一、网络服务

802．11总共提供9种服务：

分布式（distribution）

接入点收到帧，就会使用分布式服务将真传送至目的地。

整合（integration）

该服务由分布式系统提供，它让分布式系统得以链接至非IEEE802.11网络

关联（association）

移动式工作站向接入点登记，分布式系统即可根据登记信息判断哪个移动式工作站该使用哪个接入点。只有关联之后才能进行身份验证。在身份验证完成之前，接入点会丢弃来自工作站的所有数据。

重新关联（association）

当移动式工作站在同一个扩展服务区域里的基本服务区域之间移动时，它必须随时评估信号的强度并在必要时切换所关联的接入点。重新关联是由移动式工作站所开启，当信号强度现实最好切换关联对象时便会重新关联。

取消关联（disassociation）

结束现有关联。

身份验证（authentication）

认证是 STA 在扫描到合适的AP 之后，只有通过认证该STA 才能通过AP 使用WLAN。

现有的认证方式有：(1)open，即不需要认证，只要交互一个null 帧 (2)shared key，需要一个4 次握手的过程 (3)802.11i，需要到认证服务器认证

当STA 完成认证之后只需要发送ReAssociation Request 帧，然后等待ReAssociationResponse 帧完成关联也就完成了整个切换的过程。

解除身份验证

机密性

Wep等一些加密机制

MSDU传递（MAC Service Data Unit）

负责将数据传送给实际的接收端。

传输功率控制（Transmit Power Control 简称TPC）

欧洲标准要求操作与5G Hz频带的工作站必须能够控制颠簸的传输功率，避免干扰其他同样使用5G Hz频带的用户。

动态频率选择（Dynamic Frequency Selection 简称DFS）

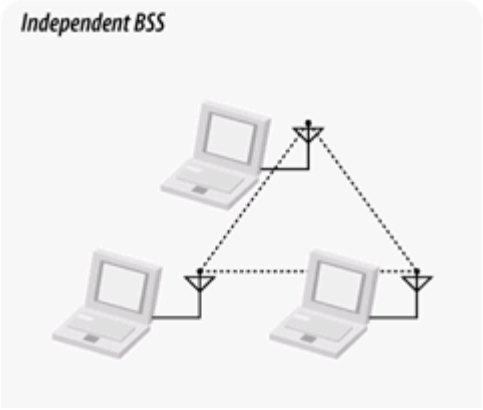
无线局域网必须能够检测到雷达系统并选择未被雷达系统所使用的频率。

二．网络类型

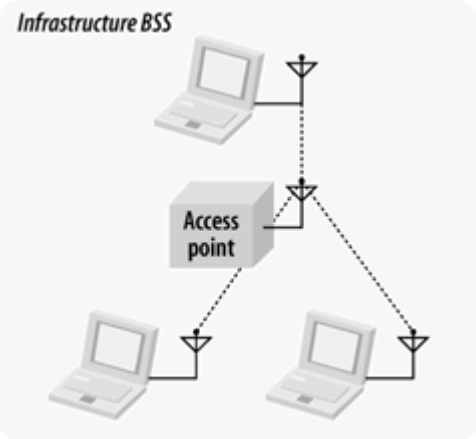
基本服务集（basic service set ,简称BBS）由一组相互通信的工作站构成。

BSS分为两种：

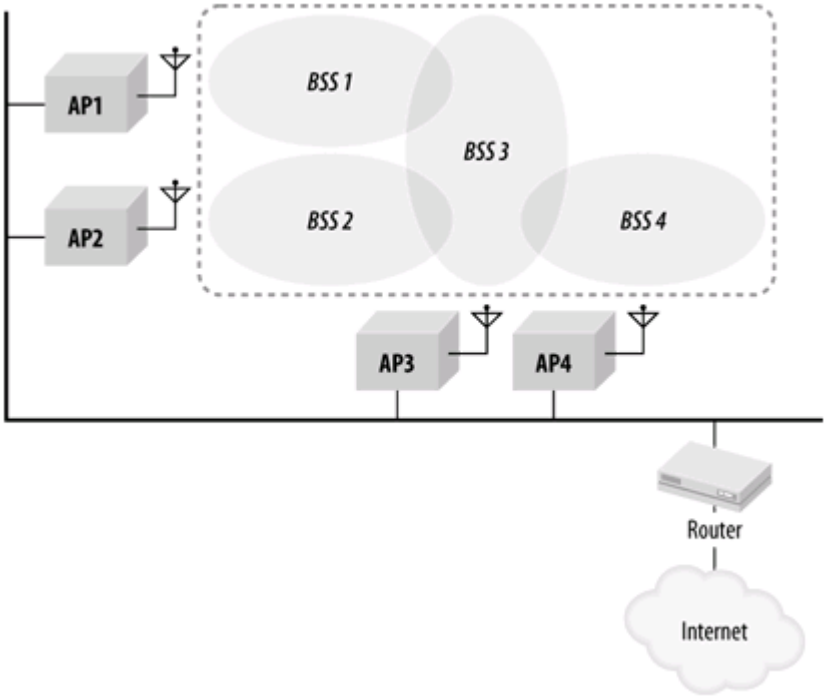
独立型网络independent BSS：通常由少数几个工作站为了特定目的而组成的暂时性网络。



基础结构型网络Infrastructure networks：有接入点。接入点负责基础结构型网络的所有通信。



扩展服务区域extended service set（ESS）
将几个BSS串联称为extended service set。所有位于同一个ESS的接入点使用相同的服务组标示符（service identifier ，简称SSID）



三．MAC层

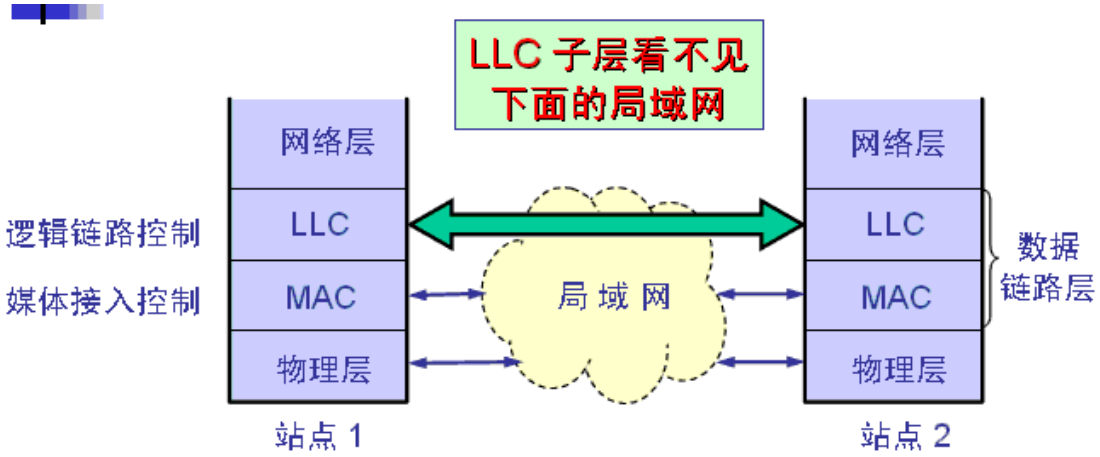
数据链路层的两个子层

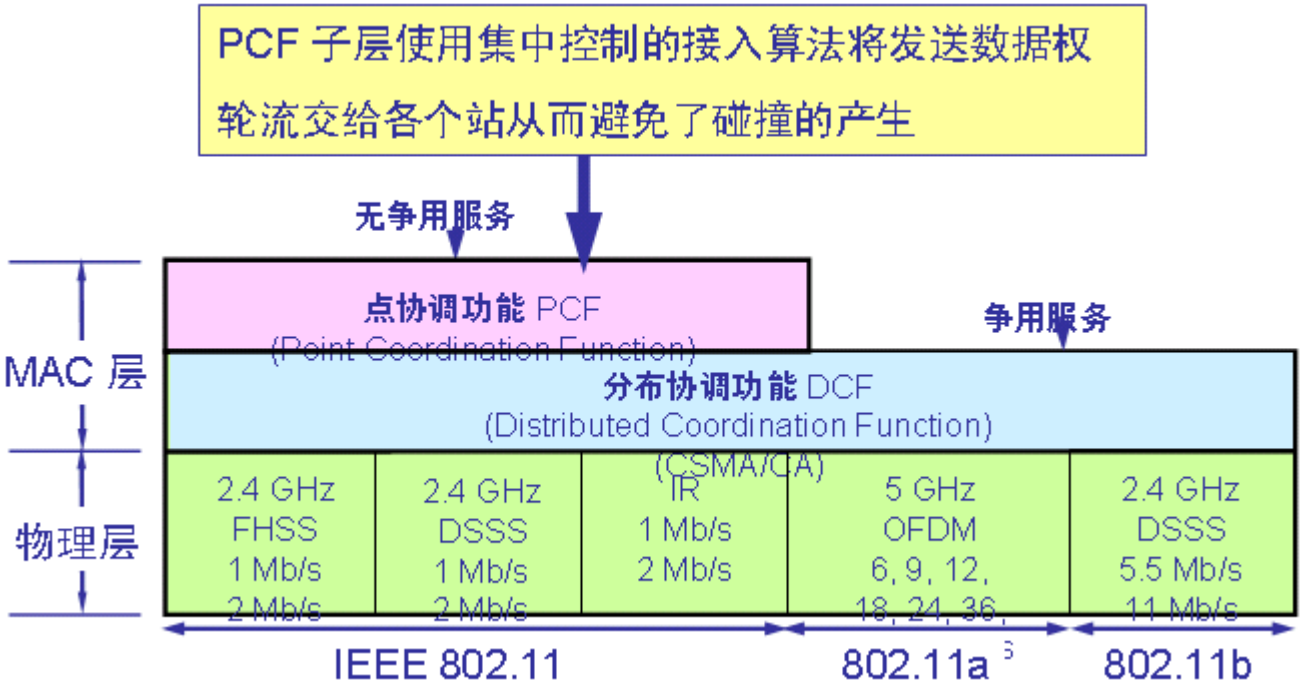
逻辑链路控制 LLC (Logical Link Control)子层

媒体接入控制 MAC (Medium Access Control)子层

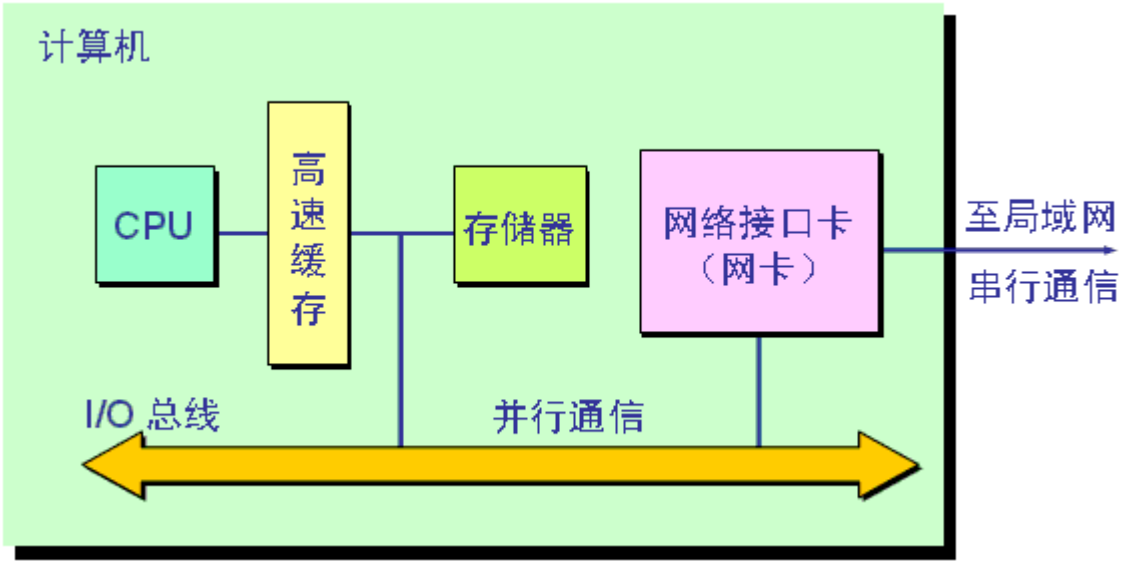
- 与接入到传输媒体有关的内容都放在 MAC子层，而LLC 子层则与传输媒体无关，

不管采用何种协议的局域网对 LLC 子层来说都是透明的





网卡及其功能



- 数据的封装与解封 发送时将上一层交下来的数据加上首部和尾部，成为以太网的帧。接收时将以太网的帧剥去首部和尾部， 然后送交上一层
- 链路管理 主要是 CSMA/CD 协议的实现
- 编码与译码 即曼彻斯特编码与译码
- 网卡从网络上每收到一个 MAC 帧就首先用硬件检查 MAC 帧中的 MAC 地址如果是发往本站的帧则收下，然后再进行其他的处理

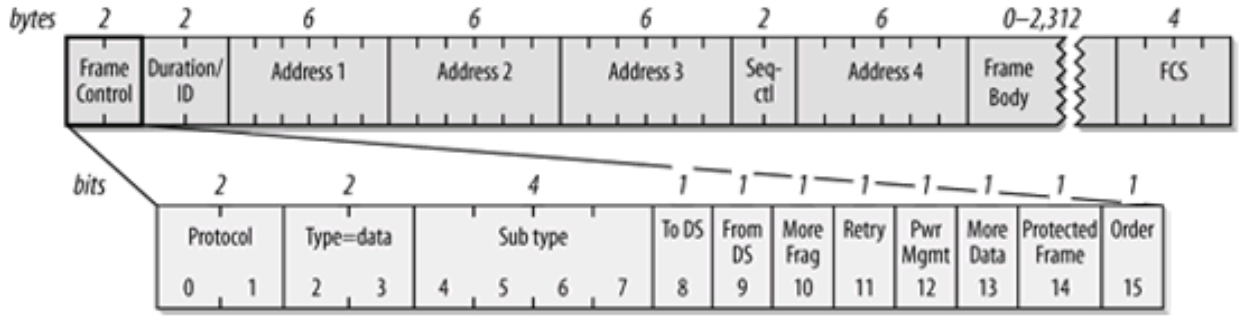
  否则就将此帧丢弃，不再进行其他的处理

四．帧

802.11帧主要有三种类型：数据帧、控制帧、管理帧

数据帧：

帧格式：



Protocol：代表MAC协议版本

Type与Subtype：制定使用帧类型(控制帧、数据帧、管理帧)

Address1：帧接收端

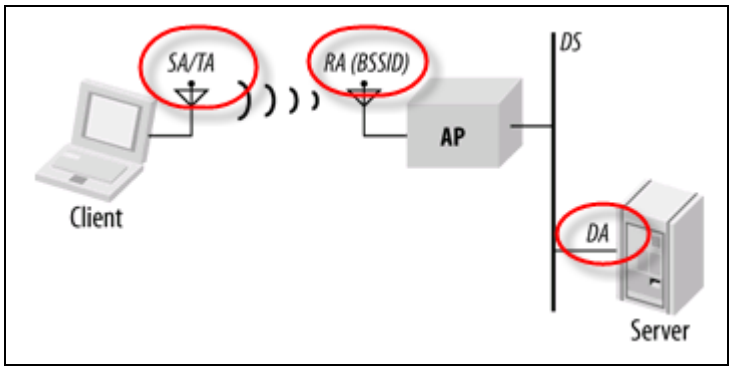
Address2：发送端的地址

Address3：供接入点与分布式系统过滤之用

Duration：媒介使用权，RTS传送段计算RTS帧结束后还需要多长时间用于帧交换。

地址信息

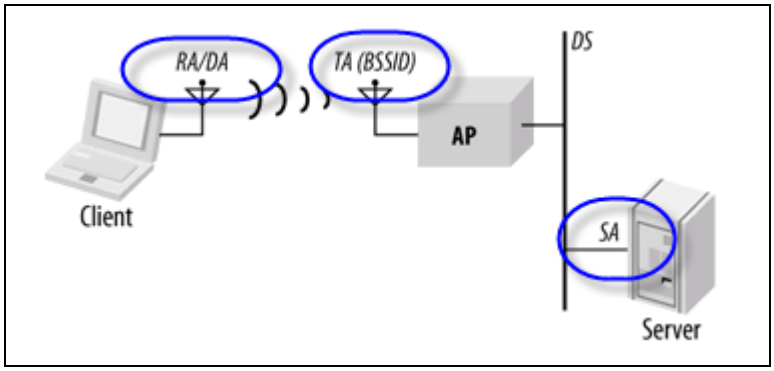
功能	ToDS	FromDS	Address 1 (接收端)	Address 2 (发送端)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	未使用
To AP (基础结构型)	1	0	BSSID	SA	DA	未使用
From AP (基础结构型)	0	1	DA	BSSID	SA	未使用
WDS (桥接器)	1	1	RA	TA	DA	SA



帧送至服务器

对应第二行

Address1 ： RA/BSSID Address2 ： SA/TA Address3 ： DA



帧来自分布式系统

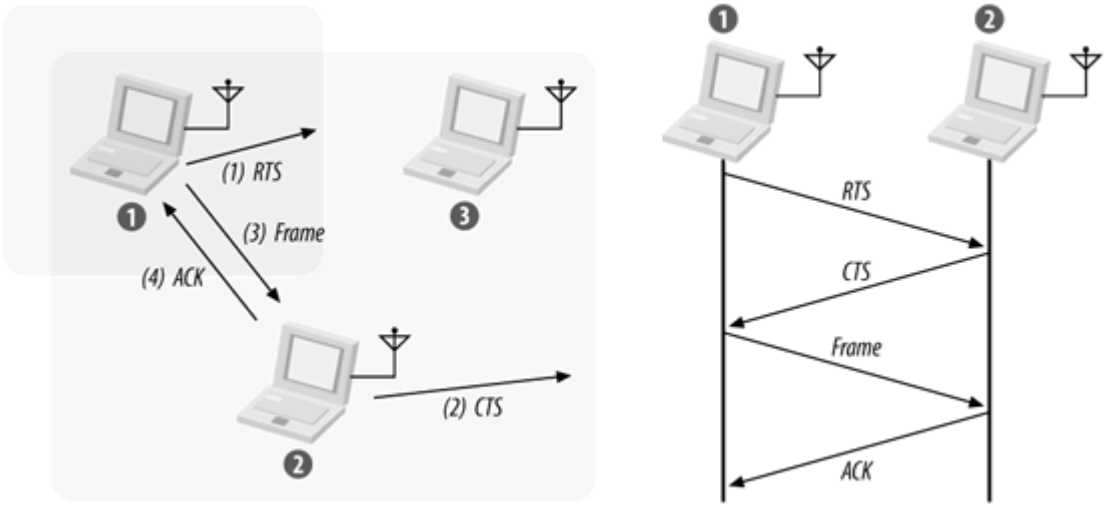
对应第三行

Address1 ： RA/DA Address2 ： TA/BSSID Address3 ： SA

控制帧：

通常与数据帧搭配使用，负责区域的清空、信道的取得、载波监听的维护，并于收到数据时予以肯定确认，借此提高工作站之间数据传送的可靠性。

因为无线收发器通常只有半双工工作模式，即无法同时首发数据，为防止冲突，**802.11**允许工作站使用**request to send(RTS)**和**clear to send**（**CTS**）信号来清空传送区域。



RTS/CTS进行清空

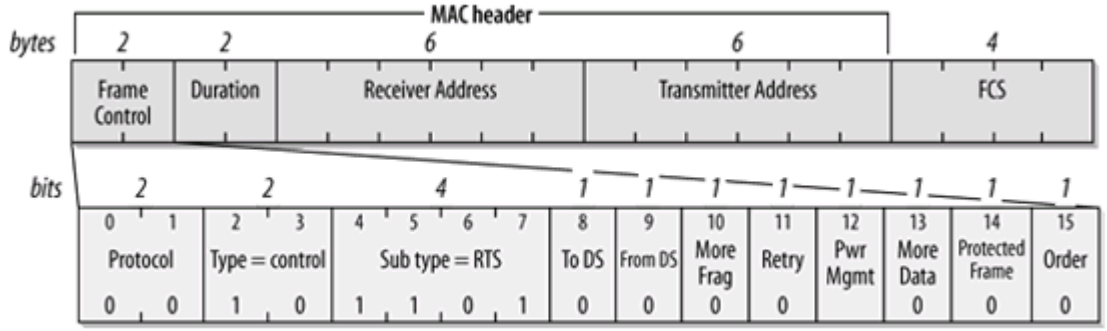
节点1有个帧待传，首先发送RTS帧，预约无线链路的使用权、要求接收到这一帧的其他工作站保持沉默。

接收到RTS帧，接收端会以CTS帧应答，RTS会令附近的工作站保持沉默。

RTS/CTS完成交换后，可发送frame。

媒介访问权只留给单播帧使用，组播和广播帧只是简单的传送。

这种机制一般只用在高用量的环境下以及传输竞争比较激烈的场合，对低用量环境而言，暂不需要。

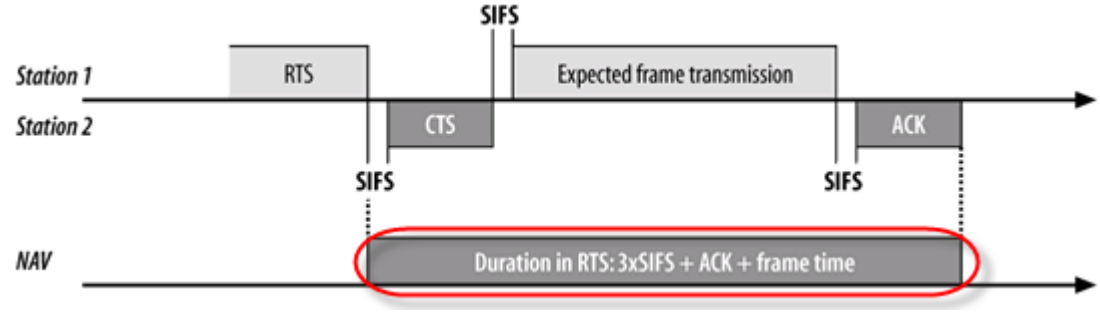


RTS帧

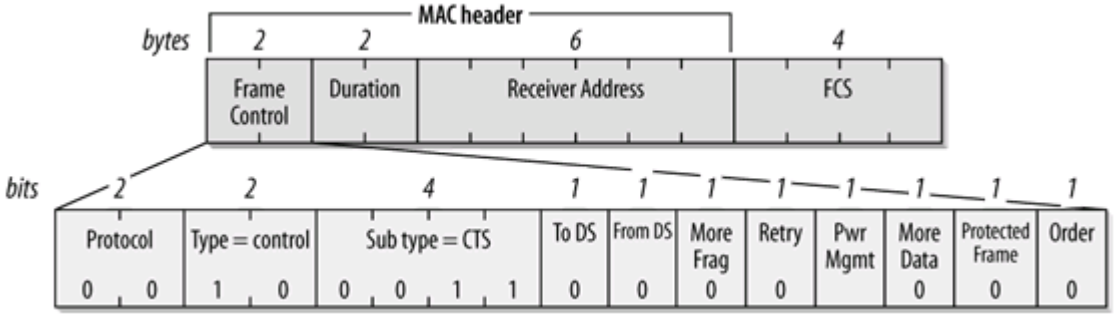
Duration：媒介使用权，RTS传送段计算RTS帧结束后还需要多长时间用于帧交换。

Address1：大型帧的工作站地址

Address2：RTS的发送端

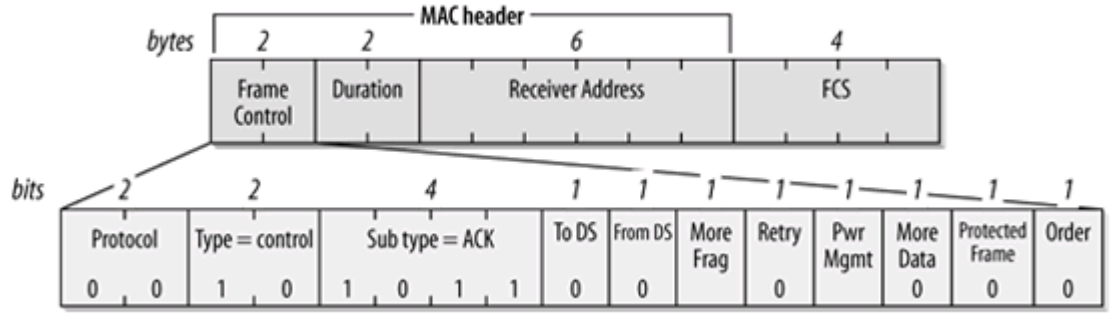


Rts的Duration



CTS帧

Address1：接收端的字段，拷贝于RTS的发送端地址。

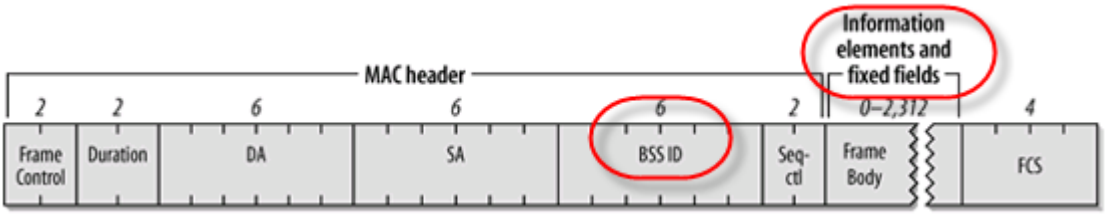


ACK帧

除了这3种控制帧，还有PS-POLL帧（省电轮询）。

管理帧

负责监督，用来加入或退出无线网络以及处理接入点之间关联的转移事宜。



为了限制广播或组播管理帧所造成的副作用，收到管理帧后，必须加以查验。只有广播或者组播帧来自工作站当前所关联的BSSID时，它们才会被送至MAC管理层。唯一例外是beacon帧。

帧主体分两种：固定字段、信息元素。

固定字段（Fixed-Length Management Frame Components）：数据使用长度固定的字段。一共有10种。

1. Authentication Algorithm Number身份验证算法编号：

0：开放系统身份验证

1：共享密钥身份验证

2~65535;保留

2. Authentication Transaction Sequence Number身份验证处理序列号

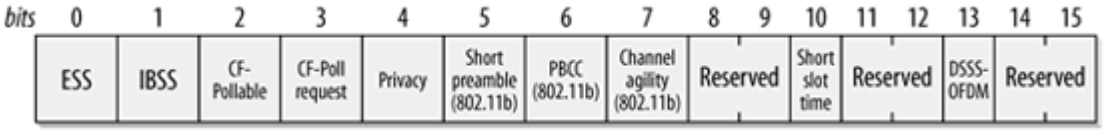
用以追踪身份验证进度。

3.beacon interval字段

用来设定**beacon**信号之间相隔多少时间单位。

4. Capability Information性能信息

传送**beacon**信号的时候，它被用来通告网络具备何种性能。



5. Current AP Address

移动式工作站用此字段表明当前关联的接入点的MAC地址，便于关联与重新关联的进行。

6. Listen interval

工作站为节省电能，暂时关闭802.11的天线，休眠中的工作站会定期醒来聆听往来消息，以判断是否有帧缓存于接入点。

其实就是以Beacon interval为单位所计算出的休眠时间。

7. Association ID关联标示符

工作站与接入点关联时就会被赋予一个关联标识符来协助控制和管理。

8. Timestamp时间戳

用来同步BSS中的工作站。

9. Reason Code原因代码

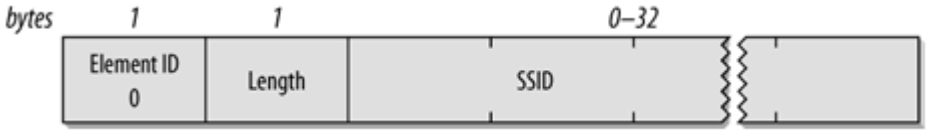
对方不适合加入网络时，工作站会发送disassociation（取消关联）或deauthentication（解除身份验证）帧作为响应。该字段用以表示产生该原因代码的理由。

10. Status Code

表示某项操作成功或失败。

信息元素：

管理帧的可变长组件。



一般管理帧的信息元素

Element ID	名称
0	服务集标示符(SSID)
1	支持速率 Supported Rates
2	跳频参数集 FH Parameter Set
3	直接序列参数集 DS Parameter Set
4	无竞争参数集 CF Parameter Set
5	传输指示映射 Traffic Indication Map (TIM)
6	IBSS 参数集
7 (802.11d)	Country
8 (802.11d)	Hopping Pattern Parameters
9 (802.11d)	Hopping Pattern Table
10 (802.11d)	Request
11-15	Reserved; unused
16	Challenge text
17-31	保留
32 (802.11h)	功率限制 Power Constraint
33 (802.11h)	Power Capability
34 (802.11h)	发送功率控制请求 Transmit Power Control (TPC) Request
35 (802.11h)	发送功率控制报告 TPC Report
36 (802.11h)	所支持的信道 Supported Channels
37 (802.11h)	信道切换声明 Channel Switch Announcement
38 (802.11h)	测量请求 Measurement Request
39 (802.11h)	测量报告 Measurement Report
40 (802.11h)	静默 Quiet
41 (802.11h)	IBSS 动态选频（DFS）
42 (802.11g)	ERP information
43-49	Reserved
48 (802.11i)	强健安全网络 Robust Security Network
50 (802.11g)	扩展支持速率 Extended Supported Rates

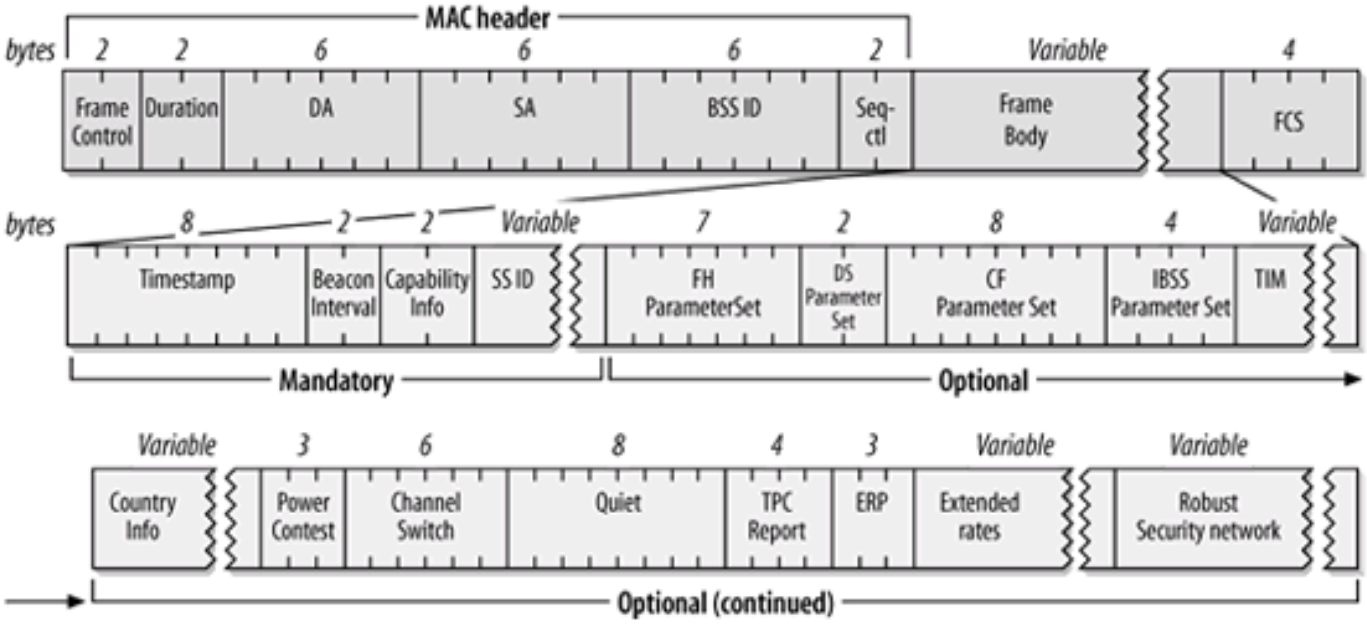
32-255	Reserved; unused
221	Wi-Fi 保护访问 Wi-Fi Protected Access

管理帧类型

管理帧的主体包含的固定字段与信息元素是用来运送信息的。管理帧主要有以下几种，负责链路层的各种维护功能。

1. Beacon（信标）帧

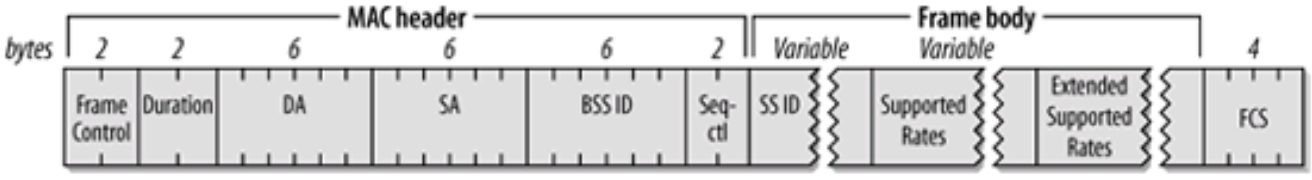
主要用来声明某个网络的存在。定期传送的信标可让station得知网络的存在，从而调整加入该网络所必需的参数。



Beacon（信标）帧

2. Probe Request探查请求

移动工作站利用Probe Request探查请求帧来扫描区域内目前有哪些802.11网络。



Probe Request帧

包含2个字段

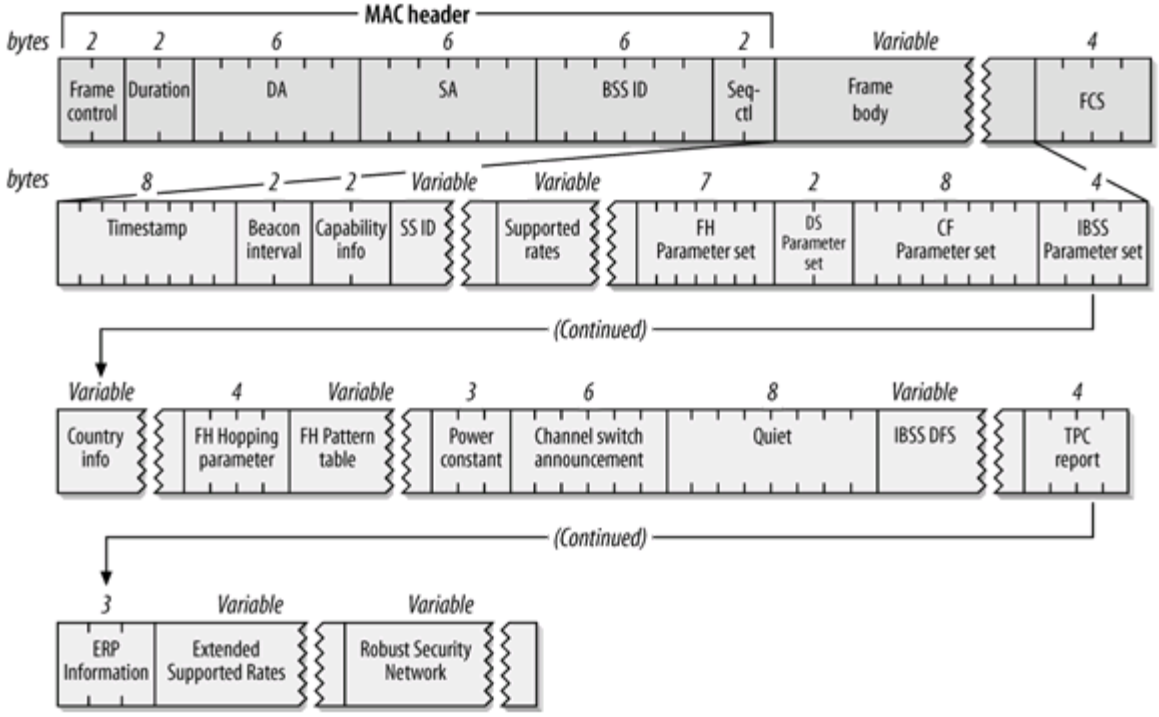
SSID：可被设定为特定网络的SSID或任何网络的SSID。

Support rates：移动工作站所支持的速率。

3.Probe Response帧

如果Probe Request所探查的网络与之兼容，该网络就会以Probe Response帧响应。送出最后一个beacon帧的工作站必须负责响应所收到的探查信息。

Probe Request帧中包含了beacon帧的所有参数，station可根据它调整加入网络所需要的参数。

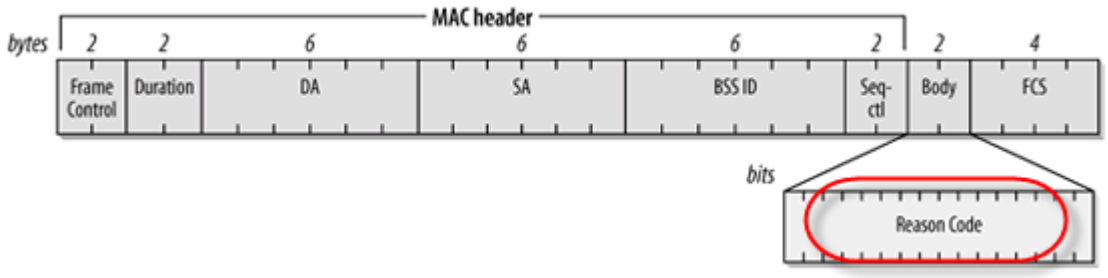


Probe Request帧

4. IBSS announcement traffic indication map (ATIM)

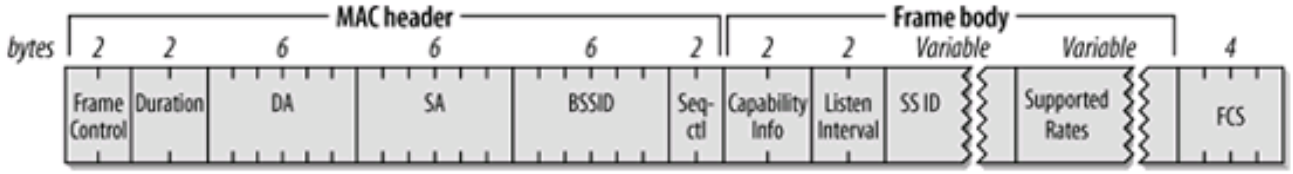
IBSS的通知传输只是消息（ATIM）帧

5. Disassociation and Deauthentication取消关联、解除验证



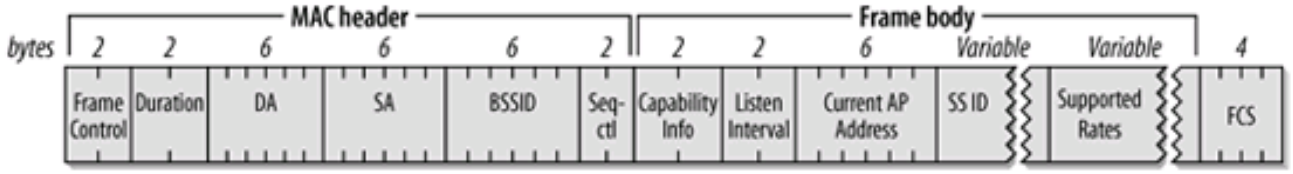
取消关联、解除验证帧

6. Association Request



关联请求帧

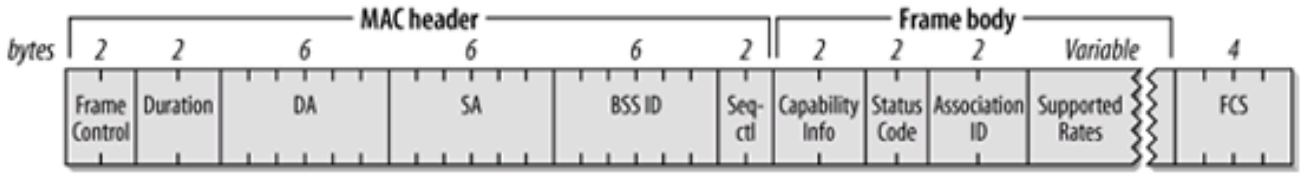
7. Reassociation Request



重新关联

8. Association Response and Reassociation Response

关联响应，重新关联响应



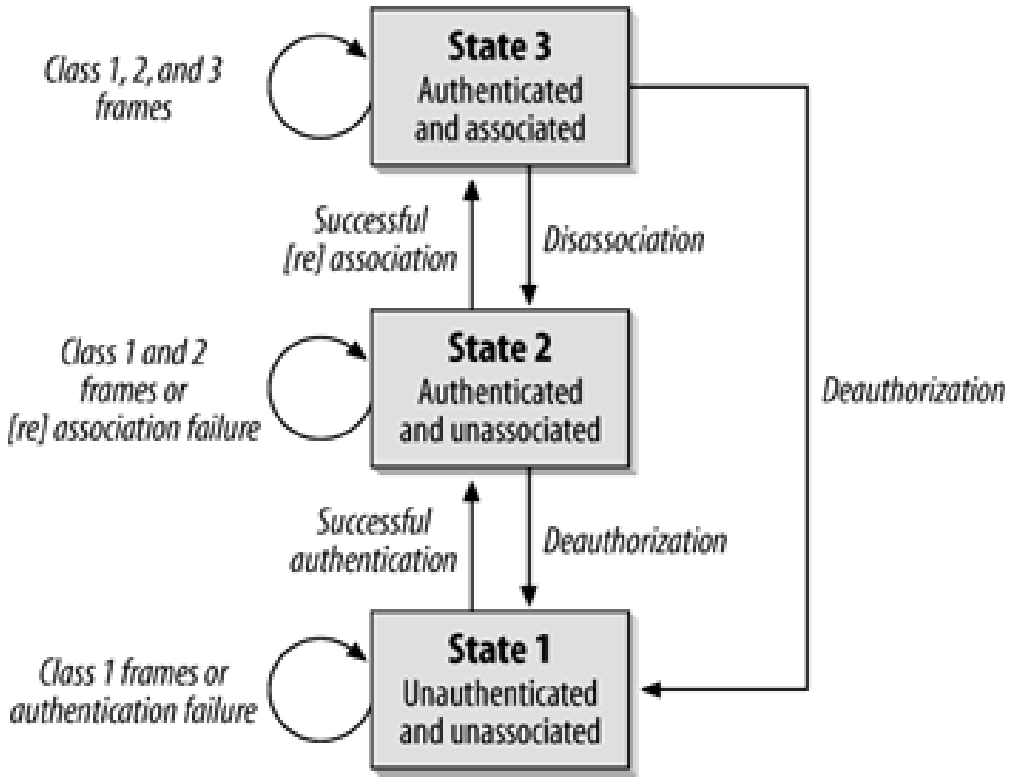
9. Authentication身份验证帧

身份验证帧

Authentication Algorithm Number ：用于算法选择

10. Action frame

帧传送、关联与身份验证的状态



状态图

State1：未经认证且尚未关联
State2：已经认证但尚未关联
State3：已经认证且已经关联

帧等级分类

	控制帧	管理帧	数据帧
第一级帧	Request to Send (RTS)	Probe Request	ToDS 或 FromDS 位都设为 0 的所有帧
	Clear to Send (CTS)	Probe Response	
	Acknowledgment (ACK)	Beacon	

	CF-End	Authentication	
	CF-End+CF-Ack	Deauthentication	
		Announcement Traffic Indication Message (ATIM)	
第二级帧	None	Association Request/Response	None
		Reassociation Request/Response	
		Disassociation	
第三级帧	PS-Poll	Deauthentication	任何帧，包含 ToDS 或 FromDS 位都设为 1 的所有帧

madwifi

1.
madwifi的结构，主要是有三层，hal是硬件层，然后是ath层，在之上的是802.11层，整个madwifi源码中重要的就是hal文件夹（硬件），ath文件夹，ath_rate文件夹 ，net80211文件夹（802.11协议相关），tools文件夹（一些工具）

当驱动被加载的时候，它会取探测物理设备是否存在，然后通过ath_attach()函数安装此设备。同时，驱动会自动创建一个虚拟的网络接口，通过函数ieee80211_create_vap( )实现。这个虚拟网络接口的初始状态为INIT，在此状态下硬件不会接收数据包。

当实际的AP接口开始工作（例如通过ifconfig ath0 up命令激活），驱动会将对硬件进行适当的设置并且进入SCAN状态。

在SCAN状态下，AP会扫描所有它支持的通道。
扫描包括两个方面，一个是主动扫描，即AP会发送适当的请求报文；一个是被动扫描，即AP监听临近AP的beacons。

在SCAN状态下，AP不会传输数据报。
在所有的通道都扫描完成以后，AP选择一个无线信号强度最低的通道然后进入RUN状态（ap_end( )）。

在RUN状态下，AP执行一个存取节点的普通操作。它约每隔100ms向外广播一个beacon消息（ath_beacon_send( )），

应答其它AP发送的请求，应答终端发送来的认证消息和连接/重连接消息，并且传输数据包。

当接口被关闭的时候，AP会发送取消认证消息到每一个连接了的终端，然后释放所它们所占有的资源并进入INIT状态。

需要注意控制消息的使用，如：RTS、CTS和ACK，它们是被驱动HAL（硬件抽象层）控制的。

结构体 ieee80211com中定义了各种帧处理函数指针
3. 数据接收

大多数的CSMA/CA机制被贯彻在HAL或者硬件中。当一个新的包到达时，开源的驱动部分是通过中断来获取通知的（ath_intr( )）。

包被linux的tasklet来处理（ath_rx_tasklet( )），这个包所在skb结构被找到并且它的目标节点正确。

函数ieee80211_input( )接收各种不同类型的包，在这个函数中管理报文包被传递给ieee80211_recv_mgmt( )函数处理，数据包被做相关的处理后变成以太帧格式然后传送给linux内核（netif_rx( )）或者，如果工作在桥模式下，则通过dev_queue_xmit( )发送此数据包

4. 数据的发送

Linux内核通过dev->hard_start_xmit轮流调用虚拟接口的ieee80211_hardstart()函数和物理接口的ath_hardstart（）函数实现包的传输。

ath_hardstart（）函数将以太格式的包封装成802.11格式的包。

ath_tx_start（）函数将需要加密的包进行加密处理，并将保存此包的skb映射到DMA缓冲，并根据包的优先级选定一个传输队列（QoS control）。ath_tx_txqaddbuf( )函数将映射后的缓冲（buffer）插入到选定的传输队列里面并通知HAL开始传输。

管理帧由802.11层产生。它们通过ieee80211_mgmt_output（）函数发送。

Beacon消息由HAL触发。当发送beacon消息的时间到达，HAL会制造一个中断，然后调用函数ath_beacon_send( )来发送。Beacon消息直接被传递到HAL并发送。

HAL成功发送完一个包后也会产生一个中断来通知驱动。

函数ath_tx_tasklet()会更新发送相关的信息。如果有工作在监视模式（monitor mode）的虚拟端口存在，

这个包会在函数ath_tx_capture()中被传递给监视接口。

5　madwifi加载到内核的顺序

：

```
insmod wlan.o
insmod ath_hal.o
insmod ath_rate_amrr.o
insmod ath_rate_onoe.o
insmod ath_rate_sample.o
insmod wlan_acl.o
insmod wlan_ccmp.o
insmod wlan_scan_ap.o
insmod wlan_scan_sta.o
insmod wlan_tkip.o
insmod wlan_wep.o
insmod wlan_xauth.o
insmod ath_pci.o
```