检验算法，然后把得到的校验和未加密的报文串联在一起，得到完整性检验结果IVC（Integrity Check Value）。然后通过对IVC和PRNG输出值进行数学上的按位异或运算，生成报文，结束真个加密过程。然后把IV和密文串联在一起，得到的报文送出去。

WEP解密过程



WEP加密解密过程

- 对输入的数据进行解密是一个相反的过程。在解密时，利用和加密时一样的密钥与IV生成种子，然后该种子被送到伪随机数生成器PRNG中，生成与密文等长的伪随机八位组密钥序列，与密文进行异或运算，得到原始的明文和CIV值，此时再将得到的明文进行一次完整性检验,结果IVC（Integrity Check Value）与异或得到的CIV值进行比较，如果相等，说明接收无误，可将得到的明文传给LLC。如果不相等，说明得到的MPDU有误，数据不再下传，还要发送一个错误报告给MAC管理单元，声明该帧错误，需重传。

CCK,OFDM调制解调单元

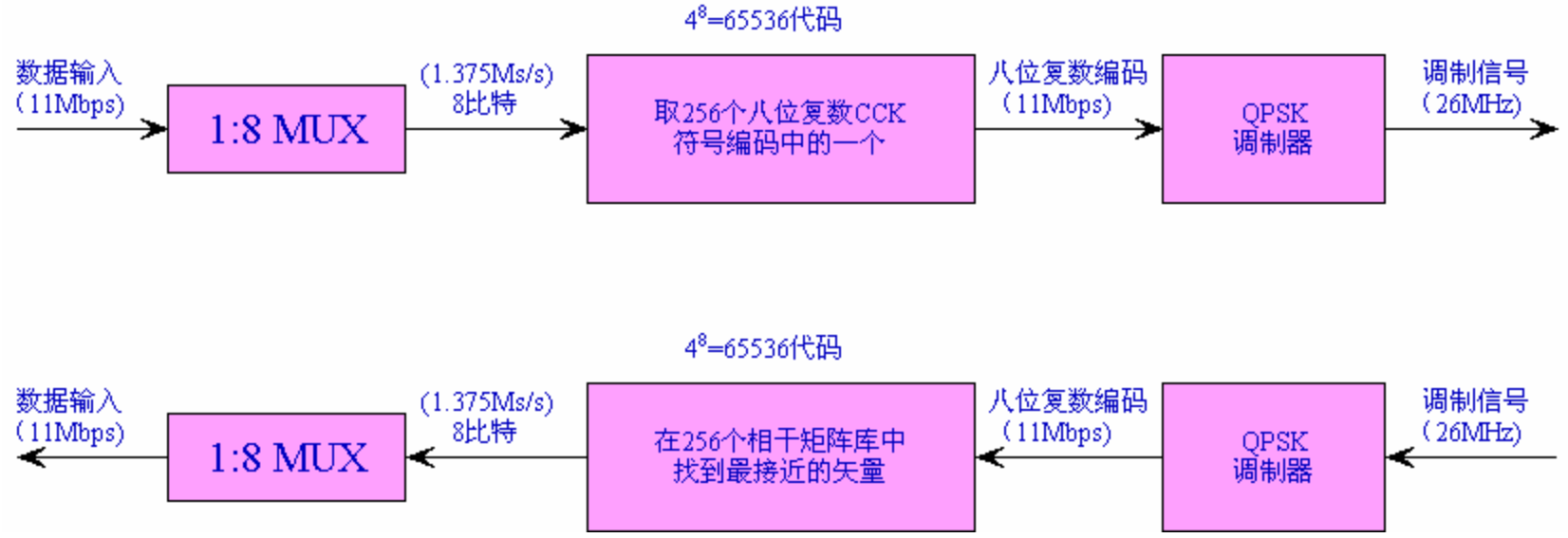
- 该单元负责完成数据在传输之前的调制和编码。
- 802.11g标准采用的了兼容802.11a和802.11b标准的技术，同时支持前两种标准所采用的编码技术。

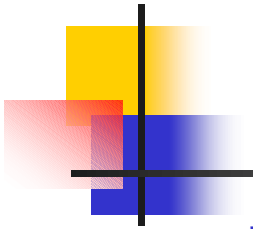
- CCK(Complementary code keying)互补编码键控法：它在802.11b标准中被采用，进行11Mbps的传输.其基本原理为：输入的数据流被分组，8个比特一组，共有256个符号，速率为11Mbps/8＝1.375Mbps，编码器把每一个8比特符号映射成为8位四相编码符号。这里使用256个符号，这256个符号是从4^8＝65536个符号里选出来的，并且它们彼此正交。8位四相编码块的每一个符号采用QPSK四相调制器串行发送，在接收器总，每8个从QPSK解调器解调接收的复数波形再被编组成块送到解码器，根据解调后的8位的四相位信号来找出最接近的八位符号。下面的方程给出了编码时采用的映射规则：

$$c = \left\{ e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, \right.$$

$$\left. -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \right\}$$

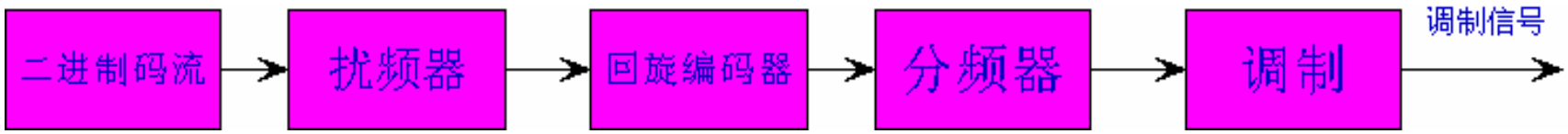
- 8位输出的比特进一步分组成4个双比特复数四相符号。这样产生的4个相位Φ1，Φ2，Φ3，Φ4代入上面公式就得到8个复数编码的波形再送到串行再送到QPSK调制解调器进行调制。





- OFDM（Orthogonal frequency division multiplexing）正交频分复用：采用改技术，能使数据的最高传输速率达到54Mbps。它是802.11g兼容802.11a的一种编码方式。
- 它包含了多速率，多符号和多载波调制三种原理。
- 在多符号调制技术中，它采用了多个幅度和多个相位调制以及编码技术来增加数据的速率。
- 在多速率的调制就是在信道状况恶劣的情况下提供一个和多个的低效运行（fallback），工作模式来提高通信的可靠性。
- 多载波是指在传输中，每个不同的信道都有不同的子载波用于信息传输。我们可以通过调节每一个信道的发射功率来补偿由于频率选择性衰落对不同信道造成的不同影响。

- 首先信息数据串会先经过由扰频器，由127个随机位码将数据串处理成不要都是连续的1或0，接着在加上有错误修正码功能的回旋编码器，器编码率有1/2,2/3,3/4,然后依据不同的速率进行分频处理使数据串具有频分的特性，而可以减少传输通道的不良影响，使误码率降至最低，然后在进行调制。



参考资料

- 《OFDM无线局域网》 Juha Heiskala/John Terry 电子工业出版社
- 《无线网络安全防护》 Christran Barnes等著 机械工业出版社
- www.gb.tomshardware.com/consumer/01q3/010827/ - 27k
- http://network.ccidnet.com/pub/html/network/focus/wlan/
- http://www.iturls.com/TechHotspot/TH_wifi.asp