



# 中华人民共和国国家标准

GB 15629.11—2003

*Anywlan*

*Anywhere WLAN! Anytime WLAN!!*  
中国无线门户!

## 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分: 无线局域网媒体访问控制和物理层规范

Information technology—Telecommunications and information exchange  
between systems—Local and metropolitan area networks—Specific  
requirements—Part 11: Wireless LAN Medium Access Control (MAC)  
and Physical Layer (PHY) Specifications

(ISO/IEC 8802-11:1999, MOD)

全国信息技术标准化技术委员会 中国宽带无线IP标准工作组	赠送
<a href="http://www.chinabwips.org">http://www.chinabwips.org</a>	

2003-05-12 发布

2003-12-01 实施

中华人民共和国  
国家质量监督检验检疫总局 发布

***Anywlan***

***Anywhere WLAN!Anytime WLAN!!***

**中国无线门户!**

## 目 次

前言	X III
引言	X V
1 综述	1
1.1 范围	1
1.2 目的	1
2 规范性引用文件	1
3 术语和定义	2
4 缩略语	6
5 一般描述	9
5.1 体系结构的一般描述	9
5.1.1 无线网络如何不同	9
5.2 本部分体系的组成部分	10
5.2.1 独立 BSS 作为 ad hoc 网	10
5.2.2 分布式系统概念	10
5.2.3 区域概念	12
5.2.4 与有线 LAN 的集成	13
5.3 逻辑服务接口	13
5.3.1 STA 服务(SS)	14
5.3.2 分布式系统服务(DSS)	14
5.3.3 多逻辑地址空间	15
5.4 服务综述	15
5.4.1 DS 内的消息分发	16
5.4.2 支持分布式服务的服务	16
5.4.3 访问与机密性控制服务	17
5.5 服务之间的关系	18
5.5.1 第 1 类帧(状态 1、2、3 与 4 均允许)	19
5.5.2 第 2 类帧(当且仅当已链路验证的状态 2、3、4 允许)	20
5.5.3 第 3 类帧(当且仅当已关联的状态 3、4 允许)	20
5.5.4 第 4 类帧(当且仅当已鉴别的状态 4 允许)	20
5.6 ESS 与 IBSS LAN 之间的区别	21
5.7 支持服务的消息信息内容	21
5.7.1 数据	21
5.7.2 关联	22
5.7.3 重新关联	22
5.7.4 解除关联	22
5.7.5 保密	23
5.7.6 链路验证	23
5.7.7 解除链路验证	23
5.8 参考模型	23

## GB 15629.11—2003

6	MAC 服务定义	24
6.1	MAC 服务综述	24
6.1.1	异步数据服务	24
6.1.2	安全服务	24
6.1.3	MSDU 排序	24
6.2	详细服务规范	25
6.2.1	MAC 数据服务	25
7	帧格式	27
7.1	MAC 帧格式	27
7.1.1	约定	27
7.1.2	一般帧格式	28
7.1.3	帧字段	28
7.2	独立类型帧格式	32
7.2.1	控制帧	32
7.2.2	数据帧	34
7.2.3	管理帧	35
7.3	管理帧帧体组成部分	38
7.3.1	固定字段	38
7.3.2	信息元素	41
8	鉴别与保密	44
8.1	鉴别服务	44
8.1.1	系统和端口	44
8.1.2	受控和非受控接入	45
8.2	鉴别服务单元(ASU)	46
8.2.1	公钥证书	47
8.2.2	公钥证书管理	48
8.2.3	椭圆曲线数字签名算法	49
8.3	WAI 鉴别基础结构	49
8.3.1	安全接入	49
8.3.2	WAI数据格式	51
8.4	WPI 保密基础结构	55
8.5	安全相关管理信息库	55
8.5.1	与鉴别相关的 MIB 属性	55
8.5.2	与保密相关的 MIB 属性	56
8.6	自组网(ad hoc)模式	56
9	MAC 子层功能	56
9.1	MAC 体系结构	56
9.1.1	分布式协调功能(DCF)	57
9.1.2	点协调功能(PCF)	57
9.1.3	DCF 和 PCF 的共存	57
9.1.4	分段/重组综述	57
9.1.5	MAC 数据服务	58
9.2	分布式协调功能(DCF)	58

9.2.1	载波侦听机制	59
9.2.2	MAC 级确认	59
9.2.3	帧间间隔(IFS)	59
9.2.4	随机退避时间	61
9.2.5	DCF 访问规程	62
9.2.6	定向 MPDU 的传送规程	66
9.2.7	广播与组播 MPDU 的传送规程	67
9.2.8	ACK规程	67
9.2.9	重复帧的检测与恢复	67
9.2.10	DCF 的定时关系	68
9.3	PCF	69
9.3.1	CFP 结构与定时	70
9.3.2	PCF 访问规程	71
9.3.3	PCF 传送规程	72
9.3.4	无竞争轮询列表	74
9.4	分段	75
9.5	重组	76
9.6	多速率支持	76
9.7	帧交换序列	77
9.8	MSDU 传输限制	78
10	层管理	78
10.1	管理模型综述	78
10.2	通用管理原语	78
10.3	MLME SAP 接口	80
10.3.1	功率管理	80
10.3.2	扫描	81
10.3.3	同步	83
10.3.4	链路验证	84
10.3.5	解除链路验证	85
10.3.6	关联	86
10.3.7	重新关联	88
10.3.8	解除关联	89
10.3.9	重新设置	90
10.3.10	启动	91
10.4	PLME SAP 接口	93
10.4.1	PLME-RESET.request	93
10.4.2	PLME-CHARACTERISTICS.request	93
10.4.3	PLME-CHARACTERISTICS.confirm	93
10.4.4	PLME-DSSSTESTMODE.request	95
10.4.5	PLME-DSSSTESTOUTPUT.request	96
11	MAC 子层管理实体	97
11.1	同步	97
11.1.1	基本方法	97

**GB 15629.11—2003**

11.1.2	维持同步	97
11.1.3	获取同步、扫描	98
11.1.4	调整 STA 定时器	100
11.1.5	频率跳变(FH)物理层定时同步	100
11.2	功率管理	101
11.2.1	基础结构网中的功率管理	101
11.2.2	IBSS 中的功率管理	104
11.3	关联和重新关联	107
11.3.1	STA 关联规程	107
11.3.2	AP 关联规程	107
11.3.3	STA 重新关联规程	107
11.3.4	AP 重新关联规程	107
11.4	管理信息库(MIB)定义	107
12	物理层(PHY)服务规范	108
12.1	范围	108
12.2	PHY 功能	108
12.3	PHY 服务详细规范	108
12.3.1	应用范围和领域	108
12.3.2	服务综述	108
12.3.3	相互作用概述	108
12.3.4	基本服务和选项	108
12.3.5	PHY-SAP详细服务规范	109
13	PHY 管理	113
14	2.4GHz 工业、科学和医疗(ISM)频段的频率跳变扩展频谱(FHSS)物理层规范	113
14.1	综述	113
14.1.1	FHSS PHY 综述	113
14.1.2	FHSS PHY 功能	113
14.1.3	服务规范方法和记法	114
14.2	FHSS PHY 特定服务参数列表	114
14.2.1	综述	114
14.2.2	TXVECTOR 参数	114
14.2.3	RXVECTOR 参数	114
14.3	FHSS PLCP 子层	115
14.3.1	综述	115
14.3.2	PLCP 帧格式	115
14.3.3	PLCP 状态机	117
14.4	PLME SAP 层管理	127
14.4.1	综述	127
14.4.2	FH PHY 专用 MAC 子层管理实体(MLME) 规程	127
14.4.3	FH PHY 层的管理实体状态机	127
14.5	FHSS PMD 子层服务	129
14.5.1	应用范围和领域	129
14.5.2	服务综述	130

## GB 15629.11—2003

14.5.3	相互作用综述	130
14.5.4	基本服务和选项	130
14.5.5	PMD_SAP详细服务规范	130
14.6	FHSS PMD 子层, 1.0 Mbit/s	133
14.6.1	1Mbit/s PMD 操作规范综述	133
14.6.2	规章要求	134
14.6.3	工作频率范围	134
14.6.4	工作信道数	135
14.6.5	工作信道中心频率	135
14.6.6	占用的信道带宽	137
14.6.7	最小跳频速率	137
14.6.8	跳频序列	137
14.6.9	无用发射	139
14.6.10	调制	139
14.6.11	信道数据速率	140
14.6.12	信道切换/驻留时间	140
14.6.13	接收到发送的切换时间	140
14.6.14	PMD发射规范	140
14.6.15	PMD接收机规范	141
14.6.16	工作温度范围	142
14.7	FHSS PMD 子层, 2Mbit/s	142
14.7.1	综述	142
14.7.2	4 相 GFSK 调制	142
14.7.3	信道数据速率	143
14.8	FHSS PHY 管理信息库(MIB)	144
14.8.1	综述	144
14.8.2	FH PHY 属性	144
14.9	FH PHY 参数	149
15	为 ISM 应用指定的 2.4GHz 频段的直接序列扩展频谱(DSSS)PHY 规范	150
15.1	综述	150
15.1.1	范围	151
15.1.2	DSSS PHY 功能	151
15.1.3	服务规范方法和记法	151
15.2	DSSS PLCP 子层	151
15.2.1	综述	151
15.2.2	PLCP 帧格式	151
15.2.3	PLCP 字段定义	152
15.2.4	PLCP/DSSS PHY 数据加扰器和解扰器	154
15.2.5	PLCP 数据调制和调制速率改变	155
15.2.6	PLCP 发送规程	155
15.2.7	PLCP 接收规程	157
15.3	DSSS 物理层管理实体(PLME)	159
15.3.1	PLME_SAP 子层管理原语	159

## GB 15629.11—2003

15.3.2	DSSS PHY MIB	159
15.3.3	DS PHY 特性	161
15.4	DSSS PMD 子层	162
15.4.1	应用范围和领域	162
15.4.2	服务综述	162
15.4.3	相互作用综述	162
15.4.4	基本服务与选项	162
15.4.5	PMD_SAP 详细服务规范	164
15.4.6	PMD 总体操作规范	168
15.4.7	PMD 发射规范	170
15.4.8	PMD 接收机规范	173
16	红外线(IR)PHY 规范	174
16.1	综述	174
16.1.1	范围	175
16.1.2	IR PHY 功能	175
16.1.3	服务规范方法与记法	175
16.2	IR PLCP 子层	175
16.2.1	综述	175
16.2.2	PLCP 帧格式	176
16.2.3	PLCP 调制与速率改变	176
16.2.4	PLCP 字段定义	176
16.2.5	PLCP规程	177
16.3	IR PMD 子层	178
16.3.1	综述	179
16.3.2	PMD 总体操作规范	179
16.3.3	PMD 发射机规范	180
16.3.4	PMD 接收机规范	183
16.3.5	能量检测、载波侦听及 CCA 定义	183
16.4	PHY 属性	184
附录 A (规范性附录)	协议实现一致性声明(PICS)形式表	186
A.1	引言	186
A.2	缩略语和特殊符号	186
A.2.1	状态符号	186
A.2.2	缩略语	186
A.3	填写 PICS 形式表须知	186
A.3.1	PICS 形式表的通用结构	186
A.3.2	附加信息	187
A.3.3	异常信息	187
A.3.4	条件项目	187
A.4	PICS 形式表	188
A.4.1	实现识别	188
A.4.2	协议概要	188
A.4.3	IUT 配置	188



A.4.4	MAC 协议	188
A.4.5	FH PHY 功能	192
A.4.6	直接序列 PHY 功能	195
A.4.7	红外基带 PHY 功能	197
附录 B	(资料性附录) 跳频序列	200
附录 C	(规范性附录) MAC 操作的形式描述	212
C.1	MAC 正式说明	215
C.1.1	基本假设	215
C.1.2	记法约定	215
C.1.3	建模技术	215
C.2	MAC 状态机的数据类型和算子定义	216
C.3	用于 MAC 站的状态机	262
C.4	MAC 接入点的状态机	333
附录 D	(规范性附录) MAC 和 PHY 管理信息库的 ASN.1 编码	396
参考文献		439
图 1	基本服务集	10
图 2	分布式系统和接入点	11
图 3	扩展服务集	11
图 4	一个典型的信号强度图	12
图 5	排列覆盖区	13
图 6	与其他 GB 15629 LAN 的连接	13
图 7	本部分完整的体系结构	15
图 8	状态变量与服务间的关系	19
图 9	符合本部分的完整体系结构图	21
图 10	IBSS 逻辑体系结构	21
图 11	适用于本部分的基本参考模型构成	24
图 12	MAC 帧格式	28
图 13	帧控制字段	28
图 14	序列控制字段	32
图 15	控制帧中帧控制字段的子字段值	33
图 16	RTS 帧	33
图 17	CTS 帧	33
图 18	ACK 帧	33
图 19	PS-Poll 帧	34
图 20	CF-End 帧	34
图 21	CF-End+CF-ACK 帧	34
图 22	数据帧	34
图 23	管理帧格式	35
图 24	链路验证算法序号固定字段	38
图 25	链路验证交换序号固定字段	39
图 26	信标间隔固定字段	39
图 27	能力信息固定字段	39

## GB 15629.11—2003

图 28	当前 AP 地址固定字段	40
图 29	侦听间隔固定字段	40
图 30	原因码固定字段	40
图 31	AID 固定字段	40
图 32	状态码固定字段	41
图 33	时戳固定字段	41
图 34	元素格式	41
图 35	SSID 元素格式	42
图 36	支持速率元素格式	42
图 37	FH 参数集合元素格式	42
图 38	DS 参数集合元素格式	43
图 39	CF 参数集合元素格式	43
图 40	TIM 元素格式	43
图 41	IBSS 参数集合元素格式	44
图 42	鉴别器系统示意图	45
图 43	受控端口的鉴别状态	45
图 44	受控端口和非受控端口的用法	46
图 45	鉴别系统结构	46
图 46	基于 ASU 的 WAI 逻辑拓扑结构示意图	47
图 47	公钥证书的格式	47
图 48	STA 接入鉴别流程图	50
图 49	WAI 鉴别系统的数据分组基本格式	51
图 50	接入鉴别请求分组的数据字段	52
图 51	STA 证书内容定义	52
图 52	签名算法定义	52
图 53	证书有效期定义	53
图 54	接入鉴别响应分组的数据内容	53
图 55	STA 证书鉴别结果信息定义	53
图 56	AP 证书鉴别结果信息定义	54
图 57	密钥协商请求分组的数据内容	54
图 58	密钥协商响应分组的数据内容	54
图 59	WAI 鉴别系统的数据报文基本格式	55
图 60	证书鉴别请求报文的数据内容	55
图 61	证书鉴别响应报文的数据内容	55
图 62	MAC 体系结构	57
图 63	分段	58
图 64	IFS 之间的关系	60
图 65	CW 的指数方式增长示例	61
图 66	基本访问机制	62
图 67	退避规程	63
图 68	RTS/CTS/数据/ACK 和 NAV 设置	64
图 69	利用 SIFS 的多分段 MSDU 的传输	65
图 70	分段的 MSDU 与 RTS/CTS	65

图 71	具有发送优先权而没有得到确认的 RTS/CTS	66
图 72	直接数据/ACK 的 MPDU	67
图 73	DCF 的定时关系	69
图 74	CFP/CP 交替	70
图 75	信标帧和 CFP	70
图 76	延迟的信标和缩短的 CFP 示例	71
图 77	PCF 帧传送示例	72
图 78	GET 和 SET 操作	79
图 79	在忙网络上的信标传输	97
图 80	IBSS 中信标帧的传输	98
图 81	探测响应	100
图 82	基础结构网功率管理操作 (无 PCF 操作)	102
图 83	IBSS 中的功率管理—基本方法	105
图 84	状态图表注释示例	115
图 85	PLCP 帧格式	116
图 86	帧同步加扰器/解扰器	117
图 87	PLCP 数据白化器格式	117
图 88	PLCP 顶级状态图	118
图 89	发送状态机	119
图 90	数据白化编码规程	120
图 91	发送状态定时	123
图 92	CS/CCA 状态机	124
图 93	CS/CCA 状态定时	125
图 94	接收状态机	126
图 95	数据白化解码规程	126
图 96	接收定时	128
图 97	PLME 状态机	129
图 98	PMD 层参考模型	129
图 99	发送调制掩模	140
图 100	4 相 GFSK 发射调制	143
图 101	PLCP 帧格式	152
图 102	CCITT CRC-16 的实现	153
图 103	CRC 计算示例	154
图 104	数据加扰器	155
图 105	数据解扰器	155
图 106	PLCP 发送规程	155
图 107	PLCP 发送状态机	157
图 108	PLCP 接收规程	157
图 109	PLCP 接收状态机	159
图 110	PMD 层参考模型	162
图 111	发射频谱掩模	171
图 112	发射加电坡度	171
图 113	发射掉电坡度	171

## GB 15629.11—2003

图 114	调制精度测量示例	172
图 115	同基带眼图对齐的码片时钟	172
图 116	PLCPDU 帧格式	176
图 117	基本脉冲形状	180
图 118	发射机辐射模型掩模 1	181
图 119	掩模 2 设备方位图	182
图 120	发射机辐射模型掩模 2	182
图 121	发射频谱掩模	183
表 1	有效的类型和子类型的组合	29
表 2	数据类型帧中去往 DS 字段与来自 DS 字段的组合	29
表 3	持续时间/ID 字段编码	30
表 4	地址字段内容	35
表 5	信标帧体	36
表 6	解除关联帧体	36
表 7	关联请求帧体	37
表 8	关联响应帧体	37
表 9	重新关联请求帧体	37
表 10	重新关联响应帧体	37
表 11	探测请求帧体	37
表 12	探测响应帧体	38
表 13	链路验证帧体	38
表 14	解除链路验证帧体	38
表 15	STA 对 CF-Pollable 子字段和 CF-Poll 请求子字段的用法	39
表 16	AP 对 CF-Pollable 子字段和 CF-Poll 请求子字段的用法	39
表 17	原因码	40
表 18	状态码	41
表 19	元素 ID	42
表 20	帧序列	77
表 21	CF 帧序列	77
表 22	功率管理模式	101
表 23	PHY-SAP 对等对等服务原语	108
表 24	PHY-SAP 子层对子层服务原语	109
表 25	PHY-SAP 服务原语参数	109
表 26	向量描述	109
表 27	TXVECTOR 参数	114
表 28	RXVECTOR 参数	114
表 29	PSF 比特描述	116
表 30	PLCP 字段比特描述	121
表 31	PMD_SAP 对等服务原语	130
表 32	PMD_SAP 子层对子层服务原语	130
表 33	PMD 原语参数列表	130
表 34	发射功率等级	132

表 35	工作频率范围	135
表 36	工作信道数	135
表 37	中国、北美和欧洲标准 (除西班牙和法国)	135
表 38	日本标准	136
表 39	西班牙标准	136
表 40	法国标准	136
表 41	适用于中国、北美和欧洲大部分地区的基本跳频序列 $b(i)$	137
表 42	适用于西班牙的基本跳频序列 $b(i)$	138
表 43	适用于法国的基本跳频序列 $b(i)$	138
表 44	符号编码为载波偏移 (1Mbit/s, 2-GFSK)	139
表 45	1Mbit/s Dp	142
表 46	符号编码为载波偏移	142
表 47	2Mbit/s Dp	144
表 48	FHSS PHY 属性	144
表 49	管理域代码	146
表 50	支持的数据速率码(SupportedDataRatesTX)	147
表 51	支持的数据速率码(SupportedDataRatesRX)	147
表 52	发射天线编号	147
表 53	接收天线编号	148
表 54	分集支持码	148
表 55	分集选择天线码	148
表 56	发射功率等级	149
表 56a	FH PHY 参数	150
表 57	MIB 属性缺省值/范围	160
表 58	DS PHY 特征	161
表 59	PMD_SAP 对等对等服务原语	162
表 60	DSSS PMD_SAP 对等对等服务原语	163
表 61	PMD_SAP 子层对子层服务原语	163
表 62	PMD 原语参数列表	163
表 63	DSSS PHY 频率信道方案	169
表 64	1Mbit/s DBPSK 编码表	169
表 65	2Mbit/s DQPSK 编码表	169
表 66	发射功率电平	170
表 67	IR PMD_SAP 对等对等服务原语	178
表 68	16-PPM 基本速率映射	179
表 69	4-PPM 增强速率映射	179
表 70	作为发射机辐射掩模的函数的峰值光功率	180
表 71	发射机辐射模型掩模 1 的定义	181
表 72	发射机辐射模型掩模 2 的定义	181
表 73	接收机可视区的定义	183
表 74	IR PHY MIB 属性	184
表 75	IR PHY 特性	185
表 B.1	跳频序列组 1	200

**GB 15629.11—2003**

表 B.2 跳频序列组 2·····	204
表 B.3 跳频序列组 3·····	208

## 前 言

本部分的第8章、第14.6.2条、第14.6.3条、第15.4.6.1条、第15.4.6.5条、第15.4.7.1条、第15.4.7.5条、第16.3.3条为强制性的，其余为推荐性的。

本部分是《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求》的第11部分，修改采用 ISO/IEC 8802-11:1999《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制(MAC)和物理(PHY)层规范》(英文版)。

本部分是无线局域网媒体访问控制和物理层及其扩展的基础性规范。以下规范及相关扩展规范为其子项：

- 《无线局域网媒体访问控制和物理层规范：5GHz 频段高速物理层扩展规范》
- 《无线局域网媒体访问控制和物理层规范：2.4GHz 频段较高速物理层扩展规范》
- 《无线局域网媒体访问控制和物理层规范：附加管理区域内的工作扩展规范》
- 《无线局域网媒体访问控制和物理层规范：服务质量的 MAC 层增强规范》
- 《无线局域网媒体访问控制和物理层规范：接入点间工作规范》
- 《无线局域网媒体访问控制和物理层规范：2.4GHz 频段较高速(速率大于 20Mbit/s)扩展》
- 《无线局域网媒体访问控制和物理层规范：5GHz 频段频谱管理》
- 《无线局域网媒体访问控制和物理层规范：安全的 MAC 层增强规范》

本部分修改采用 ISO/IEC 8802-11:1999，与 ISO/IEC 8802-11:1999 相比，主要差异如下：

- 按照汉语习惯对一些编排格式进行修改；
- 标准的结构和编写规则按 GB/T 1.1—2000；
- 本部分与 ISO/IEC 8802.11:1999 的主要差异在于标准中涉及的无线局域网安全部分。原文的第8章“鉴别与保密”采用 WEP 机制来实现无线局域网中的鉴别和加密，而目前 WEP 机制已被广泛证实不具备等效于有线的安全性，故不采纳；  
本部分采用了 WAPI 机制实现无线局域网的安全，并按照 1999 年 10 月 7 日颁布的中华人民共和国国务院令 273 号《商用密码管理条例》，已送交国家密码管理委员会办公室审定并获批准。  
WAPI 机制的主要表述在本部分的第8章“鉴别与保密”。
- 本部分中采用的 WAPI 机制也向 ISO 授权的相关机构进行了提交，经审查获得认可，并分配了用于该机制的以太类型字段 (IEEE EtherType Field) 0x88B4；
- 由于“鉴别与保密”机制的差异，相应的除第8章之外的图、表和内容作了调整；
- 与 WAPI 相关联，原 5.4.3.1“鉴别”改为“链路验证”，原 5.4.3.4“保密”的内容也作了修改，本部分中的 5.4.3.3“鉴别”为新增内容；
- 在与无线电发射规范有关的章条和附录中增加了中国的内容；
- 除安全相关部分外，本部分与 ISO/IEC 8802.11:1999 兼容互通；
- 第4章删除了缩略语 ppm。删除的原因为 GB/T 1.1—2000 附录 F 中 h) 规定不应使用；
- 增加的缩略语有 AE (鉴别器实体)、ASU (鉴别服务单元)、ASUE (鉴别请求者实体)、OSI (开放系统互连)、WAI (无线局域网鉴别基础结构)、WAPI (无线局域网鉴别与保密基础结构)、WLAN (无线局域网) 和 WPI (无线局域网保密基础结构)，其中 AE、

**GB 15629.11—2003**

ASU、ASUE、WAI、WAPI 和 WPI 为本部分新定义的缩略语；

——全文删除了原图 42～图 46，新增图 20 个（图 42～图 61）。全文共增加图号 15 个（原文最后图号为 106，现为 121）。相应地，图号也作了调整；

本部分的附录 A、附录 C 和附录 D 为规范性附录，附录 B 为资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子技术标准化研究所归口。

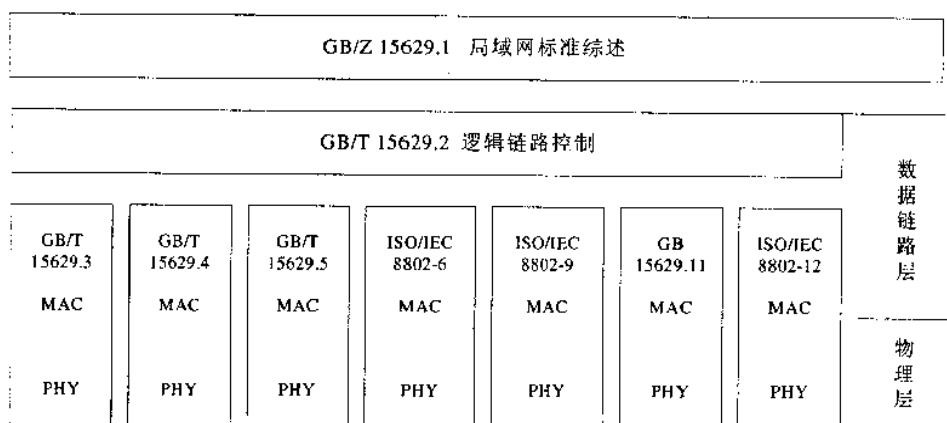
本部分由西安西电捷通无线网络通信有限公司负责起草，参加单位有国家无线电监测中心、国家商用密码研究中心、中国电子技术标准化研究所、西安电子科技大学和西安邮电学院。

本部分主要起草人：黄振海、郭宏、王育民、铁满霞、张变玲、徐冬梅、阚润田、许福英、雷鸣、焦彤彤、唐厚俭、吴立刚、李大为、常若艇、黄家英、李建东、朱志祥、陈翀。



## 引 言

本部分是局域网(LAN)和城域网(MAN)系列标准的一个部分。本部分与该系列其他几部分之间的关系如下图所示。



本系列标准涉及开放系统互连基本参考模型(GB/T 9387.1)定义的物理层和数据链路层。媒体访问标准定义了七种类型的媒体访问技术和相关的物理媒体,其中每一种适用于特定的应用,或针对特定的系统目标。其他类型正在研究过程中。

定义媒体访问技术的标准如下:

- GB/T 15629.3, 利用带碰撞检测的载波侦听多址访问(CSMA/CD)作为访问方法;
- GB/T 15629.4, 利用令牌传递总线作为访问方法;
- GB/T 15629.5, 利用令牌传递环作为访问方法;
- ISO/IEC 8802-6, 利用分布式排队双总线作为访问方法;
- ISO/IEC 8802-9, 为骨干网提供综合业务的统一的访问方法;
- GB 15629.11, 利用带碰撞避免的载波侦听多址访问(CSMA/CA)作为访问方法的无线局域网;
- ISO/IEC 8802-12:1998, 利用要求优先权作为访问方法。

GB/Z 15629.1, 局域网标准综述, 提供 GB/T 15629 标准系列的综述;

GB/T 15629.2, 逻辑链路控制, 和媒体访问标准一起向网络层协议提供数据链路层服务;

GB/T 18236.1, 媒体访问控制(MAC)服务定义, 确定了由所有 GB/T 15629 的局域网 MAC 提供的通用 MAC 服务的特征。MAC 服务以原语形式进行定义, 该原语能在对等服务用户、它们的参数、它们的相互关系和有效序列及服务的关联事件之间进行传递。

ISO/IEC 15802-2, LAN/MAN 管理, 定义了与 OSI 管理相兼容的体系结构, 以及用于在 LAN/MAN 环境中实现远程管理的服务和协议元素;

ISO/IEC 15802-3, 媒体访问控制(MAC)网桥, 规定了在逻辑链路控制协议层以下用于 GB/T 15629 局域网互连的体系结构和协议;

**GB 15629.11—2003**

ISO/IEC 15802-4, 系统负荷协议, 规定了考虑在 GB/T 15629 局域网上加载系统, 用于管理方面的一套服务和协议;

ISO/IEC 15802-5, 远程媒体访问控制(MAC)桥接, 规定了在逻辑链路控制协议层以下, 在物理分离的 GB/T 15629 局域网之间采用非局域网的通信技术进行互连的扩展。

# 信息技术 系统间远程通信和信息交换

## 局域网和城域网 特定要求

### 第 11 部分：无线局域网媒体访问控制和物理层规范

#### 1 综述

##### 1.1 范围

《信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求》的本部分（以下简称本部分）规定了局部区域范围内用于固定式、便携式与移动式站（点）无线连通性的媒体访问控制(MAC)和物理层(PHY)规范。

##### 1.2 目的

本部分的目的是为局部区域内需要快速部署的自动装置、设备或站提供无线连通性，它们可以是便携的或手持的，也可以是车载的。为了局部区域通信，本部分也为管理机构使用一个或多个频段提供了标准化方法。

本部分明确地

- 描述了符合本部分的设备在白组网和基础结构网中进行操作所必需的功能和服务，同时也描述了这些网络内的站移动性特征；
- 定义了 MAC 规程，以支持异步 MAC 服务数据单元（MSDU）交付服务；
- 定义了几种由本部分 MAC 控制的 PHY 信令技术和接口功能；
- 允许符合本部分的设备在一个 WLAN 内能操作，而该 WLAN 可与多个重叠覆盖的 WLAN 共存；
- 描述了要求和规程，以便为在无线媒体上传送的用户信息提供保密，并对符合本部分的设备进行身份鉴别。

#### 2 规范性引用文件

下列文件中的条款通过 GB 15629.11 的引用而成为本部分的条款。凡是标注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不标注日期的引用文件，其最新版本适用于本部分。

GB 7247.1-2001 激光产品的安全 第 1 部分：设备分类、要求和用户指南（idt IEC 60825-1:1993）

GB/T 9387.1-1998 信息技术 开放系统互连 基本参考模型 第 1 部分：基本模型（idt ISO/IEC 7498-1:1994）

GB/T 15629.2 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 2 部分：逻辑链路控制（GB/T 15629.2-1995，idt ISO/IEC 8802-2:1998）

ISO/IEC 8824-1:1995 信息技术 抽象句法表記法—(ASN.1)：基本记法规范

ISO/IEC 8824-2:1995 信息技术 抽象句法表記法—(ASN.1)：信息客体规范

## GB 15629.11—2003

- ISO/IEC 8824-3:1995 信息技术 抽象句法标记法一(ASN.1): 限制规范  
ISO/IEC 8824-4:1995 信息技术 抽象句法标记法一(ASN.1): 参数化 ASN.1 规范  
ISO/IEC 8825-1:1995 信息技术 ASN.1 编码规则: 基本编码规则(BER)、正则编码规则(CER)和特异编码规则(DER)的规范  
ISO/IEC 8825-2:1996 信息技术 ASN.1 编码规则: 包编码规则(PER)规范  
GB/T 18236.1 信息技术 系统间远程通信和信息交换 局域网和城域网 公共规范 第 1 部分: 媒体访问控制(MAC)服务定义 (idt ISO/IEC 15802-1:1995)  
ITU 无线电规章 卷 1-4  
ITU-T 建议 X.210(11/93) 信息技术 开放系统互连 基本参考模型: OSI 服务定义的约定 (与 ISO/IEC 是公用文本)  
ITU-T 建议 Z.100(03/93) CCITT 规范和描述语言(SDL)  
ITU-T 建议 Z.105(03/95) 与 ASN.1 结合的 SDL(SDL/ASN.1)

### 3 术语和定义

下列术语和定义适用于本部分。

#### 3.1

**访问控制** access control

防止非授权使用资源。

#### 3.2

**接入点 (AP)** access point (AP)

任何一个具备站点功能, 通过无线媒体为关联的站点提供访问分布式服务的能力的实体。

#### 3.3

**自组网** ad hoc network

仅由下列站 (点) 组成的网络, 这些站点通过无线媒体 (WM) 位于网内其他任意一个站的通信范围之内。ad hoc 网是以自发方式典型创建的。ad hoc 网络与其他网络区别的主要特征是有限的时间和空间范围。这些限定允许非常简单和方便地创建和解除 ad hoc 网络, 以使 ad hoc 网络可被网络设施的非技术性用户所使用; 即除要加入 ad hoc 网络的站 (点) 之外无需专门的技能, 并且需要的时间和其他资源的投入很少或没有。术语 ad hoc 常被用作独立基本服务集 (IBSS) 的俗称。

#### 3.4

**关联** association

用于建立接入点/站 (AP/STA) 之间的映射, 并且使站 (点) 能调用分布式系统服务 (DSSs) 的服务。

#### 3.5

**鉴别** authentication

一种服务, 它用于建立站点的身份授权, 以便关联至站点集内的其他成员。

#### 3.6

**基本服务区 (BSA)** basic service area (BSA)

概念性区域, 在其中基本服务组的成员可以进行通信。

#### 3.7

**基本服务组 (BSS)** basic service set (BSS)

受单个协调功能所控制的站集合。

#### 3.8

**BSS 基本速率集** BSS basic rate set

BSS 的所有 STA 均能接收来自无线媒体 (WM) 或向 WM 发送帧的数据传输速率的集合。对于 BSS 中所有 STA 基本速率集的数据速率都是预先设定的。

## 3. 9

**广播地址** broadcast address

规定所有站 (点) 的惟一组播地址。

## 3. 10

**信道** channel

用于传递协议数据单元(PDU)目的的一种媒体实例, 信道可在相同的空间内与相同物理层(PHY)的其他实例所用的媒体的其他实例 (其他信道) 同时使用, 信道间由于相互干扰所造成的帧差错率应低至可接受的范围。一些物理层(PHY)仅提供一个信道, 而其他的物理层提供多个信道。信道类型的例子如下表所示:

单信道	n-信道
窄带射频(RF)信道	频分复用信道
基带红外线	带码分多址的直接序列扩频(DSSS)

## 3. 11

**空闲信道评定功能(CCA)** clear channel assessment (CCA) function

确定无线媒体 (WM) 当前使用状态的一种物理层(PHY)逻辑功能。

## 3. 12

**机密性** confidentiality

不提供给或不泄漏给未授权个体、实体或进程的信息特性。

## 3. 13

**协调功能** coordination function

确定工作在 BSS 内的站点何时利用无线媒体 (WM) 接收发送协议数据单元 (PDU) 的逻辑功能。BSS 内的协调可能有一种点协调功能 (PCF), 并且包含一种分布式协调功能 (DCF)。

## 3. 14

**可轮询的协调功能** coordination function pollable

一个站 (点) 能够: (1) 用排队的可生成的数据帧响应协调功能轮询; (2) 解释发送或来自点协调器的确认。

## 3. 15

**解除鉴别** deauthentication

使现有的鉴别关系无效的服务。

## 3. 16

**定向地址** directed address

见单播帧。

## 3. 17

**解除关联** disassociation

一种服务, 它用于撤销现有的关联。

## 3. 18

**分布式协调功能(DCF)** distributed coordination function (DCF)

只要网络在运行, 相同的协调功能逻辑在 BSS 的每个站点中均处于活动状态的一类协调功能。

## 3. 19

**分发** distribution

在分布式系统 (DS) 中利用关联信息交付媒体访问控制 (MAC) 服务数据单元 (MSDU) 的服

**GB 15629.11—2003**

务。

**3.20**

**分布式系统(DS) distribution system (DS)**

用于将 BSS 集合与集成的局域网互连起来而创建扩展服务集的系统。

**3.21**

**分布式系统媒体(DSM) distribution system medium (DSM)**

ESS 中 DS 使用的媒体或媒体集, 用于 ESS 内的 AP 和泛端口之间的通信。

**3.22**

**分布式系统服务(DSS) distribution system service (DSS)**

由 DS 提供的服务集, 它使通过单一无线媒体实例彼此不能直接通信的站点间运输 MAC 服务数据单元(MSDU)。这些服务包括 ESS 内 AP 之间的 MSDU 运输, ESS 内 BSS 与泛端口之间的 MSDU 传送以及同一 BSS 内站点之间的 MSDU 传送。在最后一种情况中 MSDU 的目的地址为组播地址或广播地址, 也可以为单一地址, 但发送 MSDU 的站点选择包含 DSS。DSS 由本部分定义的 MAC 对提供。

**3.23**

**扩展速率集(ERS) extended rate set (ERS)**

由站(点)(如果有)支持的在扩展服务集(ESS)基本速率集之外的数据传送速率集。这个集可以包含由未来物理层(PHY)标准定义的数据传送速率。

**3.24**

**扩展服务区(ESA) extended service area (ESA)**

扩展服务集(ESS)的成员可以进行通信的概念性区域。ESA 大于或等于基本服务区(BSA), 可能包含重叠、不链接或二者都配置的几个基本服务集(BSSs)。

**3.25**

**扩展服务集(ESS) extended service set (ESS)**

由一个或多个互连的 BSS 与集成的局域网(LAN)构成的集合, 对与其中某个 BSS 站点关联的任何站的逻辑链路控制层而言, 它表现为单个的 BSS。

**3.26**

**高斯频移键控(GFSK) Gaussian frequency shift keying (GFSK)**

数据首先在基带被高斯滤波器滤波, 然后采用简单频率调制的一种调制方案。

**3.27**

**独立基本服务组(IBSS) independent basic service set (IBSS)**

能构成一个白包含网络并且不能访问 DS 的 BSS。

**3.28**

**基础结构 infrastructure**

基础结构包括分部式系统媒体(DSM)、接入点(AP)和泛端口实体。它还是扩展服务集(ESS)内的分部服务功能和集成服务功能的逻辑位置。一个基础结构除 DS 外, 还包含有一个或多个 AP 及零个或多个泛端口。

**3.29**

**集成 integration**

能够在 DS 和一个现有的非本部分局域网(通过泛端口)之间交付媒体接入控制(MAC)服务数据单元(MSDU)的一种服务。

**3.30**

**媒体访问控制(MAC)管理协议数据单元(MMPDU) MAC management protocol data unit(MMPDU)**

两个对等 MAC 实体之间为实现 MAC 管理协议所交换的数据单元。

3.31

MAC 协议数据单元(MPDU) MAC protocol data unit (MPDU)

两个对等 MAC 实体之间利用 PHY 层服务所交换的数据单元。

3.32

MAC 服务数据单元(MSDU) MAC service data unit (MSDU)

MAC 服务访问点 (SAP) 之间作为单元而交付的信息。

3.33

最小一致性网络 minimally conformant network

在单个基本服务区 (BSA) 内的两个站 (点) 符合本部分的网络。

3.34

移动站 (点) mobile station

在移动中使用网络进行通信的一种类型的站 (点)。

3.35

组播 multicast

组比特置位的 MAC 地址。组播 MSDU 是一个具有组播目的地址的 MSDU, 组播 MPDU 或者组播控制帧是一个具有组播接收地址的 MPDU。

3.36

网络分配向量(NAV) network allocation vector (NAV)

由每个站点维护的时间段指示器。在该时间段内, 无论站的 CCA 功能是否侦听到无线媒体空闲, 均不能在无线媒体上开始发送。

3.37

点协调功能(PCF) point coordination function (PCF)

一类可选的协调功能, 按这类功能, 在网络处于工作状态的任何给定时刻, BSS 内只有一个站点的协调功能逻辑处于活动状态。

3.38

便携站 (点) portable station

可以从一个位置移动到另一个位置, 但只有在处于固定位置 (静止) 时才进行网络通信的一种站点类型。

3.39

泛端口 portal

逻辑点, 来自非本部分 LAN 的 MSDU 在本逻辑点上进入 ESS 中的 DS。

3.40

保密 privacy

一种服务, 它用于防止非预期接收者读取消息内容。

3.41

重新关联 reassociation

一种服务, 它使已建立的关联 (AP 和站点之间) 从 AP 能转移到另一个 (或同一个) AP。

3.42

站 (点) (STA) station (STA)

包含符合本部分的与无线媒体的 MAC 和 PHY 接口的任何设备。

3.43

STA 基本速率 station basic rate

## GB 15629.11—2003

属于 ESS 基本速率集的一种数据传送速率,它用于 STA 的特定传输。STA 基本速率可随每次媒体访问控制(MAC)协议数据单元(MPDU)的传输尝试而频繁地动态变化。

## 3.44

STA 服务(SS) station service (SS)

服务集,它支持在基本服务集(BSS)内的 STA 之间运输媒体访问控制(MAC)服务数据单元(MSDU)。

## 3.45

时间单元(TU) time unit (TU)

等于 1024 $\mu$ s 的时间度量。

## 3.46

未授权泄漏 unauthorized disclosure

使信息能被未授权的个体、实体或进程获得的过程。

## 3.47

未授权的资源利用 unauthorized resource use

与安全策略不一致的资源利用。

## 3.48

单播帧 unicast frame

发往单一接收者的、非广播或组播的帧。同:定向地址。

## 3.49

无线局域网鉴别与保密基础结构(WAPI) wireless local area network authentication and privacy infrastructure (WAPI)

本部分规定的用于提供无线局域网中的身份鉴别和数据机密性的安全方案。由无线局域网鉴别基础结构(WAI)和无线局域网保密基础结构(WPI)组成。

## 3.50

无线媒体(WM) wireless medium (WM)

用于在 WLAN 的对等物理层实体之间实现传送协议数据单元(PDU)的媒体。

## 4 缩略语

ACK	确认
AE	鉴别器实体
AID	关联标识符
AP	接入点
ASE	鉴别服务实体
ASU	鉴别服务单元
ASUE	鉴别请求者实体
ATIM	通告通信量指示消息
BSA	基本服务区
BSS	基本服务集
BSSID	基本服务集标识
CCA	空闲信道评定
CF	无竞争
CFP	无竞争期



GB 15629.11—2003

CID	连接标识符
CP	竞争期
CRC	循环冗余码
CS	载波侦听
CTS	清除待发
CW	竞争窗口
DA	目的地址
DBPSK	差分二进制相移键控
DCE	数据通信设备
DCF	分布式协调功能
DCLA	直流电平调整
DIFS	分布式（协调功能）帧间间隔
DLL	数据链路层
Dp	退敏
DQPSK	差分正交相移键控
DS	分布式系统
DSAP	目的服务访问点
DSM	分布式系统媒体
DSS	分布式系统服务
DSSS	直接序列扩频
DTIM	交付通信量指示消息
ECC	椭圆曲线密码算法
ED	能量检测
EIFS	扩展的帧间间隔
EIRP	等效全向辐射功率
ERS	扩展速率集
ESA	扩展服务区
ESS	扩展服务集
FC	帧控制
FCS	帧检验序列
FER	帧差错率
FH	跳频
FHSS	跳频扩频
FIFO	先进先出
GFSK	高斯频移键控
IBSS	独立基本服务集
IDU	接口数据单元
IFS	帧间间隔
IMp	交调保护
IR	红外线
ISM	工业、科学和医疗
LAN	局域网
LLC	逻辑链路控制

**GB 15629.11—2003**

LME	层管理实体
LRC	长重传计数
lsb	最低有效位
MAC	媒体访问控制
MIB	管理信息库
MDF	管理定义字段
MLME	MAC 子层管理实体
MMPDU	MAC 管理协议数据单元
MPDU	MAC 协议数据单元
msb	最高有效位
MSDU	MAC 服务数据单元
N/A	不适用的
NAV	网络分配向量
OSI	开放系统互连
PC	点协调器
PCF	点协调功能
PDU	协议数据单元
PHY	物理层
PHY-SAP	物理层-服务访问点
PIFS	点(协调功能)帧间间隔
PLCP	物理层会聚协议
PLME	物理层管理实体
PMD	依赖于物理媒体
PN	伪随机噪声(码序列)
PPDU	PLCP 协议数据单元
PPM	脉冲位置调制
PRNG	伪随机数产生器
PS	节能(模式)
PSDU	PLCP 服务数据单元
RA	接收器地址
RF	射频
RSSI	接收信号强度指示
RTS	请求发送
RX	接收或接收器
SA	源地址
SAP	服务访问点
SDU	服务数据单元
SFD	帧起始定界符
SIFS	短帧间间隔
SLRC	站长重传计数
SME	站管理实体
SMT	站管理
SQ	信号质量(PN 码相关强度)

SRC	短重传计数
SS	站服务
SSAP	源服务访问点
SSID	服务集标识
SSRC	站短重传计数
STA	站(点)
TA	发送器地址
TBTT	目标信标传输时间
TIM	通信量指示图
TSF	定时同步功能
TU	时间单元
TX	发送或发送器
TXE	发送使能
UCT	无条件转移
WAI	无线局域网鉴别基础结构
WAPI	无线局域网鉴别与保密基础结构
WAN	广域网
WDM	无线分布式媒体
WDS	无线分布式系统
WLAN	无线局域网
WM	无线媒体
WPI	无线局域网保密基础结构

## 5 一般描述

### 5.1 体系结构的一般描述

本条提出在本部分中使用的概念和术语。在第3章定义了特定术语。若干插图表达了本部分体系结构组成部分的关键概念和相互关系。本部分使用体系结构来描述LAN的功能组成部分。体系结构描述并不用来表示本部分的任何特定的物理实现。

#### 5.1.1 无线网络如何不同

无线网络具有的基本特点和传统的有线LAN有显著的不同,国家对无线电设备除了本部分中规定的要求以外还可以施加特定要求。

##### 5.1.1.1 目的地址不等于目的位置

在有线LAN中,一个地址等价于物理位置。这在有线LAN的设计中毫无疑问地采用了。在本部分中,可寻址的单元为站点(STA)。STA是消息的目的地,但(通常)位置不固定。

##### 5.1.1.2 媒体影响设计

本部分使用的物理层(PHY)在基础上与有线媒体不同。因此本部分物理层(PHY):

- 所用媒体即没有绝对的边界,也没有容易观察的边界,在此边界之外具有一致PHY收发器的STA不能接收网络帧;
- 不能避免外界信号;
- 在媒体上通信的可靠性明显低于有线LAN的PHY;
- 具有动态拓扑结构;
- 缺乏全连通性,因而一般不能假设每个STA均能侦听到其他STA(即,STAs彼此可以隐

## GB 15629.11—2003

藏);

f) 具有时变特性和非对称传播特性。

由于无线 PHY 覆盖范围有限, 因此试图覆盖一定地理区域的无线 LAN 可以由多个基本覆盖构造单元组成。

### 5.1.1.3 处理移动 STA 的影响

本部分要求之一是处理移动 STA 和便携 STA。便携 STA 可以从一个位置移动到另一个位置的站, 但只有处于固定位置时才被使用; 而移动 STA 可在移动中访问 LAN。

从技术角度考虑, WLAN 仅能处理便携 STA 是不够的。无线传播的影响使得便携 STA 与移动 STA 之间的区分变得模糊; 由于传播的影响造成固定 STA 通常表现出移动性。

另外, 移动 STA 的另一个特性是通常由电池供电, 因此需重点考虑电源管理问题。例如, 不能假定 STA 的接收机总处于加电状态。

### 5.1.1.4 与 GB 15629 各层交互

对高层(LLC)而言, 要求本部分表现为当前风格的 GB 15629 LAN, 这要求符合本部分的网络在 MAC 子层处理 STA 的移动性。为了满足 LLC 层对低层可靠性的假设, 本部分必须在 MAC 子层中合并非传统功能度。

## 5.2 本部分体系的组成部分

本部分体系结构由几个交互的组件部分构成以便提供对高层透明支持站移动性的 WLAN。

基本服务集(BSS)是本部分 LAN 的基本构造模块。图 1 示出了两个 BSS, 其中每个 BSS 拥有为 BSS 成员的两个 STA。

使用椭圆来描述 BSS 的覆盖区(区域概念通常就足够了但不精确), 在区域内 BSS 成员站可以保持通信。如果站移出其 BSS, 则不能再与 BSS 其他成员直接通信。

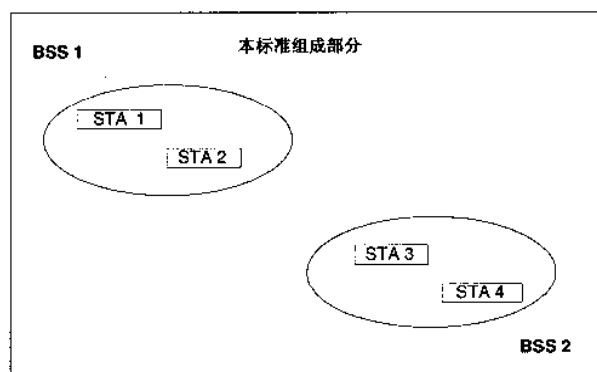


图 1 基本服务集

### 5.2.1 独立 BSS 作为 ad hoc 网

独立基本服务集(IBSS)是本部分 LAN 的最基本的类型。最小的本部分 LAN 可仅由两个 STA 构成。

图 1 示出了两个 IBSS。当符合本部分的 STA 之间能够直接通信时, 该操作模式是可能的。由于该类型的本部分 LAN 不需要预先规划(只要需要)这种操作类型通常称作 ad hoc 网。

#### 5.2.1.1 STA 与 BSS 的动态关联

STA 与 BSS 的关联是动态的(开启、关闭、进入范围和移出范围)。为了成为基础结构 BSS 的成员, STA 应成为“已关联”。这些关联是动态的, 并且涉及到 5.3.2 中描述的分布式系统服务(DSS)的应用。

### 5.2.2 分布式系统概念

PHY 的限制决定了在 STA 到 STA 可支持的距离。对某些网络来说该距离是足够的; 对另一些

网络要求增加覆盖范围。除了现有的独立的 IBSS, BSS 还可以是由多个 BSS 构成的扩充型网络的组成部分。用来互联 BSS 的体系结构组成部分是指分布式系统 (DS)。

本部分在逻辑上将无线媒体(WM)从分布式媒体(DSM)中分离出来,每个逻辑媒体被体系结构的不同组成部分用于不同的用途。本部分定义既不排除也不要求多种媒体是相同或不同。

认识到多个媒体逻辑上的差异是理解体系结构灵活性的关键。所规定的本部分体系结构与任何特定实现的媒体的物理特性无关。

DS 通过提供必要的逻辑服务使移动设备支持处理地址与目的地的映射和多个 BSS 的无缝集成。接入点(AP)除具有 STA 的功能之外,还通过提供 DS 服务提供对 DS 的访问。

图 2 是把 DS 和 AP 组添加到本部分的体系结构图。

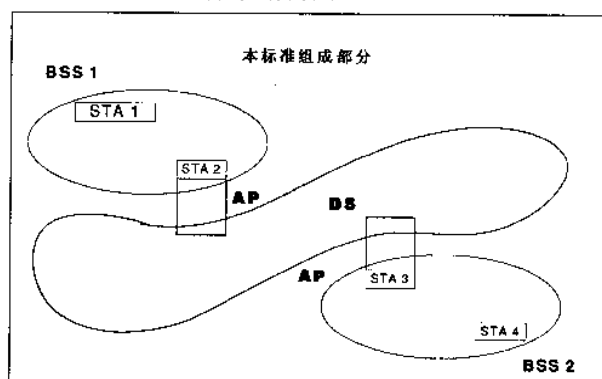


图 2 分布式系统和接入点

在 BSS 和 DS 之间的数据通过 AP 移动。注意：所有的 AP 也是 STA；因此它们是可寻址的实体。在 WM 和 DSM 上进行通信时，AP 所使用的地址不必相同。

#### 5.2.2.1 扩展服务集 (ESS)：大覆盖范围网络

DS 和 BSS 允许本部分创建任意规模和复杂度的无线网络，本部分称这种类型的网络为扩展服务集(ESS)网络。

关键概念是 ESS 网络对 LLC 层来说表现为和 IBSS 网络相同。ESS 内的 STA 可以进行通信，移动 STA 可以对 LLC 透明地从一个 BSS 移动到另一个 BSS（处于同一 ESS 内）。

图 3 中对 BSS 的相关物理位置本部分并未作任何假设。

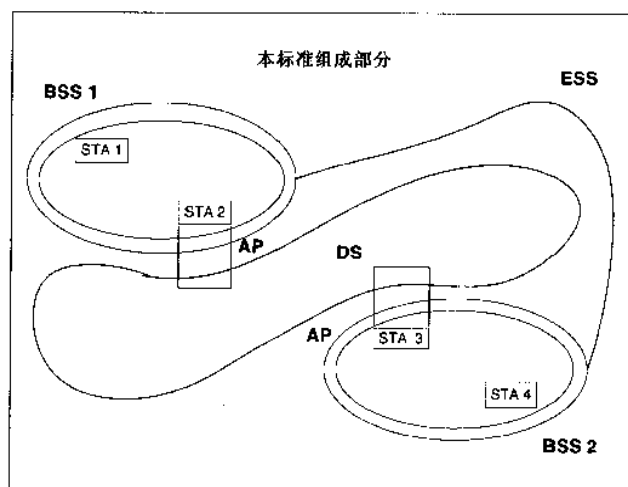


图 3 扩展服务集

## GB 15629.11—2003

下列全部内容都是可能的：

- a) BSS 之间可以部分重叠，这常用于对物理容量安排连续覆盖；
- b) BSS 在物理上可能是分离的，在逻辑上 BSS 之间的距离没有限制；
- c) BSS 在物理上可以排列起来，这可以提供冗余度；
- d) 一个或多个 IBSS 或 ESS 网络在物理上可以出现在与另一个或多个 ESS 网络相同的空间中。产生它的原因是多方面的，其中两个最通常的原因条件是：自组网在还有一个 ESS 网络的位置中操作；由不同组织已经建立的网络在物理上相互重叠。

### 5.2.3 区域概念

对无线 PHY 而言，不存在意义明确定义的覆盖区域。无线传播特性是动态和不可预测的，位置或方向的细小变化都可能导致信号强度的巨大差异。相似的影响不管 STA 是固定还是移动的都会出现（移动对象可能影响 STA 到 STA 的传播）。

图 4 示出了有一个标准金属桌和一个开放入口的简单的正方形空间中的信号强度分布图。图 4 为一个静态快照，传播模式随着环境中 STA 和物体的移动而动态改变。在图 4 中，左下方的黑色（固态）物体为金属桌，右上角有一个入口，该图用不同强度指示场强的相对差异，同时也表明即使在静态环境中场强也具有可变性。

若干体系结构图示出了 BSS 明确的边界，它是人工的图示表示，不是物理事实。由于动态的三维场强图很难绘制，本部分体系结构图采用清晰的轮廓来表示 BSS 的覆盖范围。

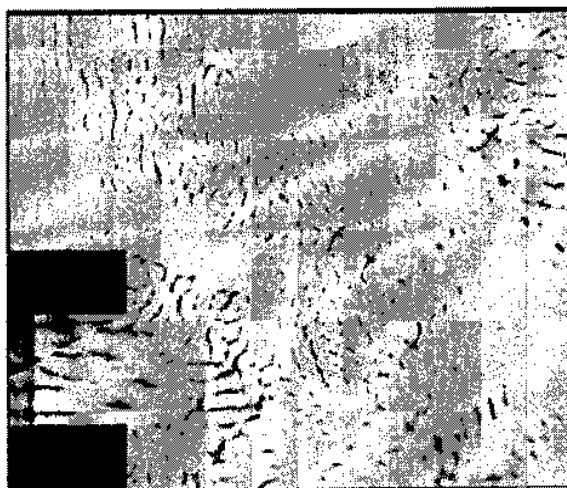


图 4 一个典型的信号强度图

当试图描述排列的覆盖区域时出现了进一步的困难。如图 5 所示，STA 6 既属于 BSS 2，也属于 BSS 3。

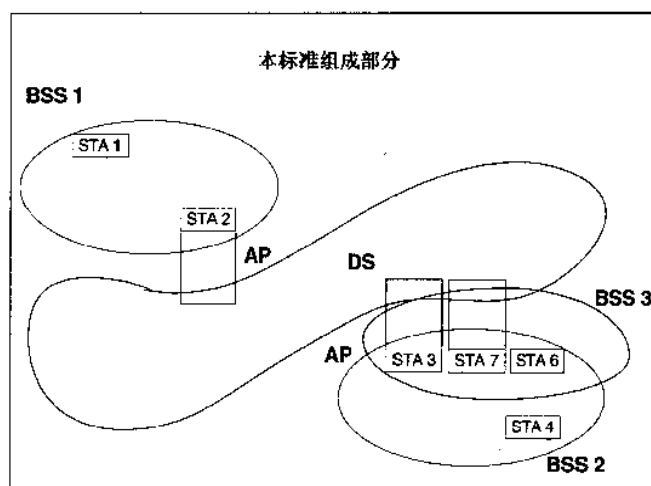


图 5 排列覆盖区

只要站集的概念是正确的，就经常便于讨论区域。对许多论题区域的概念就足够了。容量是比区域更准确的术语，尽管在技术上仍然不正确。由于历史原因和方便性，本部分使用公共术语“区域”。

#### 5.2.4 与有线 LAN 的集成

为实现本部分体系结构与传统的有线 LAN 的集成，引入一个逻辑体系结构组成部分——泛端口。

泛端口是 MSDU 从集成的非本部分局域网进入本部分 DS 的逻辑点。例如，图 6 示出了一个连接到有线 LAN 上的泛端口。

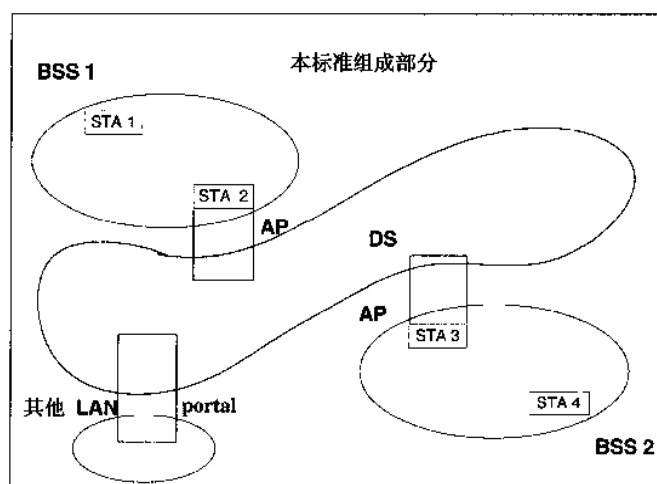


图 6 与其他 GB 15629 LAN 的连接

所有来自于非本部分 LAN 的数据均通过泛端口进入本部分 LAN 体系结构。泛端口在本部分 LAN 与现存的有线 LAN 之间提供了逻辑上的集成。某个设备可能同时提供 AP 功能和泛端口功能，这可能是根据 GB 15629 组成部分实现的 DS 的实例。

在本部分中，ESS 体系结构(AP 和 DS)提供通信量分段与范围扩充。本部分 LAN 和其他 LAN 之间的逻辑连接均借助泛端口。泛端口把 DSM 和将被集成的 LAN 媒体连接起来。

#### 5.3 逻辑服务接口

本部分体系结构考虑到 DS 可以不等同于现有的有线 LAN 的可能性。DS 可根据包含当前 GB

## GB 15629.11--2003

15629 有线 LAN 的许多不同技术构造。本部分不限制 DS 是基于数据链路层或网络层的，在性质上也  
不限制 DS 是集中式或分布式的。

本部分没有显式规定 DS 实现的细节。而是，本部分规定服务。这些服务与体系结构的组成部分  
分相关联。本部分定的服务有两类——站服务（SS）和分布式系统服务（DSS）。这两种服务均由本  
部分 MAC 子层使用。

本部分体系结构服务的完整集如下：

- a) 链路验证；
- b) 关联；
- c) 解除链路验证；
- d) 解除关联；
- e) 鉴别；
- f) 分发；
- g) 集成；
- h) 保密；
- i) 重新关联；
- j) MSDU 发送。

服务集被分作两组：一组为 STA 部分，另一组为 DS 部分。

### 5.3.1 STA 服务(SS)

本服务由 STA 提供，称为站服务。

符合本部分的每个站均提供 SS（包括 AP，因为 AP 包括站功能）。SS 是为 MAC 子层实体使用  
而规定的所有组成部分的站提供 SS。

SS 如下：

- a) 链路验证；
- b) 解除链路验证；
- c) 鉴别；
- d) 保密；
- e) MSDU 发送。

### 5.3.2 分布式系统服务(DSS)

本服务由 DS 提供，称为分布式系统服务。

这些服务在本部分系统结构中用 AP 中的箭头表示，以说明服务是用于跨越媒体和地址空间的  
逻辑边界。在图中示出服务的方便位置。各种服务的物理体现可以在物理 AP 中或不在物理 AP 中。

DSS 由 DS 提供。它们也可以通过提供 DSS 的 STA 进行访问。提供访问 DSS 的 STA 是一个 AP。

DSS 包括：

- a) 关联；
- b) 解除关联；
- c) 分发；
- d) 集成；
- e) 重新关联。

DSS 是为 MAC 子层实体使用而规定的。

图 7 组合前面各图中的组成部分和两种类型的服务，以示出了完整的本部分体系结构。



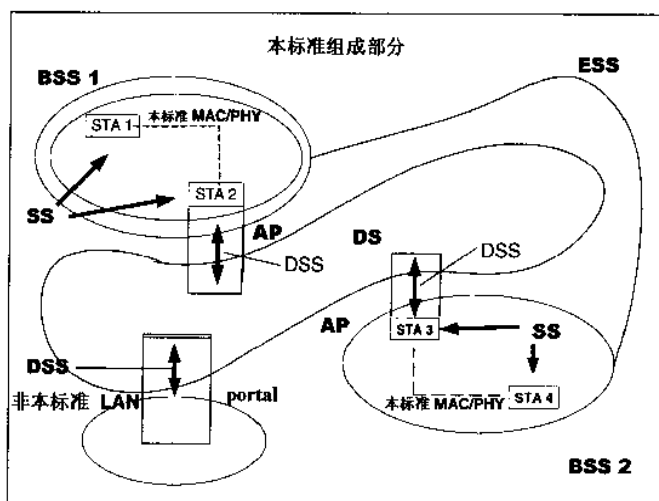


图7 本部分完整的体系结构

### 5.3.3 多逻辑地址空间

本部分的体系结构考虑到 WM、DSM 以及集成的有线 LAN 可能是不同的物理媒体，同时也考虑到每个组成部分可能在不同地址空间内运行。本部分仅使用并规定 WM 地址空间的使用。

本部分 PHY 运行在单一媒体上（WM）。本部分 MAC 运行在单一地址空间内。本部分体系结构的 WM 上使用 MAC 地址。本部分没有必要显式地规定其地址就是“WM 地址”。这个假定贯穿于整个标准。

本部分已选择 48 比特的地址空间（见 7.1.3.3.1）。因此本部分地址与符合 GB 15629 LAN 系列所使用的地址空间兼容。

本部分地址空间的选择隐含着对于本部分体系结构的许多实例而言，有线 LAN 的 MAC 地址空间和本部分 MAC 地址空间可能相同。在这些情况下 DS 使用 MAC 级的符合 GB 15629 系列标准的寻址是合适的，在系统中使用的全部三种逻辑地址空间是相同的。尽管这是一般情况，但不是体系结构允许的惟一组合。本部分体系结构还允许三种逻辑地址空间不同。

多地址空间的一个例子就是 DS 的实现使用了网络层寻址。在此情况下，WM 地址空间和 DS 地址空间可能是不同的。

体系结构具有处理多个逻辑媒体和地址空间的能力，这对本部分独立于 DS 实现以及与网络层移动性方法顺利接口是关键的。DS 的实现并未规定，它超出了本部分范围。

### 5.4 服务综述

本部分共定义了十种服务（链路验证、关联、解除链路验证、解除关联、鉴别、分发、集成、保密、重新关联和 MSDU 发送），其中六种服务（关联、解除关联、分发、集成、重新关联和 MSDU 发送）用于支持 STA 之间的 MSDU 交付，另外四种服务用来控制对本部分 LAN 的访问与机密性。

本条提供了服务、如何使用每种服务的综述以及如何与其他服务及本部分的体系结构如何相关的描述。这些服务是按照便于理解符合本部分的 ESS 网络操作的设计次序描述的。因此，SS 和 DSS 是按次序混合的（而不是按类分组的）。

每种服务是由一种或多种 MAC 帧类型支持的。某些服务由 MAC 管理消息支持，某些服务由 MAC 数据消息支持。所有消息均利用第 9 章规定的 MAC 子层媒体访问方法获得对 WM 的访问。

本部分 MAC 子层使用数据、管理及控制（见第 7 章）三种类型的消息。数据消息的处理是通过 MAC 数据服务通路进行的。

## GB 15629.11—2003

MAC 管理消息用于支持本部分服务并通过 MAC 管理服务数据通路来处理。

MAC 控制消息用于支持交付本部分数据和管理消息。

此处的举例均假定在 ESS 网络环境。ESS 和 IBSS 网络环境的区别在 5.6 中规定。

#### 5.4.1 DS 内的消息分发

##### 5.4.1.1 分发

分发是本部分 STA 使用的基本服务。在概念上，它由每个来自或来自工作在 ESS（此时帧通过 DS 发送）中的本部分 STA 的数据消息调用。分发通过 DSS。

参阅在图 7 所示的 ESS 网络中，考虑数据消息从 STA 1 发送到 STA 4。消息从 STA 1 发出，由 STA 2（“输入” AP）接收。AP 将消息送给 DS 的分发服务。分发服务的作业就是在 DS 中将消息交付到适当的与期望接收方相关的目的地。在本例中，消息被分发到 STA 3（“输出” AP），并且 STA 3 访问 WM，从而将消息传送到 STA 4（预期的目的地）。

本部分未规定在 DS 中如何分发消息。本部分要求向 DS 提供足够的信息，以便 DS 能够确定与要求的接收方相对应的“输出”点。必要的信息由三种与关联相关的服务（即关联、重新关联和解除关联）提供给 DS。

前面的例子中是一个示例，其中调用分发服务的 AP 不同于收到分发消息的 AP 不同。如果消息的预期送给的 STA 和发送 STA 是同一 BSS 的成员，则用于消息“输入”和“输出”的 AP 是同一个 AP。

在任一例子中下，在逻辑上调用分发服务。在实际上 DS 消息是否必须穿过 DSM 是 DS 实现的事并在本部分中不作规定。

尽管本部分未规定 DS 的实现，但它认可并支持将 WM 用作 DSM。这由本部分的帧格式明确地支持（关于细节参见第 7 章）。

##### 5.4.1.2 集成

如果分发服务确定消息的预期接收者为集成 LAN 的成员，则 DS 的“输出”点将是泛端口而非 AP。

分发到泛端口的消息使得 DS 调用集成功能（概念上在分发服务之后），集成服务负责完成将消息从 DSM 交付到集成 LAN 媒体（包括任何必需的媒体或地址空间转换）所需要任何事情。集成是一种 DSS。

DS 接收到的来自集成 LAN（借助泛端口）去往本部分 STA 的消息在分发服务分发消息前调用集成服务。

集成服务的细节依赖于特定的 DS 实现，超出了本部分的范围。

#### 5.4.2 支持分布式服务的服务

MAC 子层的主要目的是在 MAC 子层实体之间传送 MSDU。分发服务所需要的信息由关联服务提供，在分发服务处理数据消息之前，STA 应该是“已关联”的。

为了理解关联的概念，有必要先了解移动的概念。

##### 5.4.2.1 移动性类型

在本部分中描述的网络内 STA 移动的三种重要的转移类型如下：

- a) 无转移：在这种类型中，通常很难区分的两种情况标识如下：
  - 1) 静止——不移动；
  - 2) 本地移动——在通信 STA 的 PHY 范围内移动（即在 BSA 内移动）。
- b) BSS 转移：这种类型定义为一个 STA 从 ESS 内的一个 BSS 移动到同一 ESS 内的另一个 BSS 中。
- c) ESS 转移：这种类型定义为 STA 从一个 ESS 内的 BSS 移动到不同 ESS 的 BSS 中。这种情况只有在 STA 可能移动的意义之上才会支持。本部分不能保证高层连接的维护，实际上服务

的中断可能出现。

不同的关联服务支持不同移动性种类类型。

#### 5.4.2.2 关联

为了在 DS 内交付消息，对于给定的符合本部分的 STA，分发服务需要知道访问哪个 AP。该信息通过关联概念提供给 DS。~~为了支持 BSS 转移的移动性，关联是必要的但不是充分的。~~关联服务足以支持无转移的移动性。关联是一种 DSS。

在 STA 被允许通过 AP 发送数据消息之前，它应首先与该 AP 相关联。成为相关联的操作调用关联服务，该服务向 DS 提供 STA 到 AP 的映射。DS 使用该信息完成消息分发服务。关联服务提供的信息是如何在 DS 内保存和管理的，本部分未规定。

在任一给定时刻，一个 STA 可与最多一个 AP 相关联。这确保 DS 可以确定“哪个 AP 正为该 STA 服务？”的答案是惟一的。一旦关联完成，STA 可充分利用 DS（通过 AP）进行通信。关联总是通常由移动 STA 启动，而不是 AP。

一个 AP 可以在同一时刻与多个 STA 相关联。

STA 获悉哪一个存在，然后请求通过调用关联服务建立关联。STA 如何获悉关于哪一个存在的详情见 11.1.3。

#### 5.4.2.3 重新关联

关联足以在本部分的 STA 之间进行无转移消息交付。要支持 BSS 转换移动性还需要附加功能度。必需的附加功能度由重新关联服务提供。重新关联是一种 DSS。

重新关联服务被调用以将当前关联从一个 AP 移动到另一个 AP。当 STA 在 ESS 内从一个 BSS 移动到另一个 BSS 时，它始终将 AP 与 STA 之间的映射告知 DS。当 STA 保持与同一 AP 的关联时，重新关联还能使已建立关联的关联属性能改变。重新关联总是由移动 STA 启动。

#### 5.4.2.4 解除关联

只要现有的关联要被终止就调用关联服务。解除关联是一种 DSS。

在 ESS 中，该服务通知 DS 使现有的关联信息无效。因此试图通过 DS 向已解除关联的 STA 发送信息是不会成功的。

关联的任一方（非 AP 的 STA 或 AP）均可调用解除关联服务，解除关联是一个通告型而非请求型服务，它不能被关联的任一方拒绝。

由于服务或其他原因，当 AP 从网络中移走时，AP 可能需要解除它与 STA 的关联。

STA 在离开网络时会尝试解除关联，然而 MAC 协议并不依赖于 STA 调用解除关联服务。若已关联的 STA 丢失，MAC 管理应能解除该 STA 的关联。

#### 5.4.3 访问与机密性控制服务

本部分为与有线 LAN 固有的功能性等价要求提供三种服务。有线 LAN 的设计假设了线缆的物理特性，特别是有线 LAN 的设计假设有线媒体的物理封闭与受控特性。而本部分 LAN 媒体的物理开放性违反这些假设。

本部分提供了三种服务使功能性符合有线 LAN 的假设：链路验证、鉴别和保密。链路验证和鉴别用来代替有线媒体的物理连接。保密用来提供封闭有线媒体的机密特性。

##### 5.4.3.1 链路验证

在有线 LAN 中，物理的安全性用于阻止未授权的访问。而在无线 LAN 中，这是不实际的，因为无线媒体没有明确的边界。

本部分提供了通过链路验证服务控制 LAN 访问的能力。该服务由所有的站用于建立与它们要通信的站的身份确认。对于 ESS 和 IBSS 网络都是这样的。如果两个站之间没有建立一种相互可接受的链路验证等级，那么关联不应被建立。链路验证是一种 SS。

符合本部分的网络采用开放系统链路验证。在开放系统中，任何一个 STA 均可以取得链路验证。

## GB 15629.11—2003

管理信息库(MIB)功能用以支持符合本部分的开放系统链路验证。本部分要求相互接受的、成功的链路验证。

链路验证过程由两步构成：第一步为链路验证请求，第二步为链路验证响应。如果响应为成功，则 STA 之间得到相互链路验证。

## 5.4.3.1.1 预链路验证

因为链路验证过程可能是耗时的（依赖于使用的链路验证协议），链路验证服务可以和关联服务独立地调用。

预链路验证典型地由已关联到一个 AP (STA 前面与其链路验证) 的 STA 实行。本部分不要求 STA 与 AP 进行预链路验证。但是要求在关联之前要建立链路验证。

如果在重新关联的时候才进行链路验证，将影响 STA 在 AP 之间重新关联的速度，限制了 BSS-转移移动性的性能。预链路验证的使用从时间严格的重新关联过程中去除了链路验证服务开销。

## 5.4.3.2 解除链路验证

无论何时要终止现有的链路验证时，调用解除链路验证服务。解除链路验证是一种 SS。

在 ESS 中，由于链路验证是关联的先决条件，因此解除链路验证也应使 STA 解除关联。解除链路验证服务可由任何已链路验证方（非 AP STA 或 AP）调用。它不是一种请求，而是通告。解除链路验证不应被任何一方拒绝。当 AP 将解除链路验证通告发送给已关联的 STA 时，关联也应被终止。

## 5.4.3.3 鉴别

本部分支持 WLAN 鉴别基础结构 WAI(WLAN Authentication Infrastructure)，用于实现 BSS 中 STA 与 AP 之间的相互鉴别，它建立在链路验证过程和关联过程之上。只有鉴别成功后，STA 才能安全接入 AP，否则 AP 拒绝 STA 接入或 STA 拒绝接入至 AP。具体定义见第 8 章。

本部分提供本部分 STA 之间链路级的鉴别。本部分不提供端到端（消息源到消息源）和用户到用户的鉴别。本部分鉴别仅用于使无线链路具有有线链路假定的物理标准。

## 5.4.3.4 保密

在有线 LAN 中，只有在物理上连接到线缆的站可以侦听 LAN 的通信量。对无线共享媒体，情况不是这样。任何一台符合本部分的 STA 都可以侦听到在覆盖范围内所有具有与该 STA 相同的 PHY 的通信量。因此没有保密机制的无线链路连接到有线 LAN 上，会严重降低有线 LAN 的安全等级。

为使无线 LAN 的功能达到有线 LAN 设计中隐含的等级，本部分提供了加密消息内容的能力。该功能由保密服务提供。保密是一种 SS。

本部分规定了可选的保密算法：WLAN 保密基础结构 WPI(WLAN Privacy Infrastructure)，它为满足与有线 LAN “等价的”保密目标而设计。该算法并不为最终的安全而设计，而是“和有线一样安全”。详细信息见第八章。

本部分使用 WPI 机制实现实际的消息加密。为支持 WPI 提供了 MIB 功能。

注意保密可仅被数据帧调用。所有的站初始启动是“不加密的”以建立链路验证、鉴别和保密服务。

对于所有本部分的 STA，默认的保密状态为“不加密”。如果保密服务没有被调用，所有消息应不加密发送。如果该默认状态未被某一方或另一方接受，则 LLC 实体之间将不能成功地进行数据帧通信。配置成强制加密模式的 STA 接收到未加密的数据帧，或加密的数据帧使用接收站不支持的密钥，这些帧均会被丢弃，而不告知 LLC（或当 AP 接收到“To DS”字段置位的帧时，将其丢弃，而不告知分发服务）。为避免重传过程浪费 WM 带宽，这些帧将在 WM 上被确认[若接收时没有出现帧检验序列(FCS)错误]。

## 5.5 服务之间的关系

每个 STA 为所有通过 WM 与自己直接通信的 STA 需要维护三个状态变量：

——链路验证状态：值为未链路验证和已链路验证；

——关联状态：值为未关联和已关联；

——鉴别状态：值为未鉴别和已鉴别。

这三个变量为每个远端 STA 建立了四种本地状态：

——状态 1：未链路验证，未关联，未鉴别（初始启动状态）；

——状态 2：已链路验证，未关联，未鉴别；

——状态 3：已链路验证，已关联，未鉴别；

——状态 4：已链路验证，已关联，已鉴别。

图 8 给出了这些站状态变量与服务间的关系。

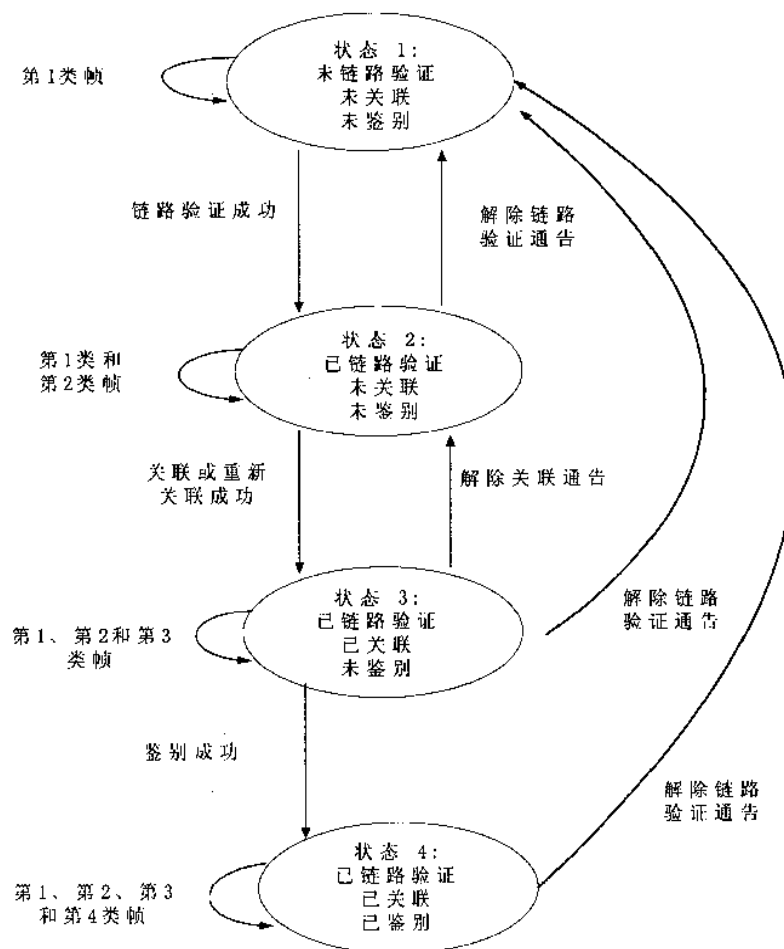


图 8 状态变量与服务间的关系

源 STA 和目的 STA 的当前状态决定了这两个 STA 之间可以交换的帧类型（见第 7 章）。图 8 中给出的发送 STA 的状态是关于预期的接收 STA 允许的帧类型被分为类组，且类是和站状态相对应的。状态 1 只允许第 1 类帧；状态 2 允许第 1 类和第 2 类帧；状态 3 允许所有第 1、2 和 3 类帧；状态 4 允许所有类型的帧（即第 1、2、3 和 4 类帧）。帧类型定义如下。

#### 5.5.1 第 1 类帧（状态 1、2、3 与 4 均允许）

a) 控制帧：

1) RTS；

## GB 15629.11—2003

- 2) CTS;
- 3) ACK;
- 4) CF-End +ACK;
- 5) CF-End.
- b) 管理帧:
  - 1) 探测请求/响应;
  - 2) 信标;
  - 3) 链路验证: 链路验证成功后使 STA 能交换第 2 类帧, 而链路验证不成功则使 STA 处于状态 1;
  - 4) 解除链路验证: 处于状态 2、状态 3 或状态 4 时, 解除链路验证通告使 STA 状态改变到状态 1。发送第 2 类帧前, STA 应再次成为已链路验证的;
  - 5) 通告通信量指示消息 (ATIM)。
- c) 数据帧:

数据: 帧控制比特“To DS”和“From DS”均未置位的数据帧。

## 5.5.2 第 2 类帧 (当且仅当已链路验证的状态 2、3、4 允许)

管理帧:

- a) 关联请求/响应:
 

关联成功后可以交换第 3 类帧, 而关联失败则使 STA 处于状态 2;
- b) 重新关联请求/响应:
 

重新关联成功后使 STA 可以交换第 3 类帧, 而重新关联失败则使 STA 处于状态 2 (关于重新关联消息所发送的目的 STA)。只有在发送方 STA 已关联在相同 ESS 内, 重新关联帧才能发送;
- c) 解除关联:
 

处于状态 3 时, 解除关联通告使 STA 状态变为状态 2。如果该 STA 希望使用 DS, 则该 STA 应再次成为已关联的。

如果 STA A 从一个没有与其建立链路验证的 STA B 那里接收到一个地址 1 字段中有单播地址的第 2 类帧, 则 STA A 应发送解除链路验证帧到 STA B。

## 5.5.3 第 3 类帧 (当且仅当已关联的状态 3、4 允许)

- a) 接入鉴别请求/响应:
 

接入鉴别成功后使 STA 可以交换第 4 类帧, 而接入鉴别失败则使 STA 处于状态 3。

如果 STA A 从没有与其建立链路验证的 STA B 那里接收到一个地址 1 字段中有单播地址的第 3 类帧, 则 STA A 将发送解除链路验证帧到 STA B。

如果 STA A 从已链路验证但还未关联的 STA B 那里接收到一个地址 1 字段中有单播地址的第 3 类帧, 则 STA A 将发送解除关联帧到 STA B。

## 5.5.4 第 4 类帧 (当且仅当已鉴别的状态 4 允许)

- a) 数据帧:
 

数据子类型: 允许传送的数据帧, 即为了使用 DSS, 帧控制比特“To DS”或“From DS”可被置位。
- b) 控制帧:
 

PS-Poll。

如果 STA A 从没有与其建立链路验证的 STA B 那里接收到一个地址 1 字段中有单播地址的第 4 类帧, 则 STA A 将发送解除链路验证帧到 STA B。

如果 STA A 从已链路验证但还未关联的 STA B 那里接收到一个地址 1 字段中有单播地址的第 4

类帧，则 STA A 将发送解除关联帧到 STA B。

如果 STA A 从已链路验证、已关联但未鉴别的 STA B 那里接收到一个地址 1 字段中有单播地址的第 4 类帧，则 STA A 将发送解除链路验证帧到 STA B。

注：在该条款中，“接收”指的是满足第 8 章和第 9 章定义的所有过滤准则的帧。

## 5.6 ESS 与 IBSS LAN 之间的区别

5.2.1 引入了 IBSS LAN 的概念。注意 IBSS 通常用于支持 ad hoc 网络。在 IBSS 网络中，STA 可以与一个或多个 STA 直接通信。考虑象图 9 示出的本部分的完整体系结构。

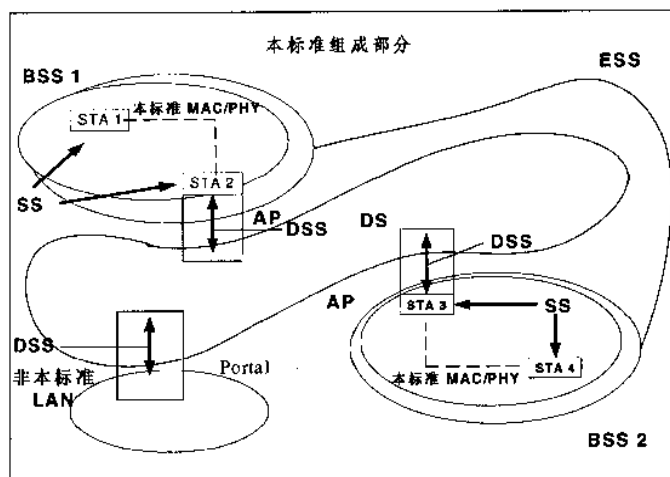


图 9 符合本部分的完整体系结构图

一个 IBSS 由直接连接的 STA 组成。因此（根据定义）只有一个 BSS。而且由于没有物理 DS，就不可能有泛端口、集成有线 LAN 或 DSS。逻辑图归纳为图 10。

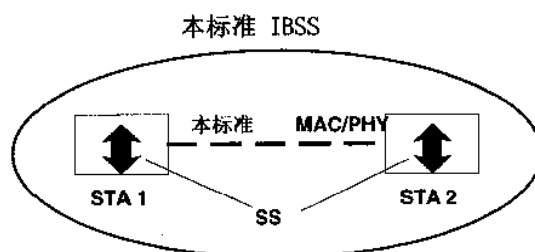


图 10 IBSS 逻辑体系结构

图 10 仅示出最少的两个站。一个 IBSS 可以有任意数目的成员。但由于没有 DS，只允许第 1 类和第 2 类帧。

应用于 IBSS 的服务为 SS。

## 5.7 支持服务的消息信息内容

每项服务都由一个或多个本部分的消息支持。信息项由名字给定，对应值见第 7 章。

### 5.7.1 数据

对于要向其他 STA 发送数据的 STA，它发送数据消息，如下所示：

数据消息：

——消息类型：数据。



## GB 15629.11—2003

——消息子类型：数据。

——信息项：

- 1) 消息的 IEEE 源地址；
- 2) 消息的 IEEE 目的地址；
- 3) BSS ID。

——消息方向：从 STA 到 STA。

### 5.7.2 关联

对于要关联的 STA，关联服务引发下述消息：

关联请求：

——消息类型：管理。

——消息子类型：关联请求。

——信息项：

- 1) 发起关联过程的 STA 的 IEEE 地址；
- 2) 发起方 STA 需关联的 AP 的 IEEE 地址；
- 3) ESS ID。

——消息方向：从 STA 到 AP。

关联响应：

——消息类型：管理。

——消息子类型：关联响应。

——信息项：请求关联的结果，其值为“成功(successful)”或“不成功(unsuccesful)”。

如果关联成功，响应应包括关联标识符 AID。

——消息方向：从 AP 到 STA。

### 5.7.3 重新关联

对于需重新关联的 STA，重新关联服务引发下述消息：

重新关联请求：

——消息类型：管理。

——消息子类型：重新关联请求。

——信息项：

- 1) 发起重新关联的 STA 的 IEEE 地址；
- 2) 发起方 STA 需重新关联的 AP 的 IEEE 地址；
- 3) 发起方 STA 当前关联的 AP 的 IEEE 地址；
- 4) ESS ID。

——消息方向：从 STA 到 AP (STA 请求重新关联的 AP)。

为有效性，消息包括当前 AP 的地址。包括当前 AP 的地址使 MAC 的重新关联与 DS 实现无关。

重新关联响应：

——消息类型：管理。

——消息子类型：重新关联响应。

——信息项：

- 1) 请求重新关联的结果，该项值为“成功”或“不成功”；
- 2) 如果重新关联成功，响应应包括 AID。

——消息方向：从 AP 到 STA。

### 5.7.4 解除关联

对于需终止活动关联的 STA，解除关联服务引发下述消息：



解除关联:

——消息类型: 管理。

——消息子类型: 解除关联。

——信息项:

1) 被解除关联 STA 的 IEEE 地址。当 AP 解除所有已关联 STA 的当前关联时, 则为广播地址;

2) STA 目前关联的 AP 的 IEEE 地址。

——消息方向: 从 STA 到 STA (例如 STA 到 AP 或 AP 到 STA)。

#### 5.7.5 保密

ST 要调用 WPI 保密算法 (由相关的 MIB 属性控制, 见第 11 章), 保密服务使 MPDU 加密。

对于采用保密服务的 STA, 保密服务对 MSDU 进行加、解密。

#### 5.7.6 链路验证

当一台 STA 同另一台 STA 进行链路验证时, 链路验证服务引发一个用于交换的链路验证管理帧。

链路验证算法在管理帧体中进行标识。

在 IBSS 环境中, 任一 STA 都可能是启动 STA(STA 1); 而在 ESS 环境中, STA 1 为移动 STA, STA 2 为 AP。

##### 5.7.6.1 链路验证 (序列的第一帧)

——消息类型: 管理。

——消息子类型: 链路验证。

——信息项:

a) 链路验证算法标识;

b) STA 身份声明;

c) 链路验证过程序列号;

——消息方向: 序列的第一帧总是从 STA 1 到 STA 2。

##### 5.7.6.2 链路验证 (序列的最后一帧)

——消息类型: 管理。

——消息子类型: 链路验证。

——信息项:

a) 链路验证算法标识;

b) 链路验证过程序列号;

c) 请求链路验证的结果, 值为 “successful” (成功) 或 “unsuccessful” (不成功)。

——消息方向: 从 STA 2 到 STA 1。

#### 5.7.7 解除链路验证

一个 STA 要使一个激活的链路验证无效, 需发送如下消息:

——消息类型: 管理。

——消息子类型: 解除链路验证。

——信息项:

a) 正被解除链路验证的 STA 的 IEEE 地址;

b) 目前已与 STA 建立链路验证的 STA 的 IEEE 地址;

c) 当一个 STA 解除目前所有已链路验证 STA 的链路验证时, 它是一个广播地址。

——消息方向: 从 STA 到 STA。

#### 5.8 参考模型

本部分给出了体系结构示意图, 强调系统分为两个部分: PHY 和数据链路层的 MAC, 这些层

## GB 15629.11—2003

紧密对应于开放式系统互连(OSI)的 ISO/IEC(ISO/IEC 7498-1:1998)基本参考模型的最低层。开放式系统互连基本参考模型符合 GB/T 9387.1-1998, 本部分描述的层与子层如图 11 所示。

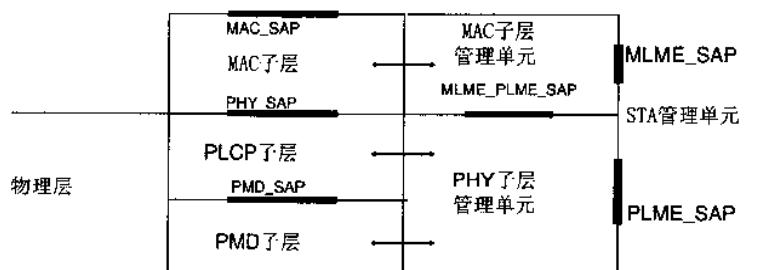


图 11 适用于本部分的基本参考模型构成

## 6 MAC 服务定义

### 6.1 MAC 服务综述

#### 6.1.1 异步数据服务

该服务为对等 LLC 实体提供了交换 MAC 服务数据单元(MSDU)的能力。为了支持这种服务,本地 MAC 利用下层的 PHY 层服务将 MSDU 运输到对等的 MAC 实体,在那里它将被交付给对等的 LLC。这种异步 MSDU 的运输以最大努力的无连接为基础来执行。不保证这些被提交的 MSDU 会被成功交付。广播和组播运输是 MAC 提供的异步数据服务的一部分。由于 WM 的特性,与单播 MSDU 相比,广播和组播 MSDU 可能获得较低质量的服务。所有的 STA 将支持异步数据服务。由于 MAC 某些功能的操作可能使一些 MSDU 重新排序(下面有更详细的讨论),因此异步数据服务有两种服务类别。通过选择所需要的服务类别,每个启动 MSDU 传送的 LLC 实体能够控制是否允许 MAC 实体对那些 MSDU 重新排序。

#### 6.1.2 安全服务

本部分的安全服务由链路验证、鉴别服务和数据保密机制(WPI)提供,提供的安全服务范围仅限于站到站之间的数据交换。本部分提供的数据保密服务对 MSDU 加密。就目的而言,WPI 可视为位于图 11 示出参考模型的 MAC 子层内的逻辑服务,保密服务的实际实现对于 LLC 和 MAC 子层以上的其他层是透明的。

本部分中提供的安全服务如下:

- 机密性;
- 链路验证;
- 鉴别;
- 与层管理相结合的访问控制。

在鉴别交换期间,A 方和 B 方交换鉴别信息在第 8 章描述。

由 WPI 提供的 MAC 子层安全服务依赖于来源于非第 2 层管理或系统实体的信息。管理实体通过一组 MIB 属性传送信息给 WPI。

#### 6.1.3 MSDU 排序

MAC 子层提供的服务允许(并且可能在某些情况下需要)对 MSDU 重新排序。除非在指定的接收站依当前操作(功率管理)模式必须提高成功传送概率,否则 MAC 不需专门对 MSDU 重新排序。对于任何一个 STA 的 MAC 服务接口来说,其对接收的 MSDU 进行重新排序的惟一影响(如果有)是:相对于来自单个源 STA 地址的定向 MSDU,广播和组播 MSDU 的交付顺序的改变。如果

## GB 15629.11—2003

采用异步数据服务的高层协议不允许这种可能的重新排序，则宜使用可选的 **StrictlyOrdered** 服务类别。使用 **StrictlyOrdered** 服务类别时，在任何一对站之间传送的 **MSDU** 不会进行相应的重新排序，而在使用可重新排序组播(**ReorderableMulticast**)服务类别时可能要重新排序。然而，一个站在期望接收采用 **StrictlyOrdered** 服务类别发送的 **MSDU** 时，不会同时使用多个 **MAC** 功率管理设备。

为了使 **MAC** 操作正常，**DS** 必须满足 **GB/T 18236.1** 的要求。

确保 **MSDU** 进行适当排序的操作限制在 9.8 中规定。

## 6.2 详细服务规范

### 6.2.1 MAC 数据服务

本部分 **MAC** 支持 **GB/T 15629.2** 定义的下列服务原语：

- MA-UNITDATA.request**
- MA-UNITDATA.indication**
- MA-UNITDATA-STATUS.indication**

原语的 **LLC** 定义和施加的特定参数值限制在 6.2.1.1 至 6.2.1.3 中给出。

#### 6.2.1.1 MA-UNITDATA.request

##### 6.2.1.1.1 功能

该原语请求将 **MSDU** 从本地 **LLC** 子层实体传送到单个对等 **LLC** 子层实体，或者在组地址情况下传送到多个对等的 **LLC** 子层实体。

##### 6.2.1.1.2 服务原语的语义

原语参数如下：

```
MA-UNITDATA.request (
    source address,
    destination address,
    routing information,
    data,
    priority,
    service class
)
```

**source address(SA)**参数规定了 **MSDU** 正被传往的子层实体的单个 **MAC** 子层地址。

**destination address(DA)**参数规定了单个或组 **MAC** 子层实体地址。

**routing information** 参数规定了传送数据所需的路由，空值指示不采用源路由选择。在本部分中，**routing information** 参数必须为空。

**data** 参数规定了 **MAC** 子层实体发送的 **MSDU**。在本部分中，**MSDU** 的长度不超过 2304 个八位位组。

**priority** 参数规定了传送数据单元所需的优先级。本部分允许两个值：竞争或无竞争。

**service class** 参数规定了传送数据单元所需的服务类别。本部分允许两个值：**ReorderableMulticast**（可重新排序组播）或 **StrictlyOrdered**（严格排序）。

##### 6.2.1.1.3 产生条件

每当 **MSDU** 被传送到单个或多个对等 **LLC** 子层实体时，该原语由 **LLC** 子层实体产生。

##### 6.2.1.1.4 收后效果

收到该原语 **MAC** 子层实体添补所有的 **MAC** 特定字段，包括 **DA**、**SA** 及所有本部分所特有的字段，并将适当格式的帧传递至较低层，以便传送到对等的单个 **MAC** 子层实体或多个 **MAC** 子层实

## GB 15629.11—2003

体。

## 6.2.1.2 MA-UNITDATA.indication

## 6.2.1.2.1 功能

该原语定义了将 MSDU 从 MAC 子层实体传送到 LLC 子层实体或组地址情况下的多个对等的 LLC 子层实体。在无差错情况下，相对于相关的原语 MA-UNITDATA.request 中的数据参数而言，数据参数的内容在逻辑上是完整的和未改变的。

## 6.2.1.2.2 服务原语的语义

原语参数如下：

MA-UNITDATA.indication (

- source address,
- destination address,
- routing information,
- data,
- reception status,
- priority,
- service class

)

SA 参数为入帧的 SA 字段规定的单个地址。

DA 参数为入帧的 DA 字段规定的单个地址或组地址。

routing information 参数规定用来传送数据所采用的路由，本部分应该字段设为空。

data 参数规定本地 MAC 实体接收的 MSDU。

reception status 参数指示那些通过本部分原语 MA-UNITDATA.indication 报告的入帧的成功或失败。若所有接收失败的帧被丢弃，且不产生原语 MA-UNITDATA.indication，则 MAC 只报告“成功”信息。

priority 参数规定了传送数据单元时所使用的接收处理优先级。本部分允许两个值：竞争或无竞争。

service class 参数规定了传送数据单元时所使用的接收服务类别。本部分允许两个值：可重新排序组播或严格排序。

## 6.2.1.2.3 产生条件

原语 MA-UNITDATA.indication 从 MAC 子层实体传递到单个 LLC 子层实体或多个 LLC 子层实体以指示本地 MAC 子层实体中帧的到达。只有帧在 MAC 子层上被有效地格式化，无错误地接收，有效（或空）解密接收且目的地址指定为本地 MAC 子层实体时，帧才能被报告。

## 6.2.1.2.4 收后效果

该原语由 LLC 子层接收，收后效果取决于帧的有效性和内容。

## 6.2.1.3 MA-UNITDATA-STATUS.indication

## 6.2.1.3.1 功能

该原语仅在本地有效，在 LLC 子层为前面相关的原语 MA-UNITDATA.request 提供状态信息。

## 6.2.1.3.2 服务原语的语义

原语参数如下：

MA\_UNITDATA\_STATUS.indication (

- source address,
- destination address,
- transmission status,

provided priority,  
provided service class  
)

参数 SA 为单个 MAC 子层实体地址, 定义同关联的 MA\_UNITDATA.request 原语。

参数 DA 为单个 MAC 子层实体地址或组 MAC 子层实体地址, 定义同关联的 MAUNIT\_DATA.request 原语。

参数 transmission status 将被用于把状态信息传递回本地请求 LLC 子层实体。本部分定义的传送状态值如下:

- a) 成功;
- b) 不可交付 (适用于当超出 aShortRetryMax 或 aLongRetryMax 重传限制时尚未确认的定向 MSDU);
- c) 数据长度超出范围;
- d) 非空源路由;
- e) 不支持的优先权 (优先权既非 Contention 也非 ContentionFree);
- f) 不支持的服务类别 (服务类别既非 ReorderableMulticast 也非 StrictlyOrdered);
- g) 不可用的优先权 (适用于当没有点协调器可用时却选择了 ContentionFree, 而在这种情况下, MSDU 在发送时本应具有被提供的 Contention 优先权);
- h) 不可用的服务类别 (适用于当 STA 的功率管理模式不是“active”时, 却选择了 StrictlyOrdered 服务);
- i) 不可交付 (TransmitMSDUTimer 在成功交付前达到 aMaxTransmitMSDULifeTime);
- j) 不可交付 (没有可用的 BSS);
- k) 不可交付 (不能用空密钥加密)。

参数 provided priority 规定传送关联的数据单元时所采用的优先权 (Contention 或 ContentionFree)。

参数 provided service class 规定传送关联的数据单元时所采用的服务等级 (ReorderableMulticast 或 StrictlyOrdered)。

#### 6.2.1.3.3 产生条件

原语 MA\_UNITDATA\_STATUS.indication 从 MAC 子层实体传递到 LLC 子层实体, 用于向相应的原语 MA\_UNITDATA.request 提供服务状态。

#### 6.2.1.3.4 收后效果

该原语由 LLC 子层接收, 收后效果依赖于 LLC 子层实体使用的操作类型。

### 7 帧格式

本章规定 MAC 帧的格式。所有站都应按照本章的规定构造发送帧和解析接收帧。

#### 7.1 MAC 帧格式

每个帧均由下述基本组成部分构成:

- a) MAC 头, 它包含帧控制、持续时间、地址及序列控制信息;
- b) 可变长度的帧体, 它包含基于帧类型的特定信息;
- c) 帧检验序列(FCS), 它包含 IEEE 32 比特循环冗余码(CRC)。

##### 7.1.1 约定

MAC 子层的 MAC 协议数据单元(MSDU)或帧被描述为按特定顺序排列的字段序列。本章的每个图对 MAC 帧中的字段和子字段均按照他们在 MAC 帧出现并由左至右传送到物理层会聚协议(PLCP)的顺序描述。

**GB 15629.11—2003**

图中, 字段的所有比特从 0 到  $k$  编号, 字段的长度为  $k+1$  比特。字段的八位位组边界可以通过对字段的比特数模 8 得到。在数字字段中长度大于单个八位位组的八位位组按照权值递增的次序描述, 从最低编号比特到最高编号比特。字段中长度大于单个八位位组的八位位组按照从包含最低编号比特的八位位组到包含最高编号比特八位位组的顺序发送至 PLCP。

任何包含 CRC 的字段对上述协定是例外的，它从最高阶系数开始发送。

MAC 地址按照已排序的比特序列分配。单个/组比特总是首先传送, 并且该比特为第一个八位位组的比特 0。

若无另外声明，十进制值按自然二进制编码。表 1 中数值为二进制，比特分配在表中示出。其他表中的数值以十进制记法示出。

保留的字段和子字段在发送时置0，而在接收时被忽略。

### 7.1.2 一般帧格式

MAC 帧格式包含在所有帧中以固定次序出现的一组字段。图 12 描述了一般 MAC 帧格式。地址 2、地址 3、序列控制、地址 4 及帧体字段只在某些类型帧中出现。每个字段均在 7.1.3 中定义。7.2 中定义了每种独立类型帧格式。

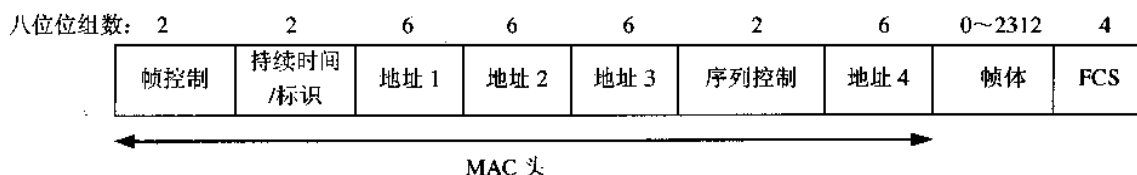


图 12 MAC 帧格式

### 7.1.3 帧字段

#### 7.1.3.1 帧控制字段

帧控制字段包含以下子字段：协议版本、类型、子类型、去往 DS、来自 DS、多分段标记、重传、功率管理、多数据标记、保留及排序。图 13 示出了帧控制字段的格式。

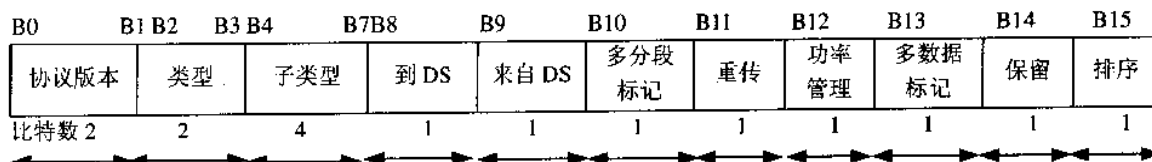


图 13 帧控制字段

#### 7.1.3.1.1 协议版本字段

协议版本字段长度为 2 个比特，且在本部分的所有修订版中长度和位置始终不变。对本部分而言，协议版本值为 0，所有的其他值保留。只有当本部分的新修订版和老版本之间存在根本不兼容时，修订版本的级别才能递增。如果设备接收到比它所支持的版本还要高的修订版本的帧时，将丢弃该帧，且不会向发送站或 LLC 给出指示信息。

#### 7.1.3.1.2 类型和子类型字段

类型字段长度为 2 个比特,子类型字段长度为 4 个比特,这两个字段共同标识帧的功能。共有三种帧类型:控制、数据和管理。每种帧类型又分为几种子类型。表 1 定义了类型和子类型的各种有效组合。

#### 7.1.3.1.3 去往 DS 字段

去往 DS 字段只有 1 个比特。在发往 DS 的数据类型帧中被置为 1，这包括关联至 AP 的 STA 发

出的所有数据类型帧；其他类型帧中，去往 DS 字段被置为 0。

#### 7.1.3.1.4 来自 DS 字段

来自 DS 字段长度为 1 个比特。在离开 DS 的数据类型帧中被置为 1，其他帧中置为 0。

表 2 示出了允许的去往 DS 和来自 DS 字段的组合及其相应含义。

表 1 有效的类型和子类型的组合

类型值 b3 b2	类型描述	子类型值 b7 b6 b5 b4	子类型描述
00	管理	0000	关联请求
00	管理	0001	关联响应
00	管理	0010	重新关联请求
00	管理	0011	重新关联响应
00	管理	0100	探测请求
00	管理	0101	探测响应
00	管理	0110—0111	保留
00	管理	1000	信标
00	管理	1001	通告通信量指示消息(ATIM)
00	管理	1010	解除关联
00	管理	1011	链路验证
00	管理	1100	解除链路验证
00	管理	1110—1111	保留
01	控制	0000—1001	保留
01	控制	1010	节能轮询(PS-Poll)
01	控制	1011	请求发送(RTS)
01	控制	1100	清除待发(CTS)
01	控制	1101	确认(ACK)
01	控制	1110	无竞争结束(CF-End)
01	控制	1111	CF-End+CF-ACK
10	数据	0000	数据(Data)
10	数据	0001	Data+CF-ACK
10	数据	0010	Data+CF-Poll
10	数据	0011	Data+CF-ACK+CF-Poll
10	数据	0100	空功能(无数据)
10	数据	0101	CF-ACK(无数据)
10	数据	0110	CF-Poll(无数据)
10	数据	0111	CF-ACK+CF-Poll(无数据)
10	数据	1000—1111	保留
11	保留	0000—1111	保留

表 2 数据类型帧中去往 DS 字段与来自 DS 字段的组合

去往或来自 DS 字段的值	含 义
去往 DS=0 来自 DS=0	同一 IBSS 内的 STA 之间的数据帧、管理帧和控制帧
去往 DS=1 来自 DS=0	到达 DS 的数据帧
去往 DS=0 来自 DS=1	离开 DS 的数据帧
去往 DS=1 来自 DS=1	从一个 AP 分发到另一个 AP 的无线分布式系统(WDS)帧

## GB 15629.11—2003

## 7.1.3.1.5 多分段标记字段

多分段标记字段长度为 1 个比特。在所有数据或管理类型帧中，若后面还有当前 MSDU 或 MMPDU 的分段，则该字段被置为 1；在其他帧中，该字段被置为 0。

## 7.1.3.1.6 重传字段

重传字段长度为 1 个比特。若数据或管理帧为前面帧的重传帧，该字段置为 1；在其他帧中置为 0。接收站利用该字段来辅助去除复制帧。

## 7.1.3.1.7 功率管理字段

功率管理字段长度为 1 个比特，用于指示 STA 的功率管理模式。在 9.7 定义的帧交换序列中，对来自某个 STA 的所有帧，该字段值保持不变。该字段还指示了在帧交换序列成功完成后站的模式。

该字段值为 1，指示 STA 处于节能模式；值为 0，指示 STA 处于活动模式。在 AP 发送的帧中，该字段的值总为 0。

## 7.1.3.1.8 多数据标记字段

多数据标记字段长度为 1 个比特，用于向处于节能模式的 STA 表明 AP 为该 STA 缓存有多个 MSDU 或 MMPDU。在由 AP 发送到处于节能模式的 STA 的定向数据或管理帧中，该字段有效。值为 1，表明为该 STA 缓存最少有一个 MSDU 或 MMPDU。

在由无竞争可轮询(CF-Pollable)的 STA 发送至点协调器(PC)的用于响应 CF-Poll 帧的定向数据帧中，该字段可以设置为 1，以表明 STA 至少还有一个缓存的 MSDU 可用于响应后续的 CF-Poll 帧。

在其他定向帧中，该字段设置为 0。

在 AP 发送的广播或组播帧中，若在信标间隔期内还有其他的广播或组播 MSDU 或 MMPDU 等待 AP 发送，该字段设置为 1。在 AP 发送的广播或组播帧中，若在信标间隔期内没有其他的广播或组播 MSDU 或 MMPDU 等待 AP 发送，该字段设置为 0。在所有非 AP 的站发送的广播或组播帧中，该字段置为 0。

## 7.1.3.1.9 保留字段

默认值为 0。

## 7.1.3.1.10 排序字段

排序字段长度为 1 个比特。在任何包含按严格排序服务类别传送的 MSDU 或其分段的数据类型帧中，该字段置为 1；在其他帧中，置为 0。

## 7.1.3.2 持续时间/标识字段

持续时间/ID 字段长度为 16 个比特，内容如下：

- 在子类型为 PS-Poll 的控制类型帧中，持续时间/ID 字段的 14 个低位比特运载发送该帧的站的关联标识(AID)，高 2 位均置 1。其中 AID 值在 1~2007 之间；
- 在其他所有帧中，持续时间/ID 字段包含 7.2 中为每种帧类型定义的持续时间。对于在无竞争期(CFP)发送的帧，该字段置为 32 768。

只要持续时间/ID 字段的值小于 32 768，该值就按照第 9 章定义的规程更新网络分配向量(NAV)。

表 3 给出了持续时间/ID 字段的编码。

表 3 持续时间/ID 字段编码

比特 15	比特 14	比特 13~0	用 途
0		0~32 767	持续时间
1	0	0	在 CFP 期间发送的帧中为定值
1	0	1~16 383	保留
1	1	0	保留
1	1	1~2007	PS-Poll 帧中的 AID



1	1	2008~16 383	保留
---	---	-------------	----

### 7.1.3.3 地址字段

MAC 帧格式中有四个地址字段，这些字段用于指示基本服务集标识、目的地址、源地址、发送站地址和接收站地址。每种类型帧的四个地址字段用缩写 BSSID、DA、SA、TA 和 RA 分别表示基本服务集标识、目的地址、源地址、发送方地址和接收方地址。某些帧可能不包括某些地址字段。

特定地址字段的用法由 MAC 帧头中地址字段(1~4)的相应位置来规定，与该字段中出现的地址类型无关。例如，接收方的地址匹配总是根据接收帧中地址 1 字段的内容执行，CTS 帧和 ACK 帧的接收方地址总是从相应的 RTS 帧或被确认的帧的地址 2 字段中获得。

#### 7.1.3.3.1 地址表示

每个地址字段包含 IEEE Std 802-1990 的 5.2 中定义的 48 比特地址。

#### 7.1.3.3.2 地址指定

MAC 子层地址有如下两种类型：

- a) 独立地址：与网络中特定的站关联的地址；
- b) 组地址：与给定网络中一个或多个站关联的多目的地址。

组地址有以下两种类型：

- 1) 组播地址：按高层约定，与一组逻辑相关的站关联的地址；
- 2) 广播地址：给定 LAN 上所有 STA 集合的一个预先定义的组播地址。目的地址字段为 1 被解释为广播地址。这个组地址对每个通信媒体而言都是预先定义好的，它包含主动连接到该媒体的所有站，用于向该媒体上的所有活动站广播。所有站均可识别广播地址，而不必须具备产生广播地址的能力。

地址空间还被分成本地管理地址和全局管理地址两部分，详见 IEEE Std 802-1990。管理全局地址的规程超出了本部分范围。

#### 7.1.3.3.3 BSSID 字段

基本服务集标识(BSSID)字段长度为 48 比特，格式同 IEEE Std 802 MAC 地址，该字段惟一标识一个 BSS。在基础结构 BSS 中，该字段的值就是 BSS 中 AP 的 STA 所用的 MAC 地址。

在 IBSS 中，该字段的值为一个本地管理的 IEEE MAC 地址，它是由按照 11.1.3 定义的规程产生的一个 46 比特的随机数形成的。地址的独立/组比特置为 0，全局/本地比特置为 1。这种机制用于保证能以较大可能性选择到惟一的 BSSID。

值为全 1 表明为广播的 BSSID。广播 BSSID 可仅用于子类型为探测请求的管理帧的 BSSID 字段中。

#### 7.1.3.3.4 目的地址(DA)字段

DA 字段包含一个独立或组 IEEE MAC 地址，用于标识帧体字段中的 MSDU（或其分段）的最终接收方的单个 MAC 实体或多个实体。

#### 7.1.3.3.5 源地址(SA)字段

SA 字段包含一个独立的 IEEE MAC 地址，用于标识帧体字段中的 MSDU（或其分段）的发送方 MAC 实体。源地址中的独立/组比特在发送时总置为 0。

#### 7.1.3.3.6 接收方地址(RA)字段

RA 字段包含一个独立或组 IEEE MAC 地址，用以标识在 WM 上的预期接收帧体字段信息的立即接收方 STA。

#### 7.1.3.3.7 发送方地址(TA)字段

TA 字段包含一个独立的 IEEE MAC 地址，用以标识已经发送到 WM 上帧体字段中包含的 MPDU 的 STA。发送方地址中的独立/组比特在发送时总置为 0。

### 7.1.3.4 序列控制字段

## GB 15629.11—2003

序列控制字段长度为 16 个比特, 由序列号和分段号两个子字段构成, 序列控制字段的格式如图 14 所示。

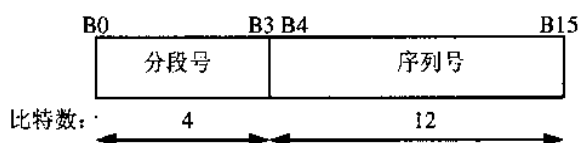


图 14 序列控制字段

## 7.1.3.4.1 序列号字段

序列号字段长度为 12 个比特, 用以指示 MSDU 或 MMPDU 的序列编号。STA 发送的每个 MSDU 或 MMPDU 被分配一个序列编号, 序列号由一个独立的模为 4096 的计数器产生, 从 0 开始, 随着每个 MSDU 或 MMPDU 的出现而以 1 递增。MSDU 或 MMPDU 每个分段的序列号相同。当 MSDU、MMPDU 或其分段重传时, 序列号保持不变。

## 7.1.3.4.2 分段号字段

分段号字段长度为 4 个比特, 用于指示 MSDU 或 MMPDU 的每个分段编号。当 MSDU 或 MMPDU 仅有一个分段时, 分段编号为 0; 当 MSDU 或 MMPDU 有多个分段时, 其第一个分段的分段编号也置为 0, 紧随其后的分段编号以 1 递增。所有重传分段的分段编号保持不变。

## 7.1.3.5 帧体字段

帧体字段长度可变, 包含独立帧类型和子类型的特殊信息。最小帧体为 0 个八位位组, 最大帧体由 MSDU 的最大长度决定。

## 7.1.3.6 FCS 字段

FCS 字段为 32 比特的 CRC, 它由 MAC 头和帧体全部字段计算得到, 这些字段被称为计算字段。FCS 采用下述 32 次方标准多项式计算得到:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

FCS 为下列模 2 和 1 的补码:

- $x^k \times (x^{31} + x^{30} + x^{29} + \dots + x^2 + x + 1)$  除以 (模 2 除)  $G(x)$  的余式,  $k$  为计算字段的比特数;
- 计算字段的内容 (作为多项式处理) 乘以  $x^{32}$  再除以  $G(x)$  的余式。

FCS 字段从最高次项的系数开始发送。

下面是一种典型实现: 在发送端, 初始余式全预置为 1, 接着由产生的多项式  $G(x)$  除以计算字段进行修改, 余式的补码被发送, 且先发送 FCS 字段的高位比特。

在接收端, 初始余式预置为全 1, 计算字段与 FCS 的串行输入被  $G(x)$  相除, 余式非 0 时表示传

送错误。惟一的余式值为下述多项式:

$$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$$

## 7.2 独立类型帧格式

## 7.2.1 控制帧

在下面的描述中, “紧跟着前面的” 帧是指一个在短的帧间间隔 (SIFS) 内接收到的帧。

控制帧中帧控制字段的子字段的设定如图 15 所示。



图 15 控制帧中帧控制字段的子字段值

## 7.2.1.1 请求发送 (RTS)帧格式

图 16 定义了 RTS 帧的帧格式。



图 16 RTS 帧

RTS 帧的 RA 是 WM 上作为已挂起的定向数据帧或管理帧的预期的立即接收方的 STA 的地址。

TA 为发送 RTS 帧的 STA 的地址。

持续时间值等于发送已挂起的数据帧或管理帧、一个 CTS 帧以及一个 ACK 帧所需的时间 (以微秒为单位), 加上三个 SIFS 间隔时间。如果计算出的持续时间值 (以微秒为单位) 是小数, 则向上取整。

## 7.2.1.2 清除待发 (CTS)帧格式

图 17 定义了 CTS 帧的帧格式。

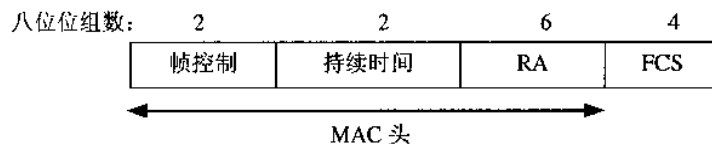


图 17 CTS 帧

CTS 帧作为对 RTS 帧的响应, 其 RA 字段的值由前面 RTS 帧的 TA 字段复制而来。

持续时间值由前面 RTS 帧的持续时间字段的值减去发送 CTS 帧所需的时间 (以微秒为单位) 和 CTS 帧前的 SIFS 间隔时间得到。如果计算出的持续时间值 (以微秒为单位) 是小数, 则向上取整。

## 7.2.1.3 确认 (ACK)帧格式

图 18 定义了 ACK 帧的帧格式。

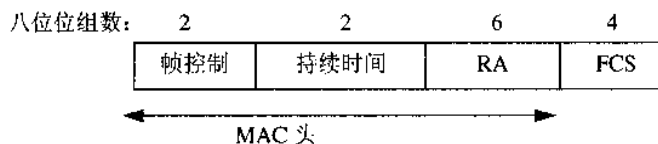


图 18 ACK 帧

ACK 帧的 RA 由前面的定向数据帧、管理帧或 PS-Poll 控制帧的地址 2 字段复制得到。

如果前面的定向数据帧或管理帧的帧控制字段中多分段标记比特置为 0, 则持续时间值设为 0; 如果前面的定向数据帧或管理帧的帧控制字段中多分段标记比特置为 1, 则持续时间值等于其前面的数据帧或管理帧中持续时间字段的值减去发送 ACK 帧所需的时间 (以微秒为单位) 和 ACK 帧前的 SIFS 间隔时间。如果计算出的持续时间值 (以微秒为单位) 是小数, 则向上取整。

## GB 15629.11--2003

## 7.2.1.4 节能轮询(PS-Poll)帧格式

图 19 定义了 PS-Poll 帧的帧格式。

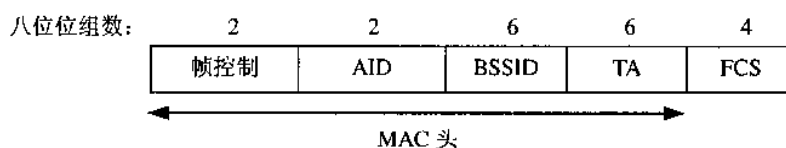


图 19 PS-Poll 帧

BSSID 为包含在 AP 中的 STA 的地址, TA 为发送帧的 STA 地址, AID 是 AP 在建立 STA 当前关联的关联响应帧中为发送 PS-Poll 帧的 STA 分配的值。

AID 值的两个最高比特总设为 1。一旦接收到 PS-Poll 帧, 所有 STA 按协调功能规则将持续时间置为发送一个 ACK 帧所需的时间 (以微秒为单位) 与一个 SIFS 间隔时间的和来更新其 NAV 设置。

## 7.2.1.5 CF-End 帧格式

图 20 定义了 CF-End 帧的帧格式。



图 20 CF-End 帧

BSSID 为包含在 AP 中的 STA 地址, RA 为广播组地址。

持续时间字段置为 0。

## 7.2.1.6 CF-End+CF-ACK 帧格式

图 21 中定义了无竞争结束确认 (CF-End+CF-ACK) 帧的帧格式。



图 21 CF-End+CF-ACK 帧

BSSID 为包含在 AP 中的 STA 的地址, RA 为广播组地址。

持续时间字段置为 0。

## 7.2.2 数据帧

数据帧的帧格式与子类型无关, 其定义如图 22 所示。

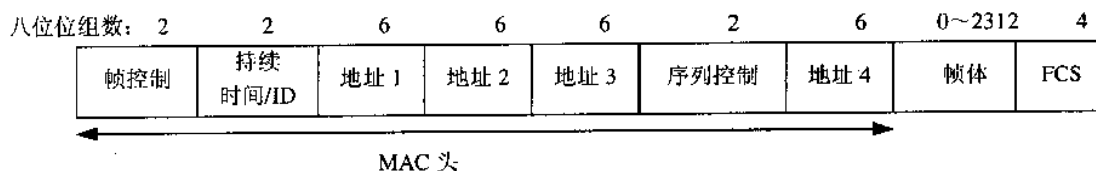


图 22 数据帧

数据帧的地址字段内容取决于去往 DS 和来自 DS 比特的值, 其定义如表 4。若字段的内容被示出为不可用 (N/A), 则该字段被忽略。

注: 地址 1 字段总是包含预期的数据帧的接收方地址 (在数据帧为组播帧时, 包含多个接收方地址), 地址 2 字段总是包含发送帧的 STA 的地址。

表 4 地址字段内容

到 DS	来自 DS	地址 1	地址 2	地址 3	地址 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

站利用地址 1 字段的内容进行地址匹配确定接收结果。当地址 1 字段包含组地址时，BSSID 也生效，用于确保广播或组播帧来自同一 BSS。

如果该数据帧需要确认，则站利用地址 2 字段的内容来引导确认帧的发送。

DA 为帧体字段中 MSDU（或其分段）的目的地址。

SA 为帧体字段中发起 MSDU（或其分段）的 MAC 实体地址。

RA 为包含在 AP 中的 STA 地址。在无线分布系统中, 该 AP 为数据帧的下一个立即接收方。

TA 为包含在 AP 中的 STA 地址。在无线分布系统中, 该 AP 正在发送该帧。

数据帧的 BSSID 按以下规则确定:

- 如果站为 AP 或已关联至 AP, 则 BSSID 是包含在 AP 中的 STA 当前使用的地址;
- 如果站为 IBSS 的成员, 则 BSSID 是 IBSS 的 BSSID。

帧体包含 MSDU 或其分段。在子类型为空功能（无数据）、CF-ACK（无数据）、CF-Poll（无数据）和 CF-ACK+CF-Poll（无数据）的数据帧中，帧体为空（长度为 0 八位位组）。

在 CFP 期间发送的所有数据类型帧中，持续时间字段的值置为 32768；而在竞争期间发送的所有数据类型帧中，持续时间字段的值按以下规则设置：

- 如果地址 1 字段包含组地址，则持续时间字段的值为 0；
- 如果帧的帧控制字段的分多段标记比特置为 0，且地址 1 字段包含单地址，则持续时间字段的值为发送一个 ACK 帧所需的时间（以微秒为单位）与一个 SIFS 间隔时间的和；
- 如果帧的帧控制字段的分多段标记比特置为 1，且地址 1 字段包含单地址，则持续时间字段的值为发送本数据帧的下一个分段和两个 ACK 帧所需的时间（以微秒为单位）与三个 SIFS 间隔时间的和。

数据帧持续时间值的计算基于 9.6 中的规则，该规则确定了帧交换序列中控制帧发送的数据速率。若计算出的持续时间值（以微秒为单位）是小数，则向上取整。所有的站对有效数据帧中不超过 32 767 的持续时间字段的值进行处理，按协调功能规则更新它们的 NAV 设置。

### 7.2.3 管理類

管理帧的帧格式与帧的子类型无关，其定义如图 23 所示。

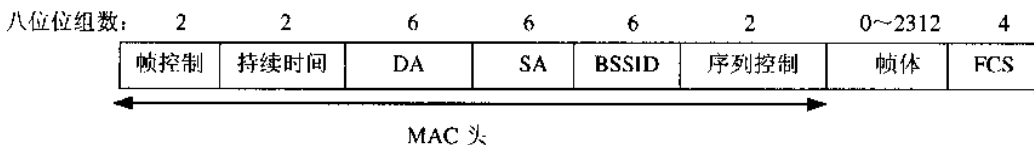


图 23 管理帧格式

STA 利用地址 1 字段中的内容进行地址匹配确定接收结果。如果地址 1 字段包含一个组地址，并且帧类型不是信标帧，则 BSSID 生效用于确保广播或组播帧来自同一 BSS 信息。如果帧类型为信标帧，则采用 11.1.2.3 规定的其他地址匹配规则。

管理帧地址字段不随帧的子类型而改变。

管理帧的 BSSID 按以下原则确定:

- a) 如果站为 AP 或已关联至 AP, 则 BSSID 是包含在 AP 中的 STA 当前使用的地址;

## GB 15629.11—2003

- b) 如果站为 IBSS 的成员, 则 BSSID 就是 IBSS 的 BSSID;
- c) 在子类型为探测请求的管理帧中, BSSID 或者是一个特定的 BSSID, 或者是在第 10 章规定的规程中定义的广播 BSSID。

DA 为帧的目的地址。

SA 为发送帧的站地址。

在 CFP 期间发送的所有管理类型帧中, 持续时间字段的值置为 32 768, 在竞争期间发送的所有管理类型帧中, 持续时间字段的值按照以下规则设置:

- 如果 DA 字段包含一个组地址, 则持续时间值置为 0;
- 如果帧的帧控制字段的分段标记比特置为 0, 且 DA 字段包含一个单地址, 则持续时间字段的值置为发送一个 ACK 帧所需的时间 (以微秒为单位) 与一个 SIFS 间隔时间的和;
- 如果帧的帧控制字段的分段标记比特置为 1, 且 DA 字段包含一个单地址, 则持续时间字段的值置为发送该管理帧的下一个分段和两个 ACK 帧所需的时间 (以微秒为单位) 与三个 SIFS 间隔时间的和。

管理帧持续时间字段值的计算基于 9.6 中的规则, 该规则确定了在帧交换序列中控制帧发送的数据速率。如果计算出的持续时间字段的值 (以微秒为单位) 是小数, 则向上取整。所有的站对有效管理帧不超过 32 767 的持续时间字段的值进行处理, 按协调功能规则适当地更新它们的 NAV 设置。

帧体由每个管理帧子类型定义的固定字段和信息元素组成。除非另有声明, 否则所有的固定字段和信息元素是必备的, 且它们只能以特定的顺序出现。如果站遇到不能解析的元素类型, 则忽略该元素。在本部分中, 没有明确定义的元素类型代码是保留的, 在任何一帧中均不会出现。

#### 7.2.3.1 信标帧格式

子类型为信标的管理帧的帧体包含的信息如表 5 所示。

表 5 信标帧体

顺 序	信 息	备 注
1	时戳	——
2	信标间隔	——
3	能力信息	——
4	SSID	——
5	支持速率	——
6	FH 参数集合	FH 参数集合信息元素出现在由采用跳频 PHY 的 STA 产生的信标帧中
7	DS 参数集合	DS 参数集合信息元素出现在由采用直接序列 PHY 的 STA 产生的信标帧中
8	CF 参数集合	CF 参数集合信息元素仅出现在由支持 PCF 的 AP 产生的信标帧中
9	IBSS 参数集合	IBSS 参数集合信息元素仅出现在由 IBSS 内的 STA 产生的信标帧中
10	TIM 参数集合	TIM 信息元素仅出现在由 AP 产生的信标帧中

#### 7.2.3.2 IBSS 通告通信量指示消息 (ATIM) 帧格式

子类型为 ATIM 的管理帧的帧体为空。

#### 7.2.3.3 解除关联帧格式

子类型为解除关联的管理帧的帧体包含的信息如表 6 所示。

表 6 解除关联帧体

顺 序	信 息
1	原因码

## 7.2.3.4 关联请求帧格式

子类型为关联请求的管理帧的帧体包含的信息如表 7 所示。

表 7 关联请求帧体

顺 序	信 息
1	能力信息
2	侦听间隔
3	SSID
4	支持的速率

## 7.2.3.5 关联响应帧格式

子类型为关联响应的管理帧的帧体包含的信息如表 8 所示。

表 8 关联响应帧体

顺 序	信 息
1	能力信息
2	状态码
3	关联 ID(AID)
4	支持的速率

## 7.2.3.6 重新关联请求帧格式

子类型为重新关联请求的管理帧的帧体包含的信息如表 9 所示。

表 9 重新关联请求帧体

顺 序	信 息
1	能力信息
2	侦听间隔
3	当前 AP 地址
4	SSID
5	支持的速率

## 7.2.3.7 重新关联响应帧格式

子类型为重新关联响应的管理帧的帧体包含的信息如表 10 所示。

表 10 重新关联响应帧体

顺 序	信 息
1	能力信息
2	状态码
3	AID
4	支持的速率

## 7.2.3.8 探测请求帧格式

子类型为探测请求的管理帧的帧体包含的信息如表 11 所示。

表 11 探测请求帧体

顺 序	信 息
1	SSID
2	支持的速率

## GB 15629.11—2003

## 7.2.3.9 探测响应帧格式

子类型为探测响应的管理帧的帧体包含的信息如表 12 所示。

表 12 探测响应帧体

顺 序	信 息	备 注
1	时戳	——
2	信标间隔	——
3	能力信息	——
4	SSID	——
5	支持速率	——
6	FH 参数集合	FH 参数集合信息元素出现在由采用跳频 PHY 的 STA 产生的探测响应帧中
7	DS 参数集合	DS 参数集合信息元素出现在由采用直接序列 PHY 的 STA 产生的探测响应帧中
8	CF 参数集合	CF 参数集合信息元素仅出现在由支持 PCF 的 AP 产生的探测响应帧中
9	IBSS 参数集合	TIM 信息元素仅出现在由 IBSS 中的 AP 产生的探测响应帧中

## 7.2.3.10 链路验证帧格式

子类型为链路验证的管理帧的帧体包含的信息如表 13 所示。

表 13 链路验证帧体

顺 序	信 息	备 注
1	链路验证算法序号	
2	链路验证交换序列号	
3	状态码	状态码信息被保留，在特定的链路验证帧中被置为 0。

## 7.2.3.11 解除链路验证

子类型为解除链路验证的管理帧的帧体包含的信息如表 14 所示。

表 14 解除链路验证帧体

顺 序	信 息
1	原因码

## 7.3 管理帧帧体组成部分

在管理帧中，长度固定的必备的帧体组成部分被定义为固定字段，而长度可变的必备的帧体组成部分和所有可选的帧体组成部分定义为信息元素。

## 7.3.1 固定字段

## 7.3.1.1 链路验证算法序号字段

链路验证算法序号字段指示一种链路验证算法，该字段长度为 2 个八位位组，如图 24 所示。该字段的值定义如下：

- 链路验证算法序号为 0：开放系统；
- 链路验证序号的其他值保留。

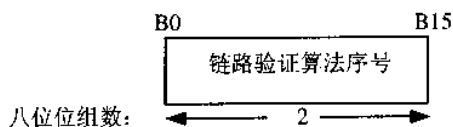


图 24 链路验证算法序号固定字段



### 7.3.1.2 链路验证交换序号字段

链路验证交换字段指示多步处理过程的当前状态，长度为 2 个八位位组，如图 25 所示。

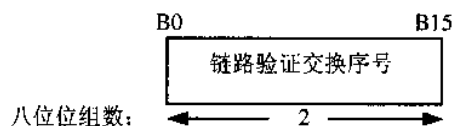


图 25 链路验证交换序号固定字段

### 7.3.1.3 信标间隔字段

信标间隔字段代表目标信标传输时间(TBTT)之间的时间单元(TU)数目。该字段的长度为 2 个八位位组，如图 26 所示。

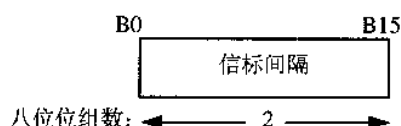


图 26 信标间隔固定字段

### 7.3.1.4 能力信息字段

能力信息字段包括用来指示请求或广播能力的多个子字段。该字段长度为 2 个八位位组，包括 ESS、IBSS、CF-Pollable 和 CF-Poll 请求子字段，其余子字段为保留。能力信息字段格式如图 27 所示。

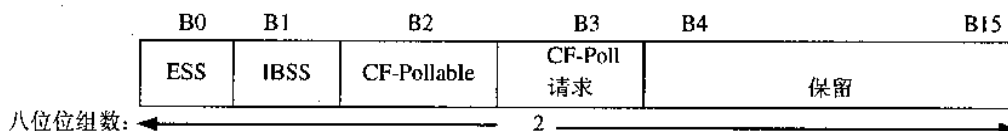


图 27 能力信息固定字段

仅在管理帧子类型中才解释每个能力信息子字段，以定义传输规则。

在发送的信标或探测响应帧中，AP 设置 ESS 子字段为 1，IBSS 子字段为 0；而 IBSS 的 STA 设置 ESS 子字段为 0，IBSS 子字段为 1。

STA 根据表 15 设置关联和重新关联请求管理帧的 CF-Pollable 和 CF-Poll 请求子字段。

表 15 STA 对 CF-Pollable 子字段和 CF-Poll 请求子字段的用法

CF-Pollable	CF-Poll 请求	含 义
0	0	STA 为非 CF-Pollable
0	1	STA 为 CF-Pollable，没有请求放置于 CF-Polling 列表中
1	0	STA 为 CF-Pollable，请求放置于 CF-Polling 列表中
1	1	STA 为 CF-Pollable，请求从不被轮询

AP 根据表 16 设置信标、探测响应、关联响应和重新关联响应等管理帧的 CF-Pollable 和 CF-Poll 请求子字段。AP 将关联响应和重新关联响应管理帧的 CF-Pollable 和 CF-Poll 请求子字段的值设置为与 AP 发送的最后的信标或探测响应帧中的值相同。

表 16 AP 对 CF-Pollable 子字段和 CF-Poll 请求子字段的用法

CF-Pollable	CF-Poll 请求	含 义
0	0	AP 上无点协调器
0	1	AP 上的点协调器仅用于交付(非轮询)
1	0	AP 上的点协调器用于交付和轮询
1	1	保留

### 7.3.1.5 当前 AP 地址字段

当前 AP 地址字段为站当前关联的 AP 的 MAC 地址，长度为 6 个八位位组，如图 28 所示。

GB 15629.11—2003



图 28 当前 AP 地址固定字段

7.3.1.6 侦听间隔字段

侦听间隔字段用于向 AP 指示 STA 苏醒并侦听信标管理帧的频率，该参数值为原语 MLME\_Associate.request 的 STA 侦听间隔参数，以信标间隔为单位。侦听间隔字段的长度为 2 个八位位组，如图 29 所示。



图 29 侦听间隔固定字段

AP 可以利用侦听间隔字段的信息来确定 AP 为 STA 缓存的帧的生存期。

7.3.1.7 原因码字段

原因码字段用于指示解除关联类型或解除链路验证类型的自发的通告管理帧产生的原因，其长度为 2 个八位位组，如图 30 所示。

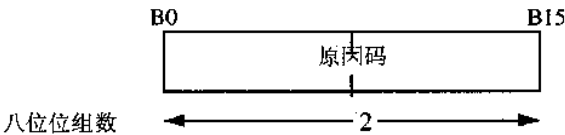


图 30 原因码固定字段

表 17 定义了原因码。

表 17 原因码

原因码	含 义
0	保留
1	未指明的原因
2	以前的链路验证不再有效
3	由于发送站正在离开(或已离开)IBSS 或 ESS 而引起的解除链路验证
4	由于处于非活动状态而引起的解除关联
5	由于 AP 不能处理所有当前已关联的站而引起的解除关联
6	接收来自未链路验证站的第 2 类别帧
7	接收来自未关联站的第 3 类别帧
8	由于发送站正在离开(或已离开)BSS 而引起的解除关联
9	请求(重新)关联的站没有被响应的站进行链路验证
10~65 535	保留

7.3.1.8 关联 ID(AID)字段

AID 字段是 AP 在关联期间分配的值，代表 STA 的 16 比特 ID。该字段的长度为 2 个八位位组，如图 31 所示。

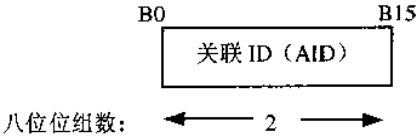


图 31 AID 固定字段

## GB 15629.11—2003

分配的关联 ID 值的变化范围为 1~2007，且用 AID 字段的低 14 比特表示；AID 字段的最高两个比特位均被置 1（见 7.1.3.2）。

## 7.3.1.9 状态码字段

状态码字段用在响应管理帧中以指示请求操作的成功或失败。该字段长度为 2 个八位位组，如图 32 所示。

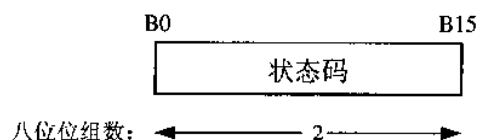


图 32 状态码固定字段

如果操作成功，则状态码被置为 0；如果操作失败，则状态码指示失败的原因。失败原因码的定义如表 18。

表 18 状态码

状态码	含 义
0	成功
1	未指明的失败
2~9	保留
10	不能支持能力信息字段中全部请求的能力
11	由于不能证实关联存在而导致重新关联被拒绝
12	由于超出本部分范围的原因而导致关联被拒绝
13	响应站不支持指定的链路验证算法
14	接收到一个超出预期的链路验证交换序列号的链路验证帧
16	由于等待序列的下一帧超时而导致链路验证被拒绝
17	由于 AP 不能处理额外的关联站而导致关联被拒绝
18	由于请求站不支持参数 BSSBasicRateSet 中的全部数据速率而导致关联被拒绝
19~65535	保留

## 7.3.1.10 时戳字段

时戳字段代表帧的源 TSFTIMER（见 11.1）的值。该字段长度为 8 个八位位组，如图 33 所示。

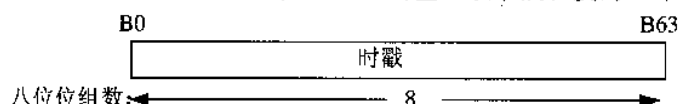


图 33 时戳固定字段

## 7.3.2 信息元素

信息元素被定义为包含 1 个八位位组的元素 ID 字段、1 个八位位组的长度字段以及可变长度的特定元素信息字段的通用格式。本部分为每个元素分配惟一的元素 ID，长度字段规定了信息字段中的八位位组数，见图 34。

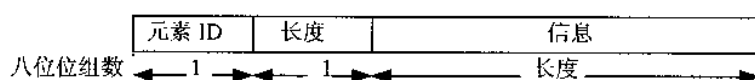


图 34 元素格式

表 19 定义了有效元素的集合。

表 19 元素 ID

信息元素	元素 ID
SSID	0
支持的速率	1
FH 参数集合	2
DS 参数集合	3
CF 参数集合	4
TIM	5
IBSS 参数集合	6
保留	7~15
保留	32~255

### 7.3.2.1 服务集标识(SSID)元素

SSID 元素指示 ESS 或 IBSS 的身份, 见图 35。

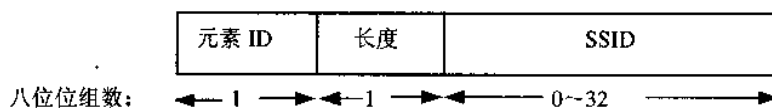


图 35 SSID 元素格式

SSID 信息字段的长度为 0~32 个八位位组, 信息字段长度为 0 指示广播 SSID。

### 7.3.2.2 支持速率元素

支持速率元素规定原语 MLME\_Join.request 和原语 MLME\_Start.request 所描述的 OperationalRateSet (操作速率集合) 中的速率。信息字段编码为 1~8 个八位位组, 每个八位位组描述单个支持速率。

在信标、探测响应、关联响应和重新关联响应管理帧中, 每个由 10.3.9.1 定义的属于 BSS 基本速率集的支持速率均被编码成最高比特 (编号为 7 的比特) 为 1 的单个八位位组 (例如, 属于 BSS 基本速率集的 1Mbit/s 速率编码为 X'82'), 而不属于 BSS 基本速率集的速率被编码成最高比特为 0 的八位位组 (例如, 不属于 BSS 基本速率集的 2Mbit/s 速率编码为 X'04')。其他管理帧类型中每个支持速率八位位组的最高位比特被接收方 STA 忽略。

信标和探测响应管理帧中的 BSS 基本速率集信息在 STA 中通过原语 MLME\_Scan.confirm 的参数 BSSBasicRateSet 交付给管理实体。如果 STA 不能以 BSS 基本速率集中的所有数据速率接收和发送, 则基本速率集信息在 STA 中被管理实体用于避免和该 BSS 关联。

支持速率元素格式如图 36 所示。

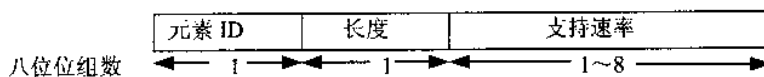


图 36 支持速率元素格式

### 7.3.2.3 FH 参数集合元素

FH 参数集合元素包含采用跳频(FH)PHY 的 STA 允许同步所必需的参数集合。该信息字段包含驻留时间、跳频集合、跳频图案及跳频索引参数, 总长度为 5 个八位位组, 见图 37。

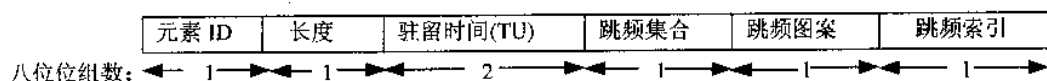


图 37 FH 参数集合元素格式

驻留时间字段长度为 2 个八位位组，包括以 TU 为单位的驻留时间。  
跳频集合字段标识当前的跳频图案集合(dot11CurrentSet)，长度为 1 个八位位组。  
跳频图案字段标识跳频图案集合中的当前跳频图案(dot11CurrentPattern)，长度为 1 个八位位组。  
跳频索引字段选择跳频图案的当前索引(dot11CurrentIndex)，长度为 1 个八位位组。  
本条采用的属性的描述见 14.8.3。

7.3.2.4 DS 参数集合元素

DS 参数集合元素包含的信息允许直接序列扩频(DSSS)PHY 的 STA 进行信道号标识。该信息字段包含单个含 dot11CurrentChannelNumber 的参数（值见 15.4.6.2）。dot11CurrentChannelNumber 参数长度为 1 个八位位组，见图 38。



图 38 DS 参数集合元素格式

7.3.2.5 CF 参数集合元素

CF 参数集合元素包含支持 PCF 所必需的参数组，信息字段包含 CFPCount、CFPPeriod、CFPMaxDuration 和 CFPDurRemaining 字段，总长度为 6 个八位位组，见图 39。

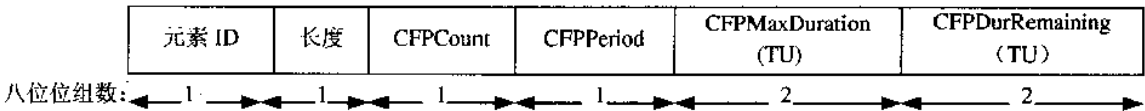


图 39 CF 参数集合元素格式

CFPCount 指示在下一个 CFP 开始之前共有多少个 DTIM（包含当前帧）出现，值为 0 指示当前的 DTIM 标志着 CFP 的开始。

CFPPeriod 指示在两个 CFP 开始时刻之间的 DTIM 间隔的数目，该值为 DTIM 间隔的整数倍。

CFPMaxDuration 指示由 PCF 产生的 CFP 的最大持续时间，以 TU 为单位。STA 用 CFPMaxDuration 在开启 CFP 信标的 TBTT 中设置其 NAV。

CFPDurRemaning 指示在当前 CFP 中剩余的最长时间，以 TU 为单位。在竞争期间发送的信标帧的 CFP 参数元素中，CFPDurRemaning 的值置为 0。CFPDurRemaning 的值以其前面的 TBTT 为参考，所有 STA 用此值在 CFP 期间更新它们的 NAV。

7.3.2.6 TIM

TIM 元素包含四个字段：DTIM Count、DTIM Period、Bitmap Control 和 Partial Virtual Bitmap，见图 40。

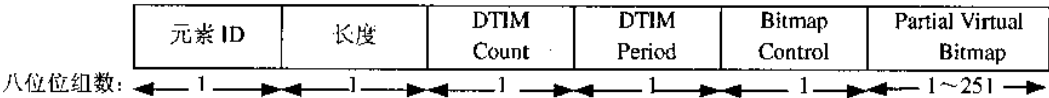


图 40 TIM 元素格式

该元素的长度字段指示信息字段的长度，并受到以下条件的限制。

DTIM Count 字段指示在下一个 DTIM 之前共有多少个信标（包括当前帧）出现，值为 0 指示当前 TIM 就是 DTIM。DTIM Count 字段的长度为 1 个八位位组。

DTIM Period 字段指示两个连续的 DTIM 之间的信标间隔的数目。如果所有的 TIM 均为 DTIM，则 DTIM Period 字段的值置为 1。DTIM Period 字段的 0 值被保留。该字段的长度为 1 个八位位组。

Bitmap Control 字段的长度为 1 个八位位组。该字段的比特 0 为与关联 ID 0 相关联的通信量指

## GB 15629.11-2003

示比特, 当 DTIM Count 字段的值为 0 时, 如果有一个或多个广播或组播帧缓存于 AP 中, 则该比特值置为 1。剩余的 7 个比特形成位图偏移量。

通信量指示虚拟位图由产生 TIM 的 AP 维持, 它包含 2008 个比特, 分为 251 个八位位组。位图编号为  $N$  ( $02N007$ ) 比特对应于编号为  $\lfloor N/8 \rfloor$  的八位位组中编号为  $(N \bmod 8)$  的比特, 且每个八位位组的低位比特编号为 0, 高位比特编号为 7。通信量指示虚拟位图的每个比特对应 BSS 中为特定站缓存的服务, AP 准备在信标帧发送时刻进行交付。如果对应于关联 ID 为  $N$  的站没有直接帧缓存, 则比特  $N$  置 0; 如果对于该站存在缓存的定向帧, 并且 AP 准备交付它们, 则在通信量指示虚拟位图中比特  $N$  置为 1。当 PC 不准准备轮询某些 CF-Pollable 站时 (见 11.2.1.5), 可以不在 TIM 中设置相应的比特。

部分虚拟位图字段由通信量指示虚拟位图编号为  $N1$  到  $N2$  的若干八位位组组成, 其中,  $N1$  为能使位图中比特 1 至比特  $(N1 \times 8) - 1$  全部为 0 的最大偶数,  $N2$  为能使位图中比特  $(N2 + 1) \times 8$  至比特 2007 全部为 0 的最小偶数。此时, 位图偏移子字段的值包含整数  $\lfloor N1/2 \rfloor$ , 长度字段被设置为  $(N2 - N1) + 4$ 。

若当虚拟位图中除比特 0 之外其余比特全部为 0, 部分虚拟位图字段按等于 0 的单个八位位组进行编码, 位图偏移字段为 0。

### 7.3.2.7 IBSS 参数集合元素

IBSS 参数集合元素包含支持 IBSS 所必需的一组参数, 其信息字段包含 ATIM 窗口参数。IBSS 参数集合元素格式见图 41。

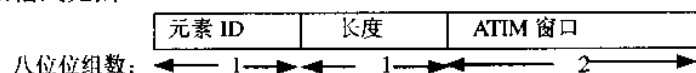


图 41 IBSS 参数集合元素格式

ATIM 窗口字段长度为 2 个八位位组, 包含以 TU 为单位的 ATIM 窗口长度。

## 8 鉴别与保密

本章定义了无线局域网鉴别与保密基础结构 WAPI(WLAN Authentication and Privacy Infrastructure), 它由无线局域网鉴别基础结构 WAI(WLAN Authentication Infrastructure)和无线局域网保密基础结构 WPI(WLAN Privacy Infrastructure)组成。

本章涉及的密码算法按照 1999 年 10 月 7 日颁布的中华人民共和国国务院令第 273 号《商用密码管理条例》执行。

### 8.1 鉴别服务

本部分定义了 WAI 鉴别基础结构, 它采用公钥密码技术, 用于 BSS 中 STA 与 AP 之间的相互身份鉴别。该鉴别建立在关联过程之上, 是实现 WAPI 的基础。

下面定义基于接入控制的鉴别系统结构及物理设备操作和接入控制功能之间的关系。

#### 8.1.1 系统和端口

本部分中 AP 提供两种访问 LAN 的逻辑通道, 定义为两类端口, 即受控端口与非受控端口, 见 8.1.2。

AP 提供 STA 连接到鉴别服务单元(ASU)的端口 (即非受控端口), 确保只有通过鉴别的 STA 才能使用 AP 提供的数据端口 (即受控端口) 访问网络。在基于端口的接入控制操作中, 本部分定义三个实体:

- 鉴别器实体 AE(Authenticator Entity): 为鉴别请求者在接入服务之前提供鉴别操作的实体。该实体驻留在 AP 中。
- 鉴别请求者实体 ASUE(Authentication SUPPLICANT Entity): 需通过鉴别服务单元进行鉴别的

实体。该实体驻留在 STA 中。

- c) 鉴别服务实体 ASE(Authentication Service Entity): 为鉴别器和鉴别请求者提供相互鉴别的实体。该实体驻留在 ASU 中。

上述三个实体在鉴别过程中是必备的。

### 8.1.2 受控和非受控接入

图 42 给出了基于端口接入控制的鉴别器系统示意图。

非受控端口允许鉴别数据在 WLAN 中传送, 该传送过程不受当前鉴别状态的限制。对于受控端口, 只有当该端口的鉴别状态为已鉴别时, 才允许协议数据通过。受控端口和非受控端口可以是连接到同一物理端口的两个逻辑端口, 所有通过物理端口的数据都可以到达受控端口和非受控端口, 此时根据鉴别状态决定数据的实际流向(受控端口或非受控端口)。

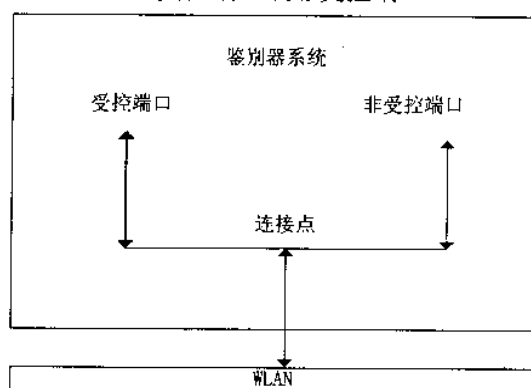


图 42 鉴别器系统示意图

图 43 给出了与受控端口相关的两种不同的鉴别状态 On 或 Off, 分别允许或拒绝受控端口的协议数据单元(PDU) 通过。其中 On 表示端口状态为已鉴别, Off 表示端口状态为未鉴别。图 43 给出了两个系统, 在鉴别器系统 1 中, 受控端口鉴别状态是未鉴别, 此时受控端口拒绝通过任何数据; 在鉴别器系统 2 中, 受控端口鉴别状态是已鉴别, 受控端口允许 PDU 通过。

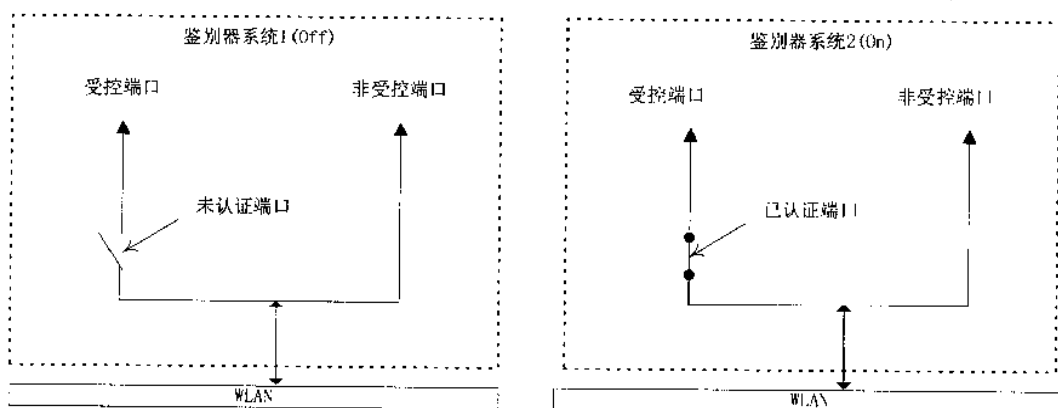


图 43 受控端口的鉴别状态

系统的每一个受控端口状态由系统鉴别控制参数确定。系统鉴别控制参数的值可为“启动鉴别”或“不启动鉴别”, 具体的数字编码见 8.5.1。如果系统鉴别控制参数设置为“不启动鉴别”时, 所有的受控端口的鉴别控制状态为“强制已鉴别”; 如果系统鉴别控制参数设置为“启动鉴别”, 系统的每一个受控端口的鉴别状态由下述三种鉴别控制类型决定。

当系统鉴别控制参数设置为“启动鉴别”时, 受控端口可以被设定为“强制非鉴别”、“自动”或“强制已鉴别”三种类型, 默认类型为“自动”。这三种类型的数字编码见 8.5.1, 具体描述为:

## GB 15629.11—2003

- a) 强制非鉴别：鉴别器实体强制某一个受控端口的状态为未鉴别，即无条件指定受控端口状态为未鉴别（即使已经鉴别也不能通过受控端口传送数据）；
- b) 强制已鉴别：鉴别器实体强制某一个受控端口的状态为已鉴别，即无条件指定受控端口状态为已鉴别（无需鉴别即可通过受控端口传送数据）；
- c) 自动：自动是指根据鉴别器实体和鉴别请求者实体之间通过鉴别服务单元相互鉴别的结果来设定受控端口状态（只有鉴别通过才可通过受控端口传送数据）。

除鉴别数据外，系统中 AP 和 STA 之间的网络协议数据交换是通过一个或多个受控端口来实现的。图 44 给出了受控端口和非受控端口的逻辑结构图，系统中受控端口的鉴别状态是由鉴别器实体根据 ASU 对 STA 的鉴别结果来设定的。

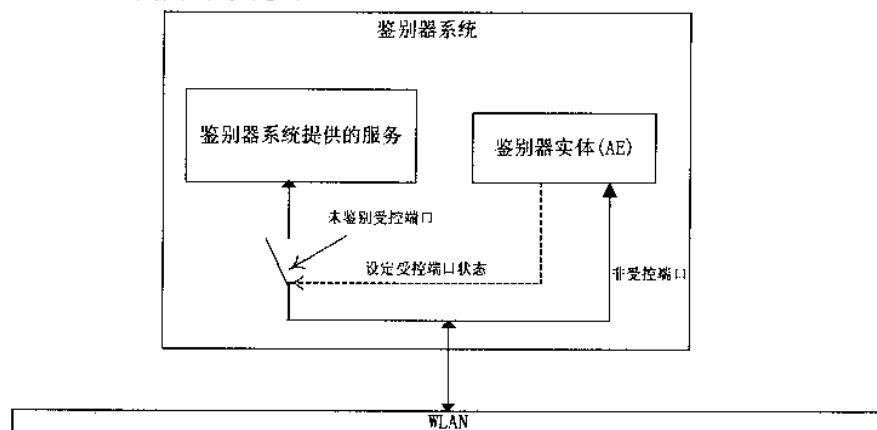


图 44 受控端口和非受控端口的用法

图 45 给出了鉴别请求者、鉴别器和鉴别服务实体之间的关系及信息交换过程。在该图中，鉴别器的受控端口处于未鉴别状态，鉴别器系统拒绝提供服务。鉴别器实体利用非受控端口和鉴别请求者通信。

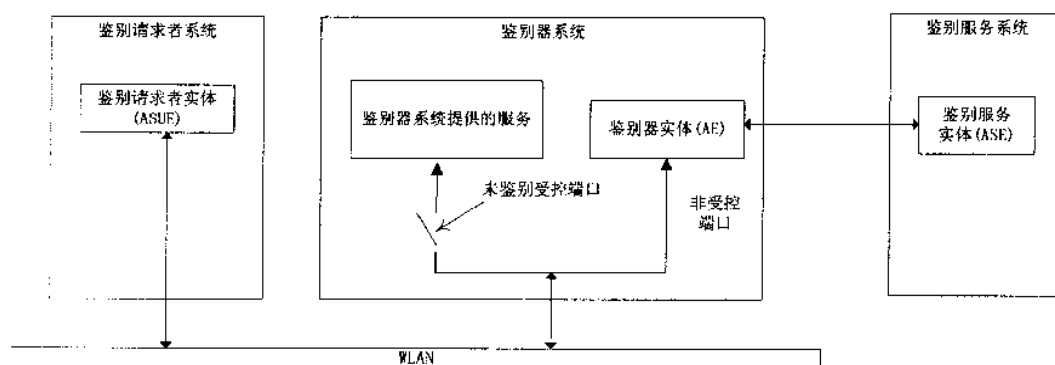


图 45 鉴别系统结构

## 8.2 鉴别服务单元(ASU)

鉴别服务单元 ASU(Authentication Service Unit)是基于公钥密码技术的 WAI 鉴别基础结构最为重要的组成部分，它的基本功能是实现 STA 用户证书的管理和 STA 用户身份的鉴别等。

ASU 作为可信任和具有权威性的第三方，保证公钥体系中证书的合法性。ASU 为每个客户颁发公钥数字证书，并为使用该证书的客户证明公钥合法性的证明。ASU 的数字签名确保证书不被伪造或篡改。ASU 负责管理所有参与网上信息交换的各方所需的数字证书（包括产生、颁发、吊销、更



新等), 是实现电子信息安全交换的核心。

ASU 是 STA 信任的机构, 它完成的功能如下:

- 识别持有公钥信息实体的身份;
- 确保用于产生公钥的非对称密钥对的质量;
- 保证鉴别过程和用于签名的公钥信息和私钥的安全;
- 管理公钥信息中的系统特别数据, 如公钥证书序列号、鉴别机构标识等;
- 指定并检查证书的有效期;
- 通告公钥信息标识实体的身份合法性;
- 确保两个不同的实体未被赋予相同的身份, 以便它们能被区分出来;
- 证书吊销和更新;
- 维护并发布吊销列表;
- 记录公钥证书产生过程中的所有步骤。

在无线局域网中, 基于 ASU 的 WAI 逻辑拓扑结构如图 46 所示。

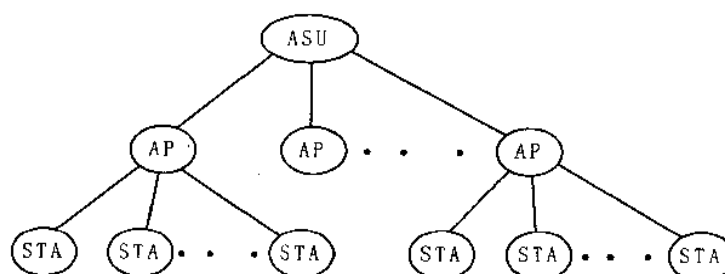


图 46 基于 ASU 的 WAI 逻辑拓扑结构示意图

ASU 对它管理范围内的 AP 与 STA 进行管理并提供服务。一个 ASU 可以管理一个或多个 BSS, 在同一 ASU 的管理范围内, STA 与 AP 之间需通过 ASU 实现证书的双向鉴别。

### 8.2.1 公钥证书

公钥证书是 WAI 系统构造中最为重要的环节。凭借证书和私钥可以惟一地确定网络设备的身份, 公钥证书是网络设备在网络环境中的数字身份凭证。通过与密码技术及安全协议相结合, 确保公钥证书的惟一性、不可伪造性及其他性能。公钥证书格式定义如图 47:

公钥证书的版本号
证书的序列号
证书颁发者采用的签名算法
证书颁发者名称
证书颁发者的公钥信息
证书的有效期
证书持有者名称
证书持有者的公钥信息
证书类型
扩展
证书颁发者对证书的签名

图 47 公钥证书的格式

## GB 15629.11—2003

### 8.2.1.1 公钥证书的版本号

该字段指定证书的格式，以使具体的协议能提取该公钥证书的有效数据项。

### 8.2.1.2 证书的序列号

每个由 ASU 颁发的公钥证书都需要分配一个惟一的序列号，由证书的序列号和证书颁发者的名称可以惟一地确定证书持有者。

### 8.2.1.3 证书颁发者采用的签名算法

该字段指定了证书颁发者所采用的签名算法，包括签名算法名称、签名长度与签名者所使用的公钥长度。本部分采用国家密码管理委员会办公室批准的用于 WLAN 的椭圆曲线密码(ECC)体制实现签名算法。

### 8.2.1.4 证书颁发者名称

该字段指定证书颁发者的身份。

### 8.2.1.5 证书颁发者的公钥信息

该字段为证书颁发者的公钥信息。

### 8.2.1.6 证书的有效期

该字段用于规定公钥证书可以有效使用的时间，采用 UTC 时间格式，表示 1970 年 1 月 1 日 0 时到当前时间的秒数。

### 8.2.1.7 证书持有者名称

该字段指定证书持有者的身份。

### 8.2.1.8 证书持有者的公钥信息

该字段为证书持有者的公钥信息。

### 8.2.1.9 证书类型

该字段表示证书持有者的设备类型，即 STA、AP 或 ASU。

### 8.2.1.10 扩展

该字段保留，用于以后的扩展应用。

### 8.2.1.11 证书颁发者对证书的签名

该字段由证书颁发者(ASU)对该证书上的所有字段项进行签名得到。

## 8.2.2 公钥证书管理

### 8.2.2.1 证书颁发

申请证书时，先在 ASU 处登记，ASU 对证书申请实体的身份进行确认后，按照申请者所需的安全等级为其制作和颁发证书。证书产生步骤如下：

- ASU 产生实体的非对称密钥对；
- 检查公钥信息；
- 接受公钥信息；
- 添加公钥证书管理所需的数据；
- 计算公钥证书的签名；
- 审计记录登记，记录 ASU 在公钥证书产生过程中的行为。

证书颁发可以采用拖拉模式，由一个证书本（数据库）记录所有用户的证书，用户需要时通过数据库提取出所需证书；另一种采用推进模式，证书生成后送给所有的用户或定期向用户发放。

### 8.2.2.2 证书吊销

ASU 可以在证书到期之前吊销证书。具体的原因包括：

- 实体私钥的损坏或丢失；
- 实体请求吊销；

- 实体隶属关系的改变;
- 实体的终止;
- 实体的错误识别;
- ASU 私钥的损坏;
- ASU 的终止。

因此,应有一定的程序和快速的通信方法以便能安全且可鉴别地吊销:

- 一个或多个实体的一个或多个证书;
- 由 ASU 颁发的基于单个非对称密钥对的一系列公钥证书,ASU 用该非对称密钥对来签发公钥信息;
- 由 ASU 颁发的所有公钥证书。

在已知或怀疑 ASU 的私钥泄露时,或在用于签发证书的非对称密钥对被更换时,后两项要求为吊销公钥证书提供了手段。无论公钥证书是过期还是被吊销,旧的公钥证书的拷贝应由可信任的第三方保留一段时间。

当实体或 ASU 的私钥因为某种原因而被取消时,颁发该公钥证书的 ASU 应立即主动通知系统中的所有实体,所有有关的公钥证书都被吊销。可采取的形式有:由 ASU 鉴别并发送给所有实体的消息、由另一 ASU 鉴别的消息、由可信任的第三方保存的一个在线的已吊销公钥证书列表以及公开已吊销或有效的公钥证书列表。

当一个公钥证书因被怀疑或已知某一私钥损坏而被吊销时,该私钥不能继续使用。如果数据已在吊销前签名,公钥证书应只用于验证,而且任何由该公钥证书加密的密钥材料(无论何种类型)都应在操作方便时更换。

吊销列表包括一个带时戳的顺序表或公钥证书标识符表,以表示由 ASU 吊销的公钥证书。在吊销列表中使用两种时间标记:

- ASU 颁布的吊销日期和时间;
- 已知或怀疑泄露的日期和时间。

如果知道泄露的日期和时间,就更加容易审计可疑消息。公钥证书在吊销列表上至少应保持到截止期为止。

一旦由于已知或怀疑泄露而执行吊销,如果签名是在怀疑密钥泄露之后进行的或签名日期无法确定,应认为使用有关私钥签发的信息不再有效。不能使用已吊销的公钥加密消息。

吊销列表应该由 ASU 注明吊销日期并进行签名,以使实体能确认该表的完整性,并确定颁发日期;吊销列表由 ASU 定期发布,即使自上次发布之日起无任何变化。系统的所有实体都可以获得吊销列表,除非由法律、法规所排除在外的。

以下分发机制可用于吊销列表,包括:

- 由可信任的第三方作为消息/报告发送给每个用户;
- 由用户请求可信任的第三方提供指定公钥证书的当前情况;
- 向 ASU 索取当前的吊销列表。

ASU 应定期生成并公布新的吊销列表。

### 8.2.3 椭圆曲线数字签名算法

本部分采用国家密码管理委员会办公室批准的用于 WLAN 的椭圆曲线密码(ECC)算法实现数字签名。

## 8.3 WAI 鉴别基础结构

### 8.3.1 安全接入

当 STA 关联或重新关联至 AP 时,必须进行相互身份鉴别。若鉴别成功,则 AP 允许 STA 接入,否则解除其关联。整个鉴别过程包括证书鉴别与会话密钥协商,如图 48 所示。

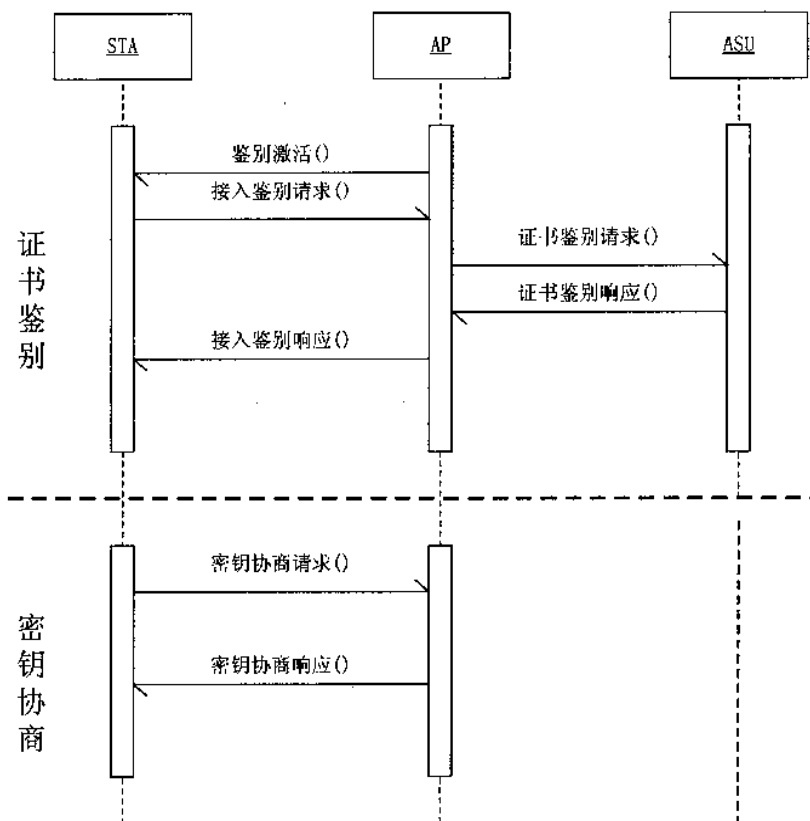


图 48 STA 接入鉴别流程图

## 8.3.1.1 证书鉴别

图 48 具体定义如下：

- 鉴别激活。当 STA 关联或重新关联至 AP 时，由 AP 向 STA 发送鉴别激活以启动整个鉴别过程。
- 接入鉴别请求。STA 向 AP 发出接入鉴别请求，即将 STA 证书与 STA 的当前系统时间发往 AP，其中系统时间称为接入鉴别请求时间。
- 证书鉴别请求。AP 收到 STA 接入鉴别请求后，首先记录鉴别请求时间，然后向 ASU 发出证书鉴别请求，即将 STA 证书、接入鉴别请求时间、AP 证书及 AP 的私钥对它们的签名构成证书鉴别请求发送给 ASU。
- 证书鉴别响应。ASU 收到 AP 的证书鉴别请求后，验证 AP 的签名和 AP 证书的有效性，若不正确，则鉴别过程失败，否则进一步验证 STA 证书。验证完毕后，ASU 将 STA 证书鉴别结果信息（包括 STA 证书和鉴别结果）、AP 证书鉴别结果信息（包括 AP 证书、鉴别结果及接入鉴别请求时间）和 ASU 对它们的签名构成证书鉴别响应发回给 AP。
- 接入鉴别响应。AP 对 ASU 返回的证书鉴别响应进行签名验证，得到 STA 证书的鉴别结果，根据此结果对 STA 进行接入控制。AP 将收到的证书鉴别响应回送至 STA。STA 验证 ASU 的签名后，得到 AP 证书的鉴别结果，根据该鉴别结果决定是否接入该 AP。

至此 STA 与 AP 之间完成了证书鉴别过程。若鉴别成功，则 AP 允许 STA 接入，否则解除其关联。

注：

- 由于鉴别激活信息可能在传输过程中丢失，在 AP 发送鉴别激活后未收到该 STA 的接入鉴别请求，每次收到来自 STA 的协议数据均应重发鉴别激活。
- STA 发送接入鉴别请求时，应合理设置超时时间。当超时时间已到，仍未接收到与最新发送的鉴别请求时间一致的接入鉴别响应时，STA 应重新构造接入鉴别请求并发送，重新进行鉴别过程。
- STA 接收到接入鉴别响应，但其包含的鉴别请求时间与 STA 最新发送的接入鉴别请求中该字段值不同，则丢弃该响应，否则做进一步处理。
- AP 每次收到 STA 发送的接入鉴别请求时，设置该 STA 的状态为“已链路验证、已关联、未鉴别”，即鉴别过程重新开始。
- AP 收到 ASU 的证书鉴别响应后，应首先根据鉴别请求时间判断是否为最新请求的证书鉴别响应，若不是则丢弃，否则做进一步处理。
- 若 STA 欲接入指定的无线接入点 AP，则鉴别之前 STA 应预存有 AP 的证书，以便 STA 对接收到的接入鉴别响应进行判断。

### 8.3.1.2 会话密钥协商

STA 与 AP 证书鉴别成功之后进行密钥协商，密钥协商过程定义如下：

- a) 密钥协商请求。AP 产生一串随机数据，利用 STA 的公钥加密后，向 STA 发出密钥协商请求。此请求包含请求方所有的备选会话算法信息。
- b) 密钥协商响应。STA 收到 AP 发来的密钥协商请求后，首先进行会话算法协商，若响应方不支持请求方的所有备选会话算法，则向请求方响应会话算法协商失败，否则在请求方提供的备选算法中选择一种自己支持的算法；再利用本地的私钥解密协商数据，得到 AP 产生的随机数据；然后产生一串随机数据，利用 AP 的公钥加密后，再发送给 AP。

密钥协商成功后，STA 与 AP 将自己与对方分别产生的随机数据进行模 2 和运算生成会话密钥，利用协商的会话算法对通信数据进行加、解密。

为了进一步提高通信的保密性，在通信一段时间或交换一定数量的数据之后，STA 与 AP 之间可重新进行会话密钥的协商，过程同上。

注：密钥协商请求可由 AP 或 STA 中的任意一方发起，另一方响应。

### 8.3.2 WAI 数据格式

在本部分中，STA 与 AP 之间使用一种新的以太网协议类型 WAPI 进行双向鉴别。AP 与 ASU 之间通过应用层协议进行通信。

#### 8.3.2.1 STA 与 AP 之间的鉴别数据格式

当 STA 关联或重新关联至 AP 时，AP 激活 STA 进行双向鉴别。

鉴别协议分组格式定义如图 49：

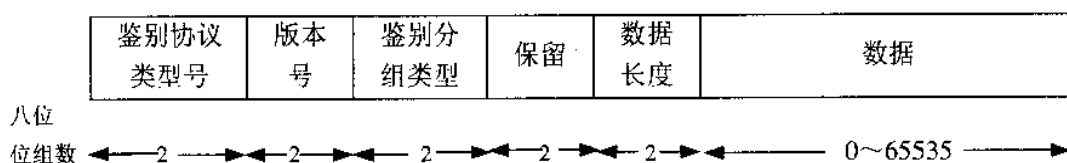


图 49 WAI 鉴别系统的数据分组基本格式

其中：

- 鉴别协议类型号长度为 2 个八位位组，其值为 0x88B4，表示 WAPI 协议类型分组。
- 版本号字段长度为 2 个八位位组，表示鉴别基础结构的版本号。当前版本号为 1。
- 鉴别分组类型字段长度为 2 个八位位组，其值含义如下：
  - “0”表示鉴别激活分组；

## GB 15629.11—2003

“1”表示接入鉴别请求分组；

“2”表示接入鉴别响应分组；

“3”表示密钥协商请求分组；

“4”表示密钥协商响应分组；

其他值保留。

——保留字段长度为2个八位位组，默认值为0。

——数据长度字段长度为2个八位位组，表示数据字段的八位位组数。

## 8.3.2.1.1 鉴别激活分组

由AP发往STA，鉴别分组类型为0，分组中的数据内容为空。

## 8.3.2.1.2 接入鉴别请求分组

由STA发往AP，鉴别分组类型为1，分组中的数据字段定义如图50：

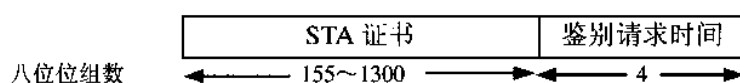


图 50 接入鉴别请求分组的数据字段

## 8.3.2.1.2.1 图 50 中 STA 证书定义如图 51：

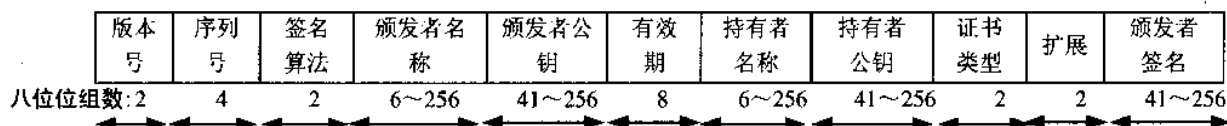


图 51 STA证书内容定义

——版本号字段长度为2个八位位组；

——序列号字段长度为4个八位位组；

——签名算法字段长度为2个八位位组，具体定义如图52：

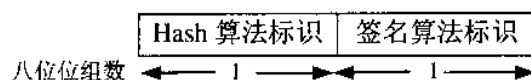


图 52 签名算法定义

## 1) Hash 算法标识为1个八位位组，其值含义如下：

“1”表示国家密码管理委员会办公室批准的用于WLAN的杂凑算法；  
其他值保留。

## 2) 签名算法标识为1个八位位组，其值含义如下：

“1”表示192位的椭圆曲线算法；

“2”表示224位的椭圆曲线算法；

“3”表示256位的椭圆曲线算法；

其他值保留。

——有效期字段长度为8个八位位组，具体定义如图53：

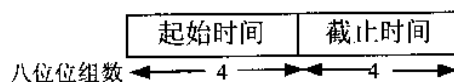


图 53 证书有效期定义

起始时间与截止时间均为4个八位位组，表示1970年1月1日0时起到当前时间的秒数计数值。

——证书类型字段为2个八位位组，标识证书应用的设备类型，其值定义如下：

“0”表示此证书为STA证书；

“1”表示此证书为AP证书；

“2”表示此证书为ASU证书；

其他值保留。

——扩展字段为2个八位位组，该字段保留。

——证书颁发者名称、证书颁发者公钥、证书持有者名称、证书持有者公钥以及颁发者签名均分别由长度字段与相应内容组成。其中长度字段均为1个八位位组，其值表示随后数据的八位位组数。

8.3.2.1.2.2 鉴别请求时间字段格式同证书有效期的起始时间。

#### 8.3.2.1.3 接入鉴别响应分组

由AP发往STA，鉴别分组类型为2，分组中的数据字段定义如图54：

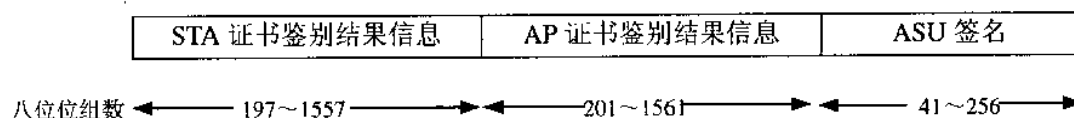


图 54 接入鉴别响应分组的数据内容

其中：

a) STA 证书鉴别结果信息字段定义如图55：

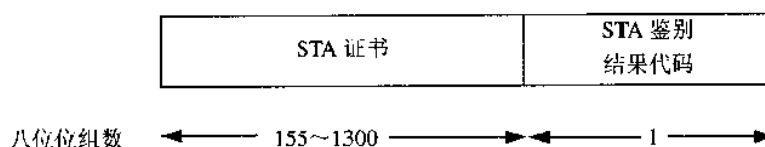


图 55 STA 证书鉴别结果信息定义

——STA 证书字段定义同8.3.2.1.2.1中的STA 证书字段。

——STA 证书鉴别结果代码字段长度为1个八位位组，表示ASU对证书的鉴别结果，其值含义如下：

“0”表示证书有效；

“1”表示证书未启用；

“2”表示证书已经过期；

“3”表示证书的颁发者不明确；

“4”表示签名错误；

其他值保留。

b) AP 证书鉴别结果信息字段定义如图56：

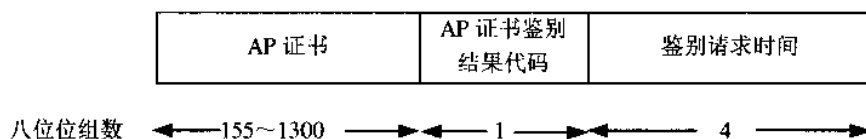


图 56 AP 证书鉴别结果信息定义

——AP 证书字段定义同 8.3.2.1.2.1 中的 STA 证书字段。

——AP 证书鉴别结果代码定义同 STA 证书鉴别结果代码。

c) ASU 签名表示 ASU 对 STA 和 AP 证书鉴别结果信息的签名，定义同证书颁发者签名。

#### 8.3.2.1.4 密钥协商请求分组

由 STA 发往 AP 或 AP 发往 STA，鉴别分组类型为 3，分组中的数据字段定义如图 57：

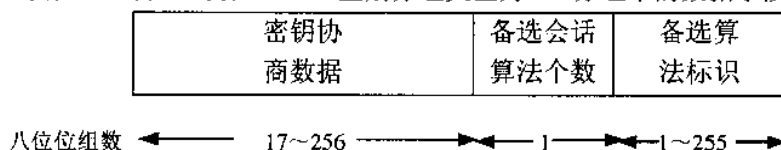


图 57 密钥协商请求分组的数据内容

其中：

——密钥协商数据字段由长度字段与相应内容组成。其中长度字段为 1 个八位位组，表示密钥协商数据的八位位组数。密钥协商数据是一串用对方公钥加密后的随机数据。本部分采用国家密码管理委员会办公室批准的用户 WLAN 的随机数产生算法。

——备选会话算法个数字段为 1 个八位位组，表示密钥协商请求方支持的会话算法的个数。该字段默认值为“1”，即仅支持国家密码管理委员会办公室批准的用于 WLAN 的对称密码算法。

——备选会话算法标识字段描述所有的备选算法。每种会话算法由一个字节描述。当前支持的会话算法标识定义如下：

“0”表示不加密；

“1”表示国家密码管理委员会办公室批准的用于 WLAN 的对称密码算法；

其他值保留。

#### 8.3.2.1.5 密钥协商响应分组

由 STA 发往 AP 或 AP 发往 STA，鉴别分组类型为 4，分组中的数据字段定义如图 58：

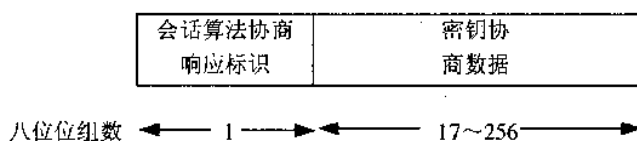


图 58 密钥协商响应分组的数据内容

其中：

——会话算法协商响应字段为 1 个八位位组。若值为“0”，则表示会话算法协商失败；否则其值为响应方从请求方的备选算法中选择的加密算法标识。

——密钥协商数据字段定义同 8.3.2.1.4。若会话算法协商失败，此字段为空。

#### 8.3.2.2 AP 与 ASU 之间的鉴别报文

AP 与 ASU 之间的通信采用 UDP 套接口，端口号为 9000。AP 与 ASU 之间鉴别报文的格式定义如图 59：



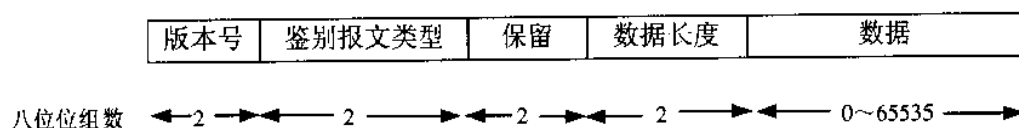


图 59 WAI 鉴别系统的数据报文基本格式

其中:

- 版本号字段长度为 2 个八位位组, 表示鉴别基础结构的版本号。当前版本号为 1。
- 鉴别报文类型字段长度为 2 个八位位组, 其值含义如下:
  - “5”表示证书鉴别请求报文;
  - “6”表示证书鉴别响应报文;
  - 其他值保留。
- 保留字段长度为 2 个八位位组, 默认值为 0。
- 数据长度字段长度为 2 个八位位组, 表示数据字段的八位位组数。

#### 8.3.2.2.1 证书鉴别请求报文

由 AP 发往 ASU, 鉴别报文类型为 5, 报文中的数据字段定义如图 60:

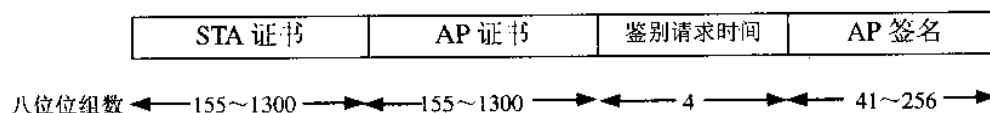


图 60 证书鉴别请求报文的数据内容

- STA 证书、AP 证书和鉴别请求+时间字段的定义同 8.3.2.1.2。
- AP 签名表示 AP 对证书鉴别报文中数据字段的签名。

#### 8.3.2.2.2 证书鉴别响应报文

由 ASU 发往 AP, 鉴别报文类型为 6, 报文中的数据字段定义如图 61:

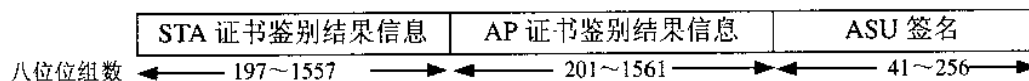


图 61 证书鉴别响应报文的数据内容

STA 证书鉴别结果信息和 AP 证书鉴别结果信息字段和 ASU 签名同 8.3.2.1.3。

### 8.4 WPI 保密基础结构

本部分采用国家密码管理委员会办公室批准的用于 WLAN 的对称密码算法实现数据保护, 对 MAC 子层的 MSDU 进行加、解密处理。

### 8.5 安全相关管理信息库

本条给出与鉴别和保密相关的 MIB 属性定义及其用法。MIB 属性的详细说明见 11.4。

#### 8.5.1 与鉴别相关的 MIB 属性

STA 是否启动鉴别功能由 MIB 属性系统鉴别控制参数 dot11SystemAuthControl 确定, 其值可取:

- 0: 不启动鉴别;
- 1: 启动鉴别;
- 其他为保留。

## GB 15629.11—2003

当 dot11SystemAuthControl 取值为“启动鉴别”时，系统的每一个受控端口的鉴别状态由鉴别控制类型 MIB 属性 dot11AuthControlledPortControl 确定，其值可取：

- 0：自动；
- 1：强制非鉴别；
- 2：强制已鉴别；
- 其他为保留。

当 dot11SystemAuthControl 取值为“不启动鉴别”时，系统的每一个受控端口的鉴别状态为已鉴别。

系统受控端口的鉴别状态的确定过程如下：

```

if dot11SystemAuthControl 为“不启动鉴别”
    此受控端口的鉴别状态为已鉴别（即不需要鉴别）
else
    if 对应此受控端口的 dot11AuthControlledPortControl 为“强制已鉴别”
        此受控端口的鉴别状态为已鉴别（即不需要鉴别）
    else
        if 对应此受控端口的 dot11AuthControlledPortControl 为“强制非鉴别”
            此受控端口的鉴别状态为未鉴别
        else
            if 鉴别结果为成功
                此受控端口的鉴别状态为已鉴别
            else
                此受控端口的鉴别状态为未鉴别

```

#### 8.5.2 与保密相关的 MIB 属性

这里给出与通信过程中数据保密相关的管理信息库属性及其用法，这些属性都是只可以设置但不能读的，即这些 MIB 属性不能通过 MAC 管理的 SAP 来读取。11.4 给出 MIB 属性的定义。

在系统的某一个受控端口是否启动 WPI 保密基础结构由管理信息库 MIB 属性 dot11PrivacyControlledPortInvoked 确定，该属性值为一个布尔变量。如果其值为“false”，则所有此受控端口接收或发送的 MSDU 均直接明文传送；如果值为“true”，则所有接收或发送的 MSDU 均必须经过加密或解密处理。

当某受控端口的 MIB 属性 dot11PrivacyControlledPortInvoked 值为“true”时，对经过此端口的 MSDU 数据加密或解密的密钥由 MIB 属性 dot11WPIControlledPortKey 确定。

#### 8.6 自组网（ad hoc）模式

在自组网中，所有 STA 可使用同一共享密钥实现鉴别与保密。

### 9 MAC 子层功能

本章提出 MAC 的功能描述。9.1 介绍了 MAC 子层的体系结构，包括分布式协调功能(DCF)、点协调功能(PCF)及它们在本部分 LAN 中的共存。9.2 和 9.3 对这些功能进行了扩展，并提供了其完整的功能描述。9.4 和 9.5 涉及到分段与重组。9.6 指出了多速率支持，9.7 列出了允许的帧交换序列。最后，9.8 描述了若干限定 MSDU 重新排序或丢弃的许多附加限制。

#### 9.1 MAC 体系结构

如图 62 所示通过 DCF 服务提供 PCF 描述了 MAC 体系结构。

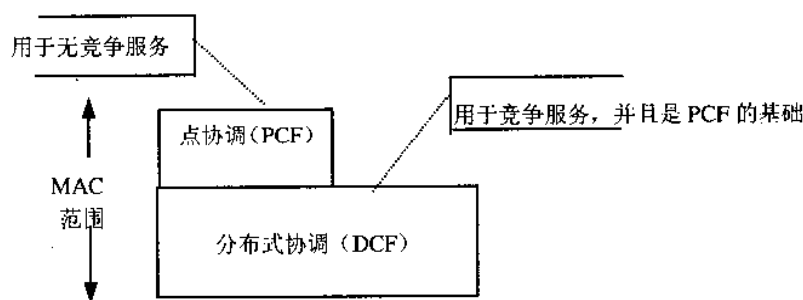


图 62 MAC 体系结构

### 9.1.1 分布式协调功能(DCF)

本部分 MAC 的基本访问方法是 DCF，称作带碰撞避免的载波侦听多址访问(CSMA/CA)。DCF 在所有的 STA 上均应实现，用于 IBSS 和基础结构网络配置中。

对于发送的 STA，它应侦听媒体以确定是否有其他的 STA 正在发送。如果不确定媒体为忙（见 9.2.1），传输可进行。CSMA/CA 分布式算法强制在连续的帧序列之间存在规定的最小持续期的间隙。发送 STA 应确保在试图发送之前需要的持续期内信道空闲。若确定媒体为忙，STA 应该推迟直到当前的传输结束为止。在缓发或者成功发送之后立即试图再次发送之前，STA 应选择随机退避时间间隔，并且当媒体空闲时，应递减退避时间间隔计数器。方法的细化用于在各种环境下进一步使碰撞数最小——这里发送和接收站在确定媒体空闲缓发和退避之后，在数据传输之前交换短控制帧[请求发送(RTS)和清除待发(CTS)帧]。9.2 中描述了 CSMA/CA、缓发和退避的细节。9.2 也提出了 RTS/CTS 交换。

### 9.1.2 点协调功能(PCF)

本部分 MAC 也可以包含一种称为 PCF 的可选的访问方法，仅用于基础结构网络配置中。该访问方法使用应运行在 BSS 接入点上的 PC，以确定当前哪个 STA 有发送的权利。该操作实质上是轮询操作，PC 担任轮询控制器的角色。PCF 的操作可能需要附加的协调（本部分未作规定）以允许在多个点协调的 BSS 在重叠物理区域的相同信道上操作时高效运行。

PCF 使用访问优先权机制辅助的虚拟载波侦听机制。PCF 在信标管理帧中分发信息，并通过设置 STA 的网络分配向量(NAV)来获取对媒体的控制。此外，在 PCF 下传送帧时采用的帧间间隔(IFS)比通过 DCF 机制传送帧时采用的 IFS 要小。使用较小的 IFS 意味着在根据 DCF 运行的重叠 BSS 内的 STA 上，点协调通信量应具有访问媒体的优先权。

由 PCF 提供的访问优先权可用于创建无竞争(CF)访问方法。PC 控制 STA 的帧传输，以消除有限时间段内的竞争。

### 9.1.3 DCF 和 PCF 的共存

DCF 和 PCF 可以在同一 BSS 内同时工作。当一个 PC 在 BSS 中工作时，两种访问方法交替使用，CFP 位于 CP 之前，具体见 9.3。

### 9.1.4 分段/重组综述

将 MAC 服务数据单元(MSDU)或 MAC 管理协议数据单元(MMPDU)划分成更小的 MAC 级帧——MAC 协议数据单元(MPDU)的过程称为分段。分段过程产生 MPDU，其长度小于原来 MSDU 或 MMPDU 的长度，以提高可靠性。对于长帧信道特性限制接收的可靠性，此时利用分段可提高 MSDU 或 MMPDU 成功传输的概率。分段由每个直接发送方完成。将多个 MPDU 重新组合成单个 MSDU 或 MMPDU 的过程定义为重组。重组由每个直接接收方完成。

只有具有单播接收方地址的 MPDU 才可被分段，而广播或组播帧不应被分段，即使它的长度已

## GB 15629.11—2003

超出分段阈值(aFragmentationThreshold)。

对于从 LLC 接收的定向 MSDU 或从 MAC 子层管理实体(MLME)接收的定向 MMPDU, 若长度大于 aFragmentationThreshold, 则 MSDU 或 MMPDU 将被分段。MSDU 或 MMPDU 被分解为多个 MPDU。每个分段为长度不超过 aFragmentationThreshold 的一个帧。每个分段均可能为小于 aFragmentationThreshold 的一个帧。分段由图 63 示出。

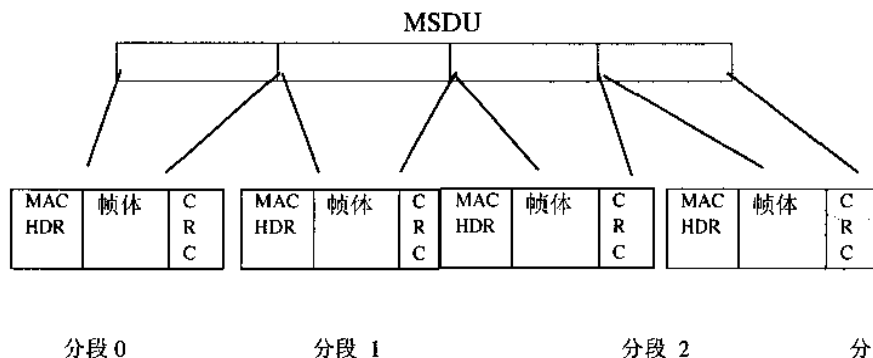


图 63 分段

由 MSDU 或 MMPDU 分段得到的 MPDU 被独立发送, 且每个分段被单独确认, 这允许对每个分段而不是对整个 MSDU 或 MMPDU 重传。对于给定的 PHY, 除非由于媒体占用的限制而被中断, 否则, 单个 MSDU 或 MMPDU 的所有分段应用一个 DCF 媒体访问规程调用在 CP 期间作为一个突发发送。单个 MSDU 或 MMPDU 的所有分段在 CFP 期间作为独立帧发送服从 PC 媒体访问规程的规则。

#### 9.1.5 MAC 数据服务

MAC 数据服务将来自 LLC 的 MAC 服务请求转换成 MAC 状态机使用的输入信号。MAC 状态服务将来自 MAC 状态机的输出信号转换成发给 LLC 的服务指示。转换由附录 C 定义的 MAC 数据服务状态机给定。

#### 9.2 分布式协调功能(DCF)

基本的媒体访问协议是 DCF, 在媒体忙条件后, 通过使用 CSMA/CA 和随机退避时间在兼容的 PHY 之间实现自动媒体共享。另外, 所有定向通信量采用立即的主动确认(ACK 帧), 若没有接收到 ACK 帧, 则发送方会安排重传。

CSMA/CA 协议就是为在很有可能发生碰撞的情况下减少访问媒体的多个 STA 之间的碰撞概率而设计。在媒体刚由繁忙变为空闲(由 CS 功能提示)时, 碰撞的概率最大。这是因为多个 STA 在等待媒体变得再次可用。在这种情况下, 采用随机退避规程来解决媒体竞争碰撞是非常必要的。

载波侦听通过物理机制和虚拟机制来实现。

虚拟载波侦听机制通过分发预约信息来宣布媒体将被使用来实现。在实际数据帧之前 RTS 和 CTS 帧的交换就是媒体预约信息分发的一种方法。RTS 和 CTS 帧包含一个持续时间/ID(Duration/ID)字段, 定义媒体将被保留以发送实际数据帧和返回 ACK 帧所需的时间周期。所有处于源 STA(发送 RTS 的 STA)或目的 STA(发送 CTS 的 STA)接收范围内的 STA 都将得知媒体的预约, 因此 STA 虽然不能接收来自源 STA 的信息, 但仍然知道媒体即将使用以发送数据帧。

分发媒体预约信息的另外一种方法是定向帧中的持续时间/ID 字段。该字段给出了到紧随其后的 ACK 帧的结束, 或当存在分段序列时到下一个分段后的 ACK 帧的结束为止媒体预约的时间。

RTS/CTS 交换还完成一类快速的碰撞判断与传输通道检测。如果发布 RTS 的源 STA 没有检测到返回的 CTS, 则源 STA 会(在遵守其他媒体使用原则的基础上)较快地重复该过程, 这比长数据帧已被发送而返回的 ACK 帧未被检测到的情况要快得多。

RTS/CTS 机制的另一个优点体现在使用同一物理交叠的信道的多个 BSS 时。媒体预约机制会跨越 BSA 的边界起作用。RTS/CTS 机制还可以改善一种典型情况下的操作，即所有 STA 可以接收 AP 的信息但不能接收 BSA 中所有其他 STA 的信息。

RTS/CTS 机制不能用于具有广播或组播定向地址的 MPDU，因为 RTS 帧将有多目的地址，潜在地会有多个同时发送的 CTS 帧进行应答。RTS/CTS 机制不需要用于每个数据帧的传输。因为额外的 RTS 和 CTS 帧会增加无效的开销，该机制并不总是合理的，尤其是对于短数据帧。

RTS/CTS 机制在属性 `dot11RTSThreshold` 的控制下操作。该属性可以在每个 STA 上设置。该机制允许 STA 被配置成总是使用 RTS/CTS、不使用 RTS/CTS 或仅对超出特定长度的帧使用 RTS/CTS 的三种操作方式。

配置成不使用 RTS/CTS 机制的 STA 会利用接收的 RTS 或 CTS 帧中包含的持续时间信息来更新其虚拟载波侦听机制，并且总是用 CTS 对传给它的 RTS 响应。

媒体访问协议允许 STA 支持不同的数据速率集。所有的 STA 应能以 `MLME_Join.request` 和 `MLME_Start.request` 原语规定的参数 `aBasicRateSet` 中的所有数据速率接收和发送。为了支持 RTS/CTS 和虚拟载波侦听机制的相应操作，所有 STA 都应能够检测 RTS 和 CTS 帧。为此 RTS 和 CTS 帧应以 BSS 基本速率集中的一个速率发送。（多速率操作的描述见 9.6）

在 DCF 下发送的数据帧应采用帧类型为数据、子类型为数据或空功能，接收数据类型帧的 STA 只将帧体作为可能发往 LLC 的指示的基础。

### 9.2.1 载波侦听机制

物理的和虚拟的载波侦听功能用于确定媒体的状态。只要任一功能指示媒体忙，媒体就被认为忙，否则媒体被认为空闲。

物理载波侦听机制应由 PHY 提供。该信息如何运送给 MAC 见第 12 章。物理载波侦听的细节由单独的 PHY 规范提供。

虚拟载波侦听机制由 MAC 提供，该机制被称为网络分配矢量(NAV)。NAV 基于持续时间信息对媒体上未来的通信量进行预测，该持续时间信息由数据交换前的 RTS/CTS 帧通告。该信息还可从在 CP 期间发送的除 PS-Poll 控制帧之外的所有帧的 MAC 头得到。9.2.5.4 描述 DCF 下使用 RTS/CTS 设置 NAV 的机制，9.3.2.2 描述 PCF 下 NAV 的使用。

载波侦听机制将 NAV 状态和使用物理载波侦听的 STA 的发送器状态结合在一起来确定媒体的忙闲状态。NAV 可被看作一个计数器，以均匀速率往下计数到 0。当计数器为 0 时，虚拟载波侦听指示为媒体闲；否则，指示为忙。只要 STA 正在发送，媒体就被确定为忙。

### 9.2.2 MAC 级确认

在 9.7、9.2.8 和 9.3.3.4 中描述的某些帧的接收，如果接收到的帧的 FCS 是正确的，则要求接收方 STA 用一个确认帧通常为 ACK 帧响应，该技术被称为主动确认。

没有接收到期望的 ACK 帧，则向源 STA 指示发生了错误。注意可能目的 STA 正确接收到帧，但 ACK 帧的接收出现了错误。对于帧交换的发起方而言，这种情况同发生在初始帧上的错误很难区分。

### 9.2.3 帧间间隔(IFS)

帧之间的时间间隔被称作 IFS。STA 通过载波侦听功能，判断媒体在规定的时间内是否空闲。定义了四种不同的 IFS 以提供访问无线媒体的优先级，由短到长依次排列。图 64 示出它们之间的关系。

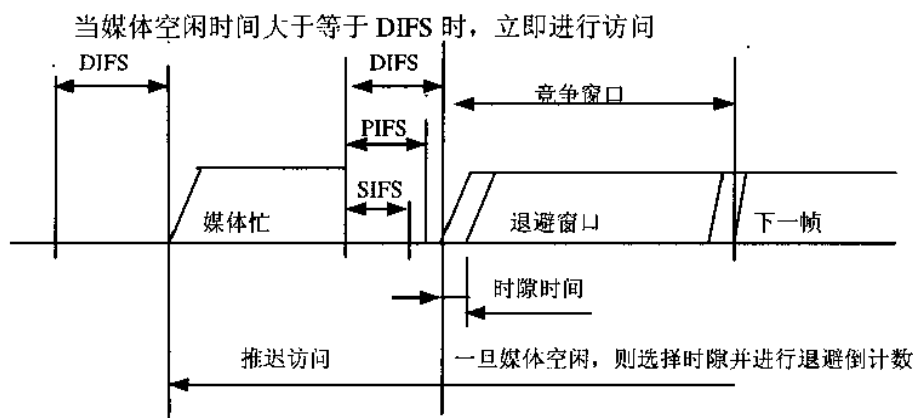


图 64 IFS 之间的关系

- a) SIFS 短的帧间间隔；
- b) PIFS PCF 帧间间隔；
- c) DIFS DCF 帧间间隔；
- d) EIFS 扩展的帧间间隔。

不同的 IFS 与 STA 的比特速率无关。IFS 定时定义为媒体的时间间隔，并且对于每个 PHY 固定不变（即使在具有多速率的 PHY 中）。IFS 的值由 PHY 规定的属性确定。

#### 9.2.3.1 短 IFS (SIFS)

SIFS 用于 ACK 帧、CTS 帧、分段突发的第二个或后续的 MPDU 以及 STA 对 PCF 任何轮询的响应。SIFS 还可以被 PC 用于 CFP 期间的任意类型帧（见 9.3）。SIFS 为从前一帧的最后符号结束到在空中接口看到的后续帧前导码的第一个符号开始之间的时间。SIFS 可以或应当适用的有效情况由 9.7 的帧交换序列列出。

当后续帧的传输在 9.2.10 规定的 TxSIFS 时隙边界启动时，得到 SIFS 定时。本部分不允许在媒体上测量的 SIFS 与其额定值之差超出 PHY aSlotTime 的  $\pm 10\%$ 。

SIFS 为最短的帧间间隔。当 STA 已经获得媒体使用权且需要保持完成帧交换序列的持续时间时，应使用 SIFS。帧交换序列传输之间采用最小的时间间隔，以阻止那些需要等待更长媒体空闲时间的 STA 试图使用媒体，从而为已启动的帧交换序列的完成提供优先权。

#### 9.2.3.2 PCF IFS (PIFS)

PIFS 只能被操作在 PCF 下的 STA 使用，以获得在 CFP 启动时访问媒体的优先权。使用 PCF 的 STA 允许发送无竞争通信量，只要其载波侦听机制（见 9.2.1）确定媒体在 9.2.10 定义的 TxPIFS 时隙边界上空闲。9.3 条描述了操作在 PCF 下的 STA 对 PIFS 的使用。

#### 9.2.3.3 DCF IFS (DIFS)

DIFS 由操作在 DCF 下的 STA 使用，以发送数据帧(MPDU)和管理帧(MMPDU)。采用 DCF 的 STA 允许发送，只要其载波侦听机制（见 9.2.1）确定媒体在 9.2.10 定义的 TxDIFS 时隙边界上空闲，并且此时帧已正确接收且退避时间到期。若接收到原语 PHY-RXEND.indication 包含错误的帧或 MAC FCS 值不正确的帧，即使确定媒体空闲，采用 DCF 的 STA 也不允许在 EIFS 期间进行发送。只有接收到使 STA 重新同步且没有错误的后续帧后，STA 才可以发送。STA 允许利用此帧后的 DIFS 进行发送。

#### 9.2.3.4 扩展的 IFS (EIFS)

只要 PHY 向 MAC 指示帧的传输已经开始，并且此帧会引起具有正确 FCS 值的完整 MAC 帧的不正确接收，则 DCF 应使用 EIFS。EIFS 的持续时间在 9.2.10 中定义。不考虑虚拟载波机制，EIFS 间隔从检测到错误帧到 PHY 指示媒体空闲开始。EIFS 定义以便在 STA 开始发送前为另一 STA 提供

足够的时间对该 STA 的未正确接收帧确认。在 EIFS 期间, 接收到无错误的帧使 STA 重新同步到媒体的实际忙/闲状态, 此时 EIFS 结束, 并在接收完此帧后继续正常的媒体访问过程 (利用 DIFS, 如果必要则进行退避)。

#### 9.2.4 随机退避时间

需要启动传送数据 MPDU 或管理 MMPDU 的 STA 应激活载波侦听机制 (见 9.2.1) 来确定媒体的忙/闲状态。如果媒体为忙, 则 STA 将推迟, 直到媒体在一段时间内一直空闲。当媒体检测到的最后一帧被正确接收时, 这段时间等于 DIFS, 当媒体检测到的最后一帧没有被正确接收时, 这段时间等于 EIFS。在该 DIFS 或 EIFS 媒体空闲时间后, STA 还要在发送前产生额外的随机时延进行退避, 除非退避定时器已包含非 0 值 (此时无需选取随机数)。这个过程减少了推迟到同一时间点上的多个 STA 之间的竞争碰撞概率。

Backoff Time (退避时间) =  $\text{Random}() \times \text{aSlotTime}$

其中,  $\text{Random}()$  为在  $[0, \text{CW}]$  范围内均匀分布的伪随机整数。CW 为整数, 其值处于 PHY 特性值  $\text{aCWmin}$  和  $\text{aCWmax}$  之间, 即  $\text{aCWmin} \leq \text{CW} \leq \text{aCWmax}$ 。重要的是设计者认识到不同 STA 的随机数据流的统计独立性的必要性。

$\text{aSlotTime}$  取相应的名为 PHY 特性值。

竞争窗口 (CW) 参数取  $\text{aCWmin}$  为初始值, 每个 STA 均维护 STA 短重传计数 (SSRC) 与 STA 长重传计数 (SLRC), 且两者均取 0 为初始值。只要与 MSDU 关联的短重传计数加 1, SSRC 就加 1; 与 MSDU 关联的长重传计数加 1, SLRC 就加 1。每次当不能成功发送 MPDU 时, CW 取集合中的下一个值, 同时引起 STA 重传计数器之一加 1, 直到 CW 达到  $\text{aCWmax}$  值为止。重传定义为在试图交付一个 MPDU 由 SIFS 隔开的发送的全部帧序列, 描述为 9.7。一旦达到最大值  $\text{aCWmax}$ , CW 应保持值为  $\text{aCWmax}$  直到被复位, 这提高了高负载情况下访问协议的稳定性。见图 65。

当 SLRC 达到长重传限制 ( $\text{aLongRetryLimit}$ ), 或 SSRC 达到短重传限制 ( $\text{dot11ShortRetryLimit}$ ) 时, 在每次成功发送 MSDU 或 MPDU 后 CW 均被复位至  $\text{aCWmin}$ 。只要接收到 RTS 帧的响应帧 CTS, 或者接收到 MPDU 或 MMPDU 的确认帧 ACK, 或者在发送帧的“地址 1”字段具有组地址, SSRC 就复位为 0。只要接收到长度超出  $\text{dot11RTSThreshold}$  的 MPDU 帧或 MMPDU 的传输响应帧 ACK 帧, 或者发送帧的“地址 1”字段具有组地址, SLRC 就复位为 0。

CW 值的设置为 2 的顺序递增的整数次幂减 1, 从 PHY 规定的  $\text{aCWmin}$  开始往上增加到 PHY 规定的  $\text{aCWmax}$ 。

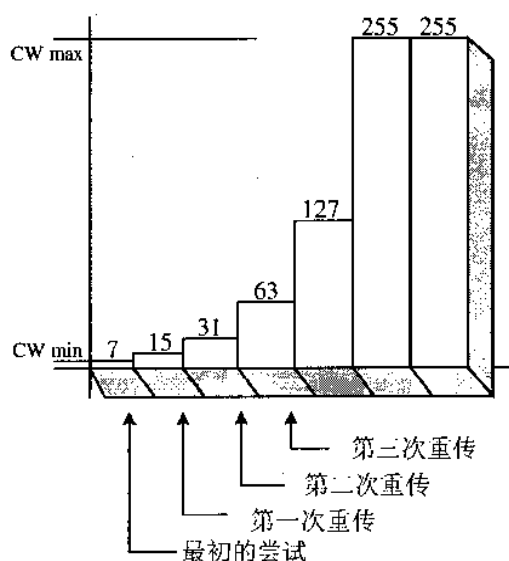


图 65 CW 的指数方式增长示例

## GB 15629.11—2003

## 9.2.5 DCF 访问规程

CSMA/CA 访问方法是 DCF 的基础，DCF 和 PCF 间的操作规则差别很小。

## 9.2.5.1 基本访问

基本访问指 STA 用于确定它是否可以发送的核心机制。

通常，当 STA 确定媒体的空闲时间大于或者等于 DIFS 时，或者如果前面的媒体忙事件是由于检测到没有接收到正确 FCS 值的帧而引起的，则媒体空闲时间大于或等于 EIFS，使用 DCF 操作的 STA 可以发送一个挂起的 MPDU，可以在没有 PC 的情况下进行，也可以在 PCF 访问方法的 CP 期间内进行。在这些条件下，CF 期间除外，如果 STA 想启动 9.7 描述的帧交换的初始帧，载波侦听机制确认媒体为忙，则遵循 9.2.5.2 描述的随机退避算法。在 9.2.5.2 和 9.2.5.5 所规定的情况下，即使首次尝试启动帧交换序列，也要遵循随机退避算法。

具有 FH PHY 的 STA，在驻留时间边界处将丢失对信道的控制权，因此在驻留时间边界后 STA 必须竞争信道，这要求具有 FH PHY 的 STA 在驻留时间边界之前就完成完整的 MPDU 与关联的确认帧（如果需要）的传输。在发送或重新发送 MPDU 时，如果没有足够的驻留时间以完成 MPDU 与确认帧（如果需要）的传输，则 STA 应利用当前的 CW（CW 不取下一个值）选择一个随机退避时间推迟传输。MSDU 的短重传计数器和长重传计数器不受影响。

基本访问机制如图 66 所示。

媒体空闲时间大于等于 DIFS，则立即访问媒体

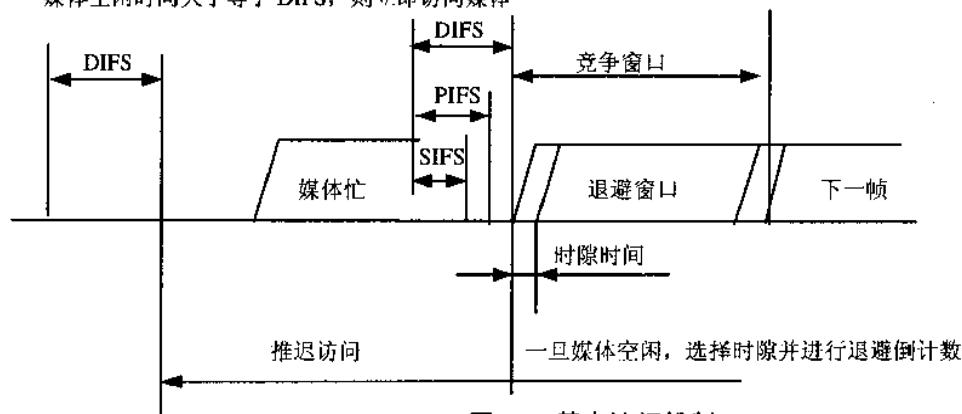


图 66 基本访问机制

## 9.2.5.2 退避规程

当物理或虚拟载波侦听机制指示媒体为忙时，STA 激活退避过程进行帧的传送（见图 67）。当正在发送的 STA 推测出如 9.2.5.7 或 9.2.8 定义的传输失败，也会激活退避过程。

为了开始退避过程，STA 应利用 9.2.4 中的公式将退避定时器置为一个随机退避时间。媒体在 DIFS 时间内被确认为一直空闲时，退避时隙紧接在 DIFS 后出现；或者在检测到一个未被正确接收的帧之后的 EIFS 时间内，如果媒体被确认为一直空闲，那么在 DIFS 后进行退避过程。

执行退避过程的 STA 采用载波侦听机制(9.2.1)来确定在每个退避时隙期间媒体状态是否有活动，如果在特定的退避时隙内，无媒体活动指示，则退避过程将退避时间减小 aSlotTime。

如果在退避时隙的任何时刻，媒体被确定为忙，则退避过程被挂起。也就是说，退避定时器在该时隙内不减小。在恢复退避过程之前，媒体应在适当的 DIFS 或 EIFS 期间（见 9.2.3）被确定为空闲。只要退避定时器减小到 0，传输过程就可以开始。

当数据类型帧、管理类型帧或子类型为 PS-Poll 的控制类型帧的 MPDU 的多分段比特设置为 0 时，每次传输结束后均应立即执行退避过程，即使当前的等待队列中没有其他发送。若传输已确认成功，则 ACK 帧的接收过程一结束，就立即开始退避过程。如果需要确认的传输过程没有成功，那么在 ACK 帧超时后开始退避过程。若传输成功，CW 值在选择随机退避间隔前变为 aCWmin，且 STA



的短重传计数和长重传计数按 9.2.4 描述的进行更新, 以确保 STA 发出的帧总是被至少一个退避间隔分开。

该规程的结果就是当多个 STA 推迟且进入随机退避时, 利用随机函数选择的最小退避时间的 STA 赢得竞争。

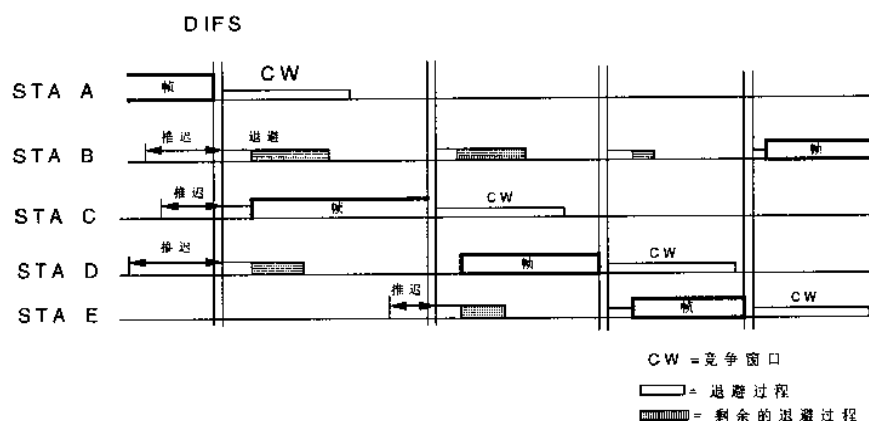


图 67 退避规程

在 IBSS 中, 对于挂起的非信标帧或非 ATIM 帧的传输, 退避时间在从目标信标传输时间(TBTT)到 ATIM 窗口耗尽的期间内不减小; 对于挂起的 ATIM 管理帧, 退避时间仅在 ATIM 窗口范围内减小(见第 11 章)。在 IBSS 内, 在信标帧的传输之前应产生独立的退避间隔, 描述见 11.1.2.2。

#### 9.2.5.3 恢复规程和重传限制

错误恢复由启动帧交换序列的 STA 负责, 定义见 9.7。许多情况都可能引起需要恢复的错误。例如在 RTS 帧发送之后没有返回 CTS 帧, 这种情况可能是由于与另一个传输发生碰撞, 或者由于在 RTS 或 CTS 帧的发送期间信道上存在干扰, 或者因为接收 RTS 帧的 STA 具有活动的虚载波侦听条件(指示媒体状态为忙的时间期间)。

错误恢复启动 STA 通过推断已失败的帧交换序列重新传输来实现。对于每个传输失败的帧交换序列, 重传一直继续, 直到传输成功或者达到相应重传限制为止。STA 为每个等待传输的 MSDU 或 MMPDU 维护一个短重传计数和一个长重传计数, 这些计数器的增加与复位相互独立。

在发送完 RTS 帧之后, STA 执行 9.2.5.7 定义的 CTS 规程。若 RTS 传输失败, 则 MSDU 或 MMPDU 的短重传计数与 STA 的短重传计数加 1, 该过程继续, 直到试图发送 MSDU 或 MMPDU 的次数达到 dot11ShortRetryLimit 为止。

在发送完需要确认的帧之后, STA 执行 9.2.8 定义的 ACK 规程。对于 MSDU 或 MMPDU 而言, 每次当长度小于或等于 dot11RTSThreshold 的 MAC 帧的传输失败时, MSDU 或 MMPDU 的短重传计数和 STA 的短重传计数加 1; 每次当传输成功时, MSDU 或 MMPDU 的短重传计数和 STA 的短重传计数被复位。对于 MSDU 或 MMPDU 而言, 每次当长度超出 dot11RTSThreshold 的 MAC 帧的传输失败时, MSDU 或 MMPDU 的长重传计数和 STA 的长重传计数加 1; 每次当传输成功时, MSDU 或 MMPDU 的长重传计数和 STA 的长重传计数被复位。对于 ACK 过程出现一次或多次失败的 MSDU 或 MMPDU, 在随后的所有重传尝试时, 数据和管理帧中的重传字段设置为 1。传输失败的重传过程一直继续, 直到 MSDU 或 MMPDU 的短重传计数达到 dot11ShortRetryLimit, 或者 MSDU 或 MMPDU 的长重传计数达到 aLongRetryLimit。不论先到达哪个限制值, 重传过程都将终止, 并丢弃该 MSDU 或 MMPDU。

在 ESS 中, 处于节能模式的 STA 通过发送 PS-Poll 帧请求来自 AP 的数据, 以启动帧交换序列。当没有从 AP 处收到 ACK 帧或者数据帧的响应 PS-Poll 帧时, STA 应在适当的时候通过发送另一个 PS-Poll 帧来重传该序列。如果 AP 发送数据帧来响应 PS-Poll 帧, 但没有收到确认该数据帧的 ACK

## GB 15629.11—2003

帧,则来自同一 STA 的下一个 PS-Poll 帧将引起最后一个 MSDU 的重传。该重复的 MSDU 将被接收方 STA 采用正常的重复帧过滤机制进行滤除。如果 AP 通过发送 ACK 帧来响应 PS-Poll 帧,则对数据帧交付错误恢复的责任就转移至 AP,这是因为数据在后续的帧交换序列中进行传送,而该序列是由 AP 启动的。AP 利用对定向 MSDU 有效的任何帧交换序列来试图将 MSDU 传送到发送 PS-Poll 帧的 STA。如果发送 PS-Poll 帧且处于节能模式的 STA 在发送 ACK 帧作为 MSDU 成功接收的响应之后,返回到休眠状态,而 AP 未能接收到该 ACK 帧,则 AP 将重传该 MSDU,直到达到相应的重传限制。额外的 PS-Poll 帧的过滤详见第 11 章。

## 9.2.5.4 设置和复位 NAV

接收到有效帧的 STA 将利用收到的持续时间/ID 字段的信息来更新自己的 NAV,但只有当新的 NAV 值大于当前的 NAV 值,且该帧未寻址到该接收方 STA 时才进行更新。其他条件也可设置或复位 NAV,在 9.3.2.2 描述。当 NAV 复位时,应发布原语 PHY-CCARESET.request。

图 68 指示 STA 可接收 RTS 帧的 NAV,而其他 STA 仅能接收 CTS 帧,导致如图示出的较小 NAV 值(除了 RTS 要发往的那个 STA)。

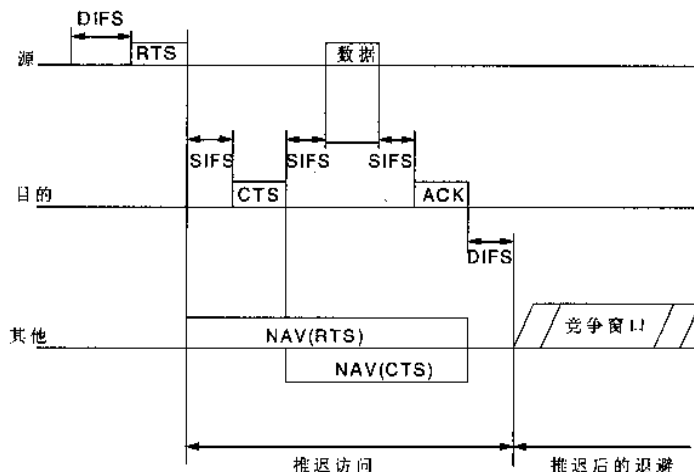


图 68 RTS/CTS/数据/ACK 和 NAV 设置

在与 RTS 帧检测相应的原语 PHY-RXEND.indication 开始后的持续时间为  $(2 \times aSIFSTime) + (CTS\_Time) + (2 \times aSlotTime)$  的时间段内,如果 PHY 未检测到原语 PHY-RXSTART.indication,则该 STA 允许将 RTS 帧中的信息作为最近的基准值来更新 NAV 的 STA 将其 NAV 复位。“CTS\_Time”应利用 CTS 帧的长度和接收用于最近 NAV 更新的 RTS 帧时采用的数据速率进行计算。

## 9.2.5.5 信道控制

SIFS 用于提供有效的 MSDU 交付机制。一旦 STA 竞争到信道,则该 STA 持续发送分段,直到某个 MSDU 或 MMPDU 的所有分段均被发送而没有收到一个确认,或者由于驻留时间边界,STA 不再发送其他任何分段为止。若由于上述原因使分段的发送中止,则只有等下次传输机会出现,该 STA 才能继续传输。如果传输没有成功,STA 用于确定下次重传哪个未传送的 MSDU 的算法超出本部分范围,但是任何一种算法都要遵守 9.8 中列出的限制。

图 69 给出了利用 SIFS 的多分段 MSDU 的传输。

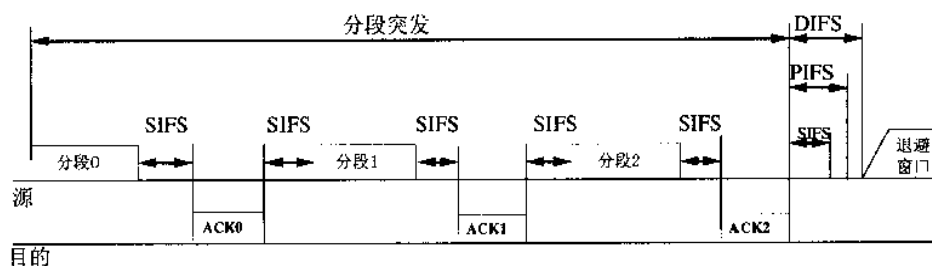


图 69 利用 SIFS 的多分段 MSDU 的传输

当源 STA 发送完一个分段后，它将释放信道，然后立即监控信道等待确认帧，描述见 9.2.8。

当目的 STA 发送完确认帧后，其后的 SIFS 被保留以使源 STA 继续发送（如需要）下一分段，发送确认帧的 STA 不能在确认后立即在信道上开始发送过程。

竞争到信道后发送多个分段的过程定义为分段突发。

如果源 STA 接收到确认帧后，由于驻留边界而没有足够的时间发送下一分段和接收确认帧，则源 STA 将在下一个驻留时间开始时竞争信道。

如果源 STA 没有收到确认帧，则它在执行完退避过程和竞争过程后，按 9.8 中的定义试重发送失败的 MSDU 或另一个合适的 MPDU。

在 STA 竞争到信道以重新发送 MSDU 的一个分段时，从未被确认的最后一个分段开始。目的 STA 按顺序接收分段（因为源 STA 按顺序发送分段，而且它们被单独确认）。然而目的 STA 可能接收到重复分段，接收方 STA 负责检测和丢弃重复分段。

在分段突发期间，只有在下述条件下 STA 将在 SIFS 后进行发送：

- STA 刚接收到需要确认的分段；
- 源 STA 接收到前一个分段的确认帧，并且还有同一 MSDU 的更多分段需要发送，同时在下一个驻留边界前有足够的时间来发送下一个分段和接收对它的确认。

同时还要满足下述规则：

- 如果 STA 发送的是一帧而不是一个初始或中间位置的分段，在该帧被确认之后，不执行退避规程，则不能在信道上发送；
- 当 MSDU 交付成功或者所有的重传尝试都已经失败而 STA 还有后续的 MSDU 需要发送时，STA 应执行退避规程；
- 只有未被确认的分段才进行重传。

#### 9.2.5.6 使用 RTS/CTS 传送分段

下面描述了使用 RTS/CTS 传送分段的 MSDU 或 MMPDU，RTS/CTS 帧定义了随后的帧与确认帧的持续时间。数据帧和确认帧(ACK)中的持续时间/ID 字段确定了下一个分段及其确认帧的总持续时间，如图 70 所示。

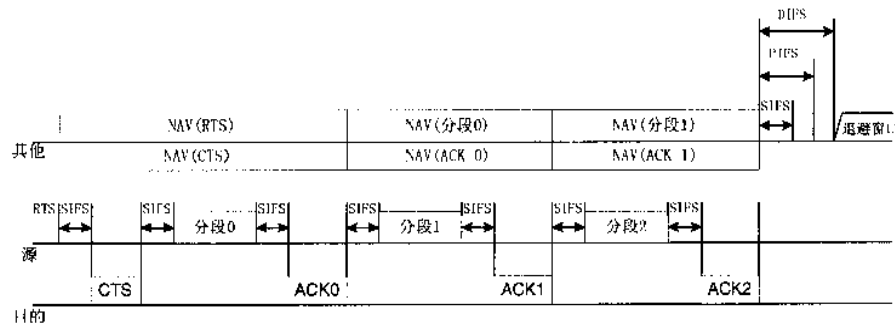


图 70 分段的 MSDU 与 RTS/CTS

## GB 15629.11—2003

每个帧包含定义下一次传输持续时间信息。RTS 帧的持续时间信息用于更新 NAV，以指示直到 ACK0 结束为止媒体一直为忙，CTS 帧的持续时间信息也用于更新 NAV，以指示直到 ACK0 结束为止媒体一直为忙。分段 0 和 ACK0 均包含持续时间信息来更新 NAV，指示直到 ACK1 结束为止媒体一直为忙。这将通过使用数据帧和 ACK 帧中的持续时间/ID 字段完成，并且一直进行到最后一个分段及其 ACK 为止。最后一个分段的持续时间等于一个 ACK 帧的发送时间加上 SIFS 时间，其 ACK 帧的持续时间/标识字段设置为 0。每个分段和 ACK 充当虚拟的 RTS 和 CTS，因此在 RTS/CTS 启动帧交换序列后，即使后续分段大于 dot11RTSThreshold，也无需产生更多的 RTS/CTS 帧。对于使用跳频 PHY 的 STA，当在下一个驻留时间边界前没有足够的时间来发送后续分段时，则启动帧交换序列的 STA 在驻留时间边界前发送的最后的帧或管理帧中，将持续时间/ID 字段设置为一个 ACK 帧的发送时间加上一个 SIFS 时间。

当确认帧已被发送但尚未被源 STA 接收时，侦听到分段或 ACK 帧的 STA 将标识下一帧交换时信道为忙，这是由于 NAV 已经根据这些帧的信息进行了更新。这是最差的情况，在图 71 示出。如果目的 STA 未发送确认，只能侦听到目的 STA 的 STA 将不会更新它们的 NAV，并且只有当它们的由以前接收的帧更新的 NAV 达到 0 后，才试图访问信道。而对于能侦听到源 STA 的 STA，当根据已发送的分段更新的 NAV 标识到期后，就可自由访问信道。

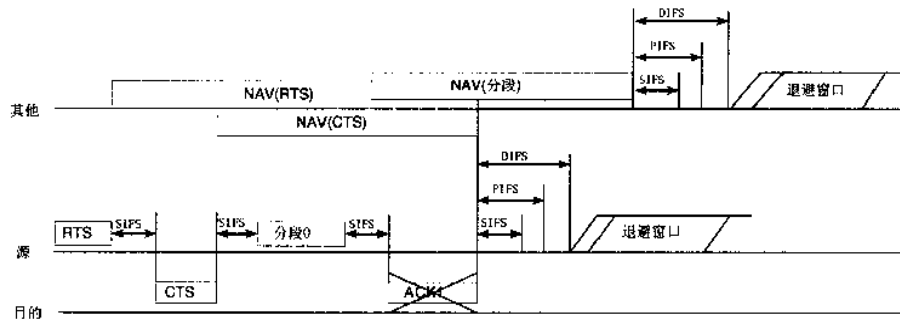


图 71 具有发送优先权而没有得到确认的 RTS/CTS

## 9.2.5.7 CTS 规程

如果 RTS 帧的目的 STA 已经接收到该 RTS 帧，并且其 NAV 指示媒体在一个 SIFS 周期内为空闲，则该 STA 将发送 CTS 帧。如果接收 RTS 的 STA 的 NAV 指示媒体非空闲，则该 STA 不会响应 RTS 帧。CTS 帧中 RA 字段的值来自 RTS 的 TA 字段，对于该 RTS 帧，CTS 帧为其响应帧。在 CTS 帧中，持续时间/ID 字段的值等于接收到的 RTS 帧的持续时间字段内的值减去 aSIFSTime 和以 RTS 帧的数据速率发送 CTS 帧所需要的时间。

发送 RTS 帧之后，STA 从原语 PHY-TXEND.confirm 开始等待超时时间(CTSTimeout)间隔。如果在 CTSTimeout 间隔期间没有出现原语 PHY-RXSTART.indication，STA 将认为 RTS 传输失败，并且在 CTSTimeout 间隔到期后激活退避规程。如果在 CTSTimeout 间隔期间出现原语 PHY-RXSTART.indication，则 STA 将等待相应的原语 PHY-RXEND.indication 以确定 RTS 传输是否成功。与 PHY-RXEND.indication 相对应，识别出 RTS 帧接收方发送的有效的 CTS 帧应被解释为成功响应，并允许帧序列继续进行（见 9.7）。任何其他识别结果，包括对其他有效帧的识别，应被认为 RTS 传输失败。此时 STA 将在接收到原语 PHY-RXEND.indication 时激活退避规程，并处理接收帧。

## 9.2.6 定向 MPDU 的传送规程

只有当 MPDU 的长度超出属性 dot11RTSThreshold 指示的长度门限时，STA 才将 RTS/CTS 交换用于定向 MPDU。

属性 dot11RTSThreshold 是 MAC MIB 内的一个被管理对象，它的值由 MAC LME 设置和获取。0 值指示所有的 MPDU 均应利用 RTS/CTS 交付；大于最大 MSDU 长度的 dot11RTSThreshold 值则指

示所有的 MPDU 均不通过 RTS/CTS 交付。

当采用 RTS/CTS 交换时,在 CTS 帧结束并经过 SIFS 时间后发送异步数据帧。在发送该数据帧时,不需要考虑媒体的忙闲状态。

当未使用 RTS/CTS 交换时,在基本访问规程成功后将发送异步数据帧。不论是否采用 RTS/CTS 交换规程,异步数据帧的目的 STA 将随后进行 ACK 规程。

### 9.2.7 广播与组播 MPDU 的传送规程

若没有 PCF,则当 STA 传送 ToDS 比特清空的广播或组播 MPDU 时,仅采用基本访问规程。不论帧的长度如何,均不采用 RTS/CTS 交换。此外,任何帧的接收方均不发送 ACK 帧。任何 ToDS 比特被置位的广播或组播 MPDU 由 STA 传送时,不仅遵从 CSMA/CA 的基本访问规程,而且遵从 RTS/CTS 交换规则,因为 MPDU 是直接发往 AP 的。广播或组播消息应分发到 BSS,发出报文的 STA 也将接收到此消息。因此所有 STA 将滤除源地址为自身地址的广播/组播报文。广播或组播 MSDU 应传播到 ESS。

除了那些 ToDS 比特置位的发送帧,广播或组播帧没有 MAC 级恢复。由于干扰、碰撞或时变信道特性增大了帧的丢失概率,因此相对定向通信量的可靠性而言,这种通信量的可靠性有所下降。

### 9.2.8 ACK 规程

ACK 帧的产生如 9.7 列出的帧交换序列。

在成功接收到 ToDS 比特置位且需要确认的帧后,AP 应产生 ACK 帧。ACK 帧由非 AP 的目的 STA 发送,只要它成功接收了要求确认的一类单播帧而非广播或组播帧。成功接收到需要确认的帧后,ACK 帧的传输应在 SIFS 时间后开始,而不考虑媒体的忙闲状态。

源 STA 等待 ACKTimeout 时间而没有接收到 ACK 帧,则判断 MPDU 发送失败(见图 72)。

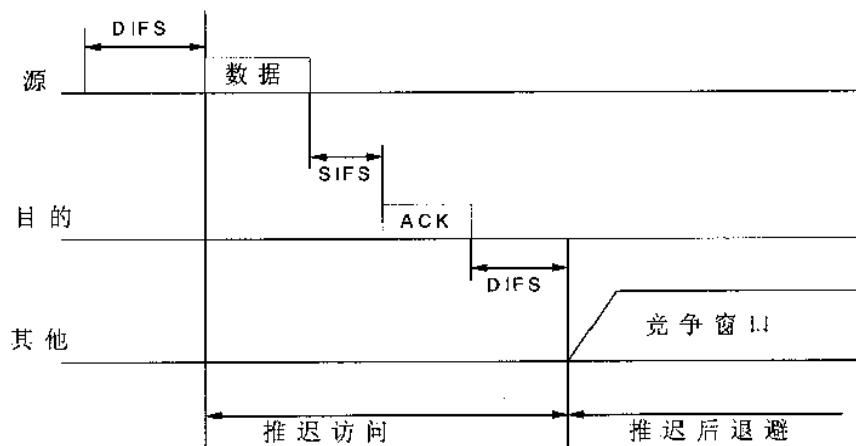


图 72 直接数据/ACK 的 MPDU

在发送完需要 ACK 帧响应的 MPDU 后(见 9.7),STA 将在原语 PHY-TXEND.confirm 开始等待一个 ACKTimeout 间隔。如果在 ACKTimeout 间隔期间没有出现原语 PHY-RXSTART.indication,STA 将认为 MPDU 传输失败,并在 ACKTimeout 间隔到期后激活退避过程。如果在 ACKTimeout 间隔期间出现 PHY-RXSTART.indication,则 STA 将等待相应的 PHY-RXEND.indication 以确定 MPDU 传输是否成功。对应于原语 PHY-RXEND.indication,对需要确认的 MPDU 的接收方发送的有效的 ACK 帧的识别将被解释为成功确认,允许帧序列继续或无需重传而结束。对任何其他、包括任何其他有效帧的识别将被解释为是 MPDU 传输失败。此时 STA 将在原语 PHY-RXEND.indication 时激活退避过程,并处理接收帧。惟一例外的是对 PS-Poll 帧接收方发送的有效数据帧的识别也将作为对 PS-Poll 帧的成功确认。

### 9.2.9 重复帧的检测与恢复

## GB 15629.11—2003

由于协议中有 MAC 级的确认和重传机制, 因此同一帧可能被多次接收, 这种重复帧将在日的 MAC 中被滤除。

重复帧的过滤由数据和管理帧中包含的序列控制字段(由序列号与分段号组成)实现。属于同一 MSDU 的 MPDU 具有相同的序列号, 不同的 MSDU (极可能) 具有不同的序列号。

序列号由发送方 STA 产生, 且为一个整数递增序列。

正在接收的 STA 应缓存最近接收的(地址 2, 序列号, 分段号)元组。正在接收的 STA 应仅保持最近的缓存表项“地址 2-序列号”对, 且只存储最近接收的对应于“地址 2-序列号”对的分段号。正在接收的 STA 忽略缓存中由广播/组播帧或 ATIM 帧得到的元组。

目的 STA 将任一个帧控制字段的重传比特置位的、与缓存表项(地址 2、序列号、分段号)元组相匹配的帧作为重复帧进行拒绝。

由于上述匹配, 帧被不适当拒绝的可能小, 然而这种情况非常少见, 且只是简单地导致了帧的丢失(类似于其他 LAN 协议中的 FCS 错误)。

目的 STA 在成功接收所有要求确认的帧后均执行 ACK 规程, 即使该帧由于重复过滤而被丢弃。

#### 9.2.10 DCF 的定时关系

IFS 规范之间的关系定义为媒体上的时间间隙, 关联属性由特定的 PHY 提供(见图 73)。

以传输结束时刻为基准的所有定时应以媒体上一帧的最后一个符号的结束时刻作为基准点。传输开始指的是媒体上下一帧的第一个符号。

每个 PHY 的 aSIFSTime 与 aSlotTime 是固定的。

$aSIFSTime = aRXRFDelay + aRXPLCPDelay + aMACProcessingDelay + aRxTxTurnaroundTime$

$aSlotTime = aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay$

PIFS 与 DIFS 由下列等式导出, 如图 73 所示:

$PIFS = aSIFSTime + aSlotTime$

$DIFS = aSIFSTime + 2 \times aSlotTime$

EIFS 由 SIFS、DIFS 和以 1Mbit/s 的速率发送 ACK 控制帧所需的时间长度根据下面等式导出:

$EIFS = aSIFSTime + (8 \times ACKSize) + aPreambleLength + aPLCPHeaderLength + DIFS$

式中:

ACKSize 为 ACK 帧的长度, 以八位位组为单位;

$(8 \times ACKSize) + aPreambleLength + aPLCPHeaderLength$  为以 PHY 的最低必备速率发送所需的微秒数。

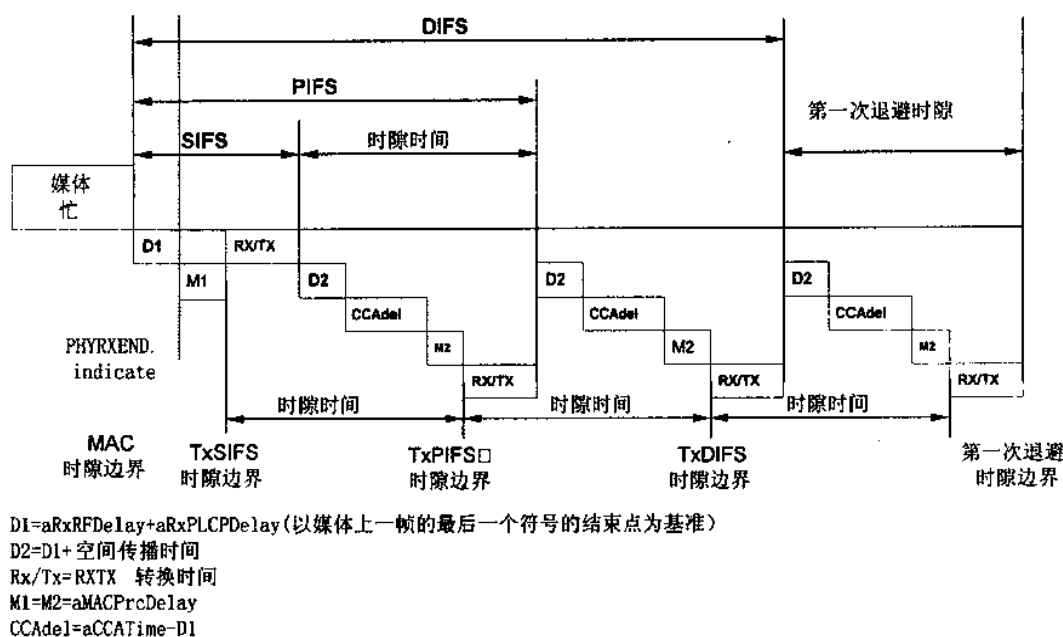


图 73 DCF 的定时关系

图 73 示出了 SIFS、PIFS 和 DIFS 之间的关系，它们在媒体上不同的 MAC 时隙边界 TxSIFS、TxPIFS 和 TxDIFS 进行测量。在对前一时隙的 CCA 结果的后续检测后，这些时隙边界定义了发射机应在何时被 MAC 打开以满足媒体上的不同 IFS 定时。

下述等式利用 PHY 提供的用于补偿实现的定时变化的属性，定义了 MAC 的时隙边界。

这些时隙边界的开始参考点为媒体上前一帧最后符号的结束时刻。

$$TxSIFS = SIFS - aRxTxTurnaroundTime$$

$$TxPIFS = TxSIFS + aSlotTime$$

$$TxDIFS = TxSIFS + 2 \times aSlotTime$$

这些容限由 PLME SAP 接口规范(10.4)规定，且仅适用于 SIFS 规范，因此容限不会累积。

### 9.3 PCF

PCF 提供无竞争的帧传送。PC 驻留在 AP 中，AP 能成为 PC 是可选项。所有的 STA 原本就遵从 PCF 的媒体访问规则，因为这些规则均基于 DCF，且在每个 CFP 的开始设置其 NAV。PCF 的操作特点是所有 STA 能够在 PC 操作的 BSS 中正常操作，并且如果 STA 已关联到一个点协调的 BSS，则它还能够接收 PCF 控制下发送的所有帧。对于 STA 来说，它能响应来自 PC 的无竞争轮询(CF-Poll)也是可选项。能够响应 CF-Poll 的 STA 指的是作为 CF-Pollable 可以请求被活动的 PC 轮询。CF-Pollable 的 STA 和 PC 在 CFP 内不采用 RTS/CTS。当被 PC 轮询时，CF-Pollable STA 只能发送一个可到达任何目的地（不只是 PC）的 MPDU，并且对于本次传输，还可“搭载”(piggyback)对已收到的来自 PC 的特定数据子类型帧的确认帧。如果数据帧未被确认，CF-Pollable STA 不重新发送该帧，除非它被 PC 再次轮询或它决定在 CF 期间重新发送。如果 CF 传输的接收方非 CF-Pollable，那么该接收方 STA 使用 DCF 确认规则确认，PC 仍保持对媒体的控制权。为了将帧交付到 STA，PC 可以只使用无竞争帧进行传送，而不轮询非 CF-Pollable 的 STA。

PC 在 CFP 期间对未确认帧的重传执行退避过程。当下一次特定的 AID 处于轮询表的顶端时，维护轮询表的 PC 可以重传未被确认的帧。

在 CFP 期间，PC 可以在 PIFS 时间后重传未被确认的帧。

在重叠的空间中，如果不止一个点协调的 BSS 在同一 PHY 信道内操作，那么独立的 PCF 传送活动之间极有可能发生碰撞。9.3.3.2 提出多个交叠的点协调 BSS 的共存规则。如图 73 所示，利用

## GB 15629.11—2003

该方案提供的访问优先等级，PCF 高于基于 CSMA/CA 的 DCF。活动的 PC 应位于 AP 中，这限制了 PCF 只能工作在基础结构网络中。通过将原语 MLMEStart.request 的 CF 参数集合中的参数 CFPMaDuration 设置为非 0 值，PCF 被具有 PC 能力的 AP 激活。

DCF 下发送的数据帧采用数据帧子类型——Data 或空功能。在 CFP 期间由 PC 发送的数据帧或为响应 PC 轮询而发送的数据帧将使用基于下述使用规则的合适的数据帧子类型：

- Data+CF-Poll、Data+CF-ACK+CF-Poll、CF-Poll 和 CF-ACK+CF-Poll 仅由 PC 发送；
- Data、Data+CF-ACK、空功能和 CF-ACK 由 PC 或任一 CF-Pollable STA 发送。

如果帧的子类型为 Data、Data+CF-ACK、Data+CF-Poll 或 Data+CF-ACK+CF-Poll，则接收数据类型帧的 STA 仅将帧体作为发往 LLC 的可能指示的基础。为了 CF 目的，CF-Pollable STA 将对接收的数据类型帧的所有子类型比特进行解释，但如果帧的子类型为 Data、Data+CF-ACK、Data+CF-Poll 或 Data+CF-ACK+CF-Poll，则仅检查帧体。

### 9.3.1 CFP 结构与定时

PCF 控制 CFP 期间帧的传送。如图 74 所示，当 DCF 控制帧的传送时，CFP 与 CP 交替出现。每个 CFP 从包含 DTIM 元素（后面称为 DTIM）的信标帧开始，且以给定的与下面段落规定的信标间隔同步的重复速率出现。

PC 以定义为若干个 DTIM 间隔的无竞争重复速率(CFPRate)产生 CFP。PC 由 CF 参数集合中的参数 CFPRate 来确定 CFPRate（图 74 和图 75 所示的重复间隔）。该值以 DTIM 间隔为单位，并在信标帧的 CF 参数集合元素的字段 CFPPeriod 中被通信至 BSS 中的其他 STA。CF 参数集合元素仅在信标与探测响应帧中出现，而这些帧由含活动 PC 的 STA 发送。

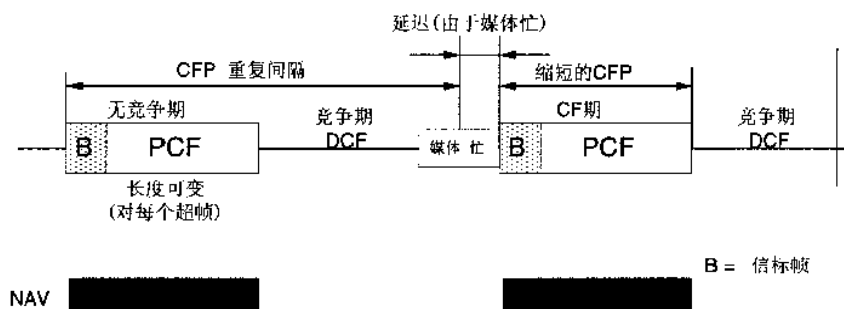


图 74 CFP/CP 交替

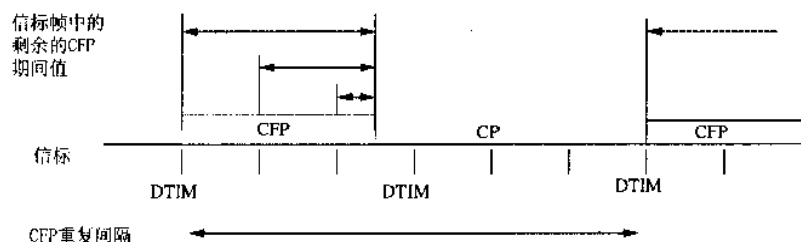


图 75 信标帧和 CFP

CFP 的长度由 PC 控制，其最大持续时间由 PC 中 CF 参数集合的参数 CFPMaDuration 规定。最大持续时间与实际持续时间（由 PC 通过子类型为 CF-End 或 CF-End+ACK 控制帧的传输来标记）均没有被限制为信标间隔的整数倍。如果 CFP 持续时间大于信标间隔，则 PC 在 CFP 期间内的适当时刻发送信标帧（由于额定时刻的通信量，所有信标帧可能存在延迟）。在 CFP 的开始时刻或在 CFP 期间，所有信标的 CF 参数集合元素均包含非 0 值的 CFPDurRemaining 字段。该值以 TU 为单位，规定了从信标传输到 CFP 结束的最大时间。在 CP 期间发送的信标中，CFPDurRemaining 字段为 0。



图 75 给出一个描述这些关系的例子,其中 CFP 为 2 倍的 DTIM 间隔,DTIM 间隔为 3 倍的信标间隔,且 CFPMaxDuration 值大约为 2.5 倍的信标间隔。

基于现有的通信量与轮询列表的大小,PC 可在 aCFPMaxDuration 前终止任何的 CFP。由于在额定的信标传输时刻媒体忙而延迟信标的传输,CFP 可根据延迟量缩短。由于 DCF 通信量而使媒体忙时,信标将延迟完成目前 DCF 帧交换所需的时间。信标传输被延迟时,CFP 开始时的信标 CFPDurRemaining 的值将规定一个在 TBTT 加上 aCFPMaxDuration 值之前结束 CFP 的时间,如图 76 所示。

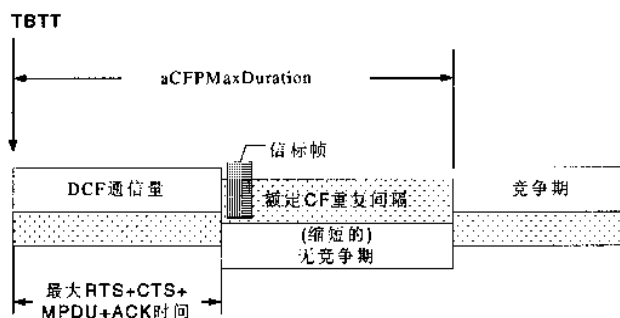


图 76 延迟的信标和缩短的 CFP 示例

### 9.3.2 PCF 访问规程

无竞争传送协议基于操作在 BSS 的 AP 中 PC 控制的轮询方案操作处。PC 在 CFP 开始就获得对媒体的控制权并试图在整个 CFP 期间维持控制权,这是通过传输之间等待比利用 DCF 访问规程的 STA 更短的时间来实现。BSS 中的所有 STA (不是 PC) 在每个 CFP 的额定开始时刻将它们 NAV 设置为 CFPMaxDuration 值,从而避免了 STA 非轮询传输导致的大多数竞争,而不论 STA 是否为 CF-Pollable。对 CFP 期间发送帧的确认通过 Data+CF-ACK、CF-ACK、Data+CF-ACK+CFP-Poll (只存在于 PC 发送的帧中) 或者 CF-ACK+CFP-Poll (只存在于 PC 发送的帧中) 帧完成,此时 Data 帧 (或 Null 帧) 紧接在被确认的帧之后,从而避免了单独的 ACK 控制帧的开销。非 CF-Pollable 或未被轮询的 CF-Pollable STA 在 CFP 期间使用 PCF 的 ACK 规程对帧进行确认。

#### 9.3.2.1 基本访问

在每个 CFP 的额定开始时刻,PC 应侦听媒体。当确认媒体在一个 PIFS 期间均为空闲时,PC 将发送一个包含 CF 参数集合元素与 DTIM 元素的信标帧。

在初始的信标帧之后,PC 将至少等待一个 SIFS 时间,然后发送下列帧之一:数据帧、CF-Poll 帧、Data+CF-Poll 帧或 CF-End 帧。如果 CFP 为空,即 PC 处没有缓存的通信量也没有要发送的轮询,将紧随初始信标帧后发送 CF-End 帧。

接收来自 PC 直接的无错帧的 STA 被期望在 SIFS 期间后,根据 9.3.3 中定义的传送进行响应。如果接收方 STA 非 CF-Pollable,接收到无错数据的响应总为一个 ACK 帧。

#### 9.3.2.2 CFP 期间的 NAV 操作

在 CFP 期间 NAV 的处理机制是使在交叠的 CFP 协调的基础结构 BSS 中的操作更加方便而设计的。关于基础结构 BSS 协调其 CFP 的机制超出本部分范围。

除带有 PC 的 STA,每个 STA 在每个目标信标传输时间 (TBTT) (见第 11 章),即 CFP 准备启动的时刻 (基于来自 PC 的信标帧的 CF 参数集合元素的 CFPeriod 字段),将其 NAV 预置为 CFPMaxDuration 值 (由来自 PC 信标帧的 CF 参数集合元素得到)。每个非 PC 的 STA 将利用接收到的信标帧的任何无错 CF 参数集合元素中的 CFPDurRemaining 更新其 NAV,这包括从其他 (重叠的) BSS 接收到的信标帧的 CF 参数集合元素中的 CFPDurRemaining 值。

## GB 15629.11—2003

上述操作防止 STA 在 CFP 期间控制媒体，这一点在 CFP 跨越多个媒体占用间隔时特别重要，例如 FH PHY 的驻留时间。隐藏的 STA 在 CFP 期间判断媒体在一个 DIFS 周期内保持空闲，从而可能会中止正在进行的传送，NAV 的这种设置减少了这种可能。

在启动任一传输之前，加入利用 PC 操作的 BSS 内的 STA 将根据接收到的任何信标或探测响应帧的 CF 参数集合的元素 CFPDutRemaining 的信息来更新 NAV。

在每个 CFP 结束时，PC 将发送 CF-End 或 CF-End+ACK 帧，一旦 STA 接收到来自任一 BSS 的这两种帧任一种，则复位其 NAV。

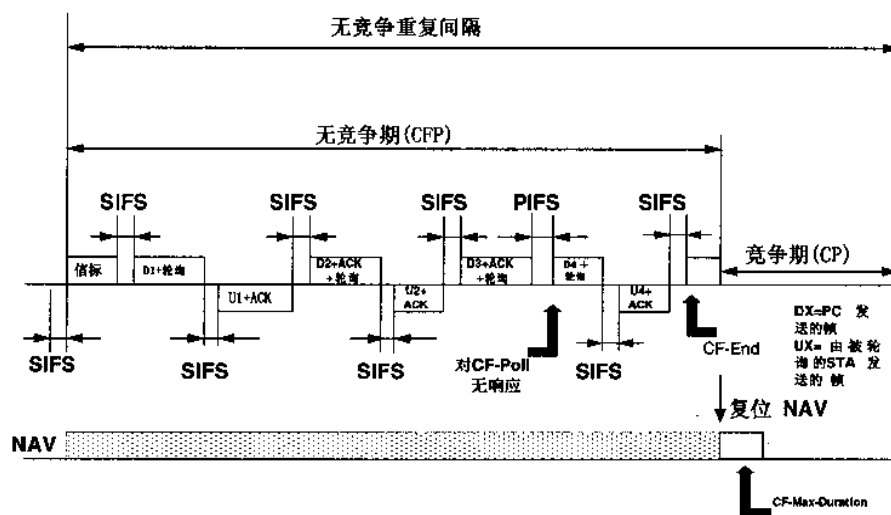


图 77 PCF 帧传送示例

## 9.3.3 PCF 传送规程

在 PCF 下，帧的传送典型包括：一种是由 AP 或 PC 发出的，另一种是发往 AP 或 PC 的。在 CFP 期间，这些传输的顺序以及在任意给定时刻点允许哪个 STA 向 PC 发送帧，都由 PC 控制。图 77 描述了典型的 CFP 期间的帧传送。帧传送规则详见下列各条。

具有 FH PHY 的 STA 在驻留时间边界将失去对信道的控制，因此它要求当前 MPDU 的传输和随后 MPDU 的确认均应在驻留时间边界前发送。当 STA 被 PC 轮询后，如果没有足够的驻留时间以允许 MPDU 与确认帧的传输，STA 将推迟 MPDU 的传输而发送一个空帧或 CF-ACK 帧。该 MSDU 的短重传计数和长重传计数均不受影响。

MaxMPDUTime 定义为发送最大长度的 MAC 帧所需的时间，同时再加上发送 PHY 前导码、头、尾及扩展位的时间。在具有 FH PHY 的 STA 中，如果在驻留边界前没有足够的时间使得 STA 对空帧或 CF-ACK 帧进行响应，则 PC 不会向 STA 发送 CF-Poll 帧。

## 9.3.3.1 当 PCF STA 为发送方或接收方时的 PCF 传送

PC 在启动 CFP 的信标帧与 CF-End 之间利用 SIFS 发送帧，除非 PC 希望另一个 STA 传输，或者在 SIFS 期间没有接收到期望的传输。在这些情况下，一旦在其最后传输之后经过了一个 PIFS 周期，PC 就可发送它的下一个已经挂起的传输，这允许 PC 在存在 BSS 交叠时保持对媒体的控制。PC 向 CF-Pollable STA 发送下述任一类型的帧：

- Data，当目的接收方未被轮询且没有先前的帧等待确认时，用于发送来自 PC 的数据；
- Data+CF-ACK，当目的接收方未被轮询且 PC 需要对本次传输前一个 SIFS 时间内接收的来自 CF-Pollable STA 的帧进行确认时，用于发送来自 PC 的数据；
- Data+CF-Poll，当目的接收方为 CFP 期间下一个被允许发送的 STA，且没有先前发送的帧等待确认时，用于发送来自 PC 的数据；

- Data+CF-ACK+CF-Poll, 当目的接收方为在 CFP 期间下一个被允许发送的 STA, 且 PC 需要对本次传输前一个 SIFS 时间内接收的来自 CF-Pollable STA 的帧进行确认时, 用于发送来自 PC 的数据;
- CF-Poll, 当 PC 没有向目的接收方发送数据, 但目的接收方是 CFP 期间下一个被允许发送的 STA, 且没有先前的帧等待确认时使用;
- CF-ACK+CF-Poll, 当 PC 没有正向目的接收方发送数据, 但目的接收方是 CFP 期间下一个被允许发送的 STA, 且 PC 需要对本次传输前一个 SIFS 时间接收的来自 CF-Pollable STA 的帧进行确认时使用;
- CF-ACK, 当 PC 没有向目的接收方发送数据或进行轮询, 但 PC 需要对本次传输前一个 SIFS 时间接收的来自 CF-Pollable STA 的帧进行确认时 (当 PC 下一次传输为管理帧, 例如信标帧时有用) 使用;
- 任何一个适合 AP 按照该类型帧的规则发送的管理帧。

PC 在 CFP 期间发送数据帧或管理帧到非 CF-Pollable、非节能模式的 STA, 这些 STA 应利用 SIFS 后的 ACK 帧对接收进行确认。PC 还可以在 CFP 期间发送广播或组播帧。由于启动 CFP 的信标帧包含 DTIM 元素, 如果有已关联的 STA 采用节能模式, 则缓存的广播和组播帧将在任何一个包含 TIM 元素的信标帧后立即发送, 其中 DTIM 计数字段值为 0。

CF-Pollable STA 如果接收了包括 CF-Poll 帧在内的任意子类型的定向数据帧, 则可在接收到 CF-Poll 帧后的一个 SIFS 期间内发送一个数据帧。在对 CF-Poll 进行响应时, CF-Pollable STA 忽略但不复位其 NAV。

在 CFP 期间接收了定向帧的非 CF-Pollable STA 将发送 ACK, 但不复位其 NAV。

对于需要 MAC 级确认的帧, 接收到 CF-Poll (任意类型) 的 CF-Pollable 的 STA 将利用 Data+CF-ACK 子类型帧响应 CF-Poll。例如, 在图 77 中, U1 帧包含对前面 D1 帧的确认, D2 帧包含对前面 U1 帧的确认。PC 利用子类型 CF-ACK 对接收到的帧进行确认, 即使利用子类型 CF-ACK 发送的数据帧寻址到另一个不被确认的 STA。期望得到确认的 CF-Pollable STA 在向 PC 进行传输后的 SIFS 时间后解释 PC 发送的帧的子类型。如果非 CF-Pollable STA 接收到需要 MAC 级确认的帧, 则该 STA 将不解释 CF-Poll 指示, 并将在一个 SIFS 期间后发送 ACK 控制帧确认该帧。

帧的长度是可变的, 长度只由用于 BSS 的帧和 (或) 分段长度限制进行界定。如果 CF-Pollable STA 在紧接 PC 传输的 SIFS 期间内未对 CF-Poll 帧 (任一类型) 作出响应, 或者非 CF-Pollable STA 在紧接着 PC 传输需要确认的帧之后的 SIFS 期间内未返回 ACK 帧, 则 PC 将继续控制信道, 并在 PC 上次传输结束后的 PIFS 期间段内发送下一帧。

CF-Pollable STA 总要对直接发往其 MAC 地址的、且无错接收的 CF-Poll 作出响应。如果 STA 被轮询时没有帧要发送, 则响应就为一个空帧。如果 STA 被轮询时没有帧要发送, 但需要对传送的 CF-Poll 帧确认, 则响应为一个 CF-ACK (无数据) 帧。要求空响应可以将 “无通信量” 状态同重叠 PC 之间的碰撞区分开来。

当从启动 CFP 的信标帧开始的 CFPD<sub>ur</sub>Remaining 时间期满, 或者当 PC 没有要发送的帧且无 STA 需被轮询时, CFP 将结束。不论哪种情况, CFP 的终止均通过 PC 传输 CF-End 来标记。如果在 CF-End 即将被发送时接收到需要确认的帧, 则 PC 将转而发送 CF-End+ACK 帧。BSS 中所有接收到 CF-End 或 CF-End+ACK 的 STA 将复位它们的 NAV, 以便它们在 CP 期间可以试图发送。

### 9.3.3.2 在交叠的点协调 BSS 内的操作

因为 PCF 的操作没有利用 CSMA/CA 竞争窗口的随机化和 DCF 的退避, 因此如果多个重叠的点协调 BSS 操作在同一 PHY 信道, 且它们的 CFP 速率和信标间隔大致相同时, 存在重复碰撞的可能。为了减少由于 CF 碰撞而造成的有效帧的丢失, 当初始信标帧由于媒体忙而推迟时, PC 将使用 DIFS 和随机退避延迟 (CW 在 1 到 aCW<sub>min</sub> 之间) 来启动 CFP。在 CFP 期间内, 在对未确认的定

## GB 15629.11—2003

向数据或管理帧重发之前，PC 可选择性地使用这种退避。

为了进一步降低 PC 间碰撞的概率，在 CFP 期间的每个 aMediumOccupancyLimit TU 内，PC 要求媒体在 DIFS 加上随机数（从 1 到 aCWmin 之间）个时隙内被确认为空闲，而这将导致重叠的 BSS 或隐藏 STA 的通信量失去对媒体的控制，因为 BSS 内的 STA 被禁止通过将它们的 NAV 设置成 CFPMaxDuration 或 CFPDurRemaining 来发送。对于与 FH PHY 协作的 PCF 操作，aMediumOccupancyLimit 将设置为等于驻留时间。对于与其他 PHY 类型协作的操作，aMediumOccupancyLimit 设置为等于 CFPMaxDuration，除非需要其他的防止 PCF 碰撞的保护。aMediumOccupancyLimit 也可用于满足频谱使用规则中强制性限制单个 STA 连续传输时间的接收过程。

### 9.3.3.3 CFPMaxDuration 限制

CFPMaxDuration 的值应受一定的限制，以允许竞争通信量和无竞争通信量共存。

CFPMaxDuration 的最小值是 2 倍的 MaxMPDUTime 与发送初始信标帧和 CFP 的 CF-End 帧所需时间的和，这可以保证当 AP 对 STA 进行轮询时，有充足的时间发送一个数据帧到 STA，同时对于被轮询的 STA，也有时间用一个数据帧进行响应。

CFPMaxDuration 的最大值为  $(\text{BeaconPeriod} \times \text{DTIMPeriod} \times \text{CFPRate}) - [\text{MaxMPDUTime} + (2 \times \text{aSIFSTime}) + (2 \times \text{aSlotTime}) + (8 \times \text{ACKSize})]$ ，单位为微秒，此时竞争窗口为 aCWmin。其中 MaxMPDUTime 为发送最大长度的 MAC 帧所需的时间加上发送 PHY 前导码、头、尾及可能的扩展比特所需的时间，这允许足够的时间在 CP 期间最少发送一个数据帧。

### 9.3.3.4 无竞争使用规则

PC 可向任一活动的 STA 和处于节能模式的 CF-Pollable STA 发送广播或组播帧以及定向数据帧或管理帧。在 CFP 期间，CF-Pollable STA 在 SIFS 期间后，利用 Data+CF-ACK 或 CF-ACK（无数据）帧对接收到的每个 Data+CF-Poll 帧或者 Data+CF-ACK+CF-Poll 帧确认，或者利用数据或空（无数据）帧确认每个接收到的 CF-Poll（无数据）帧，或者利用 ACK 控制帧确认接收到的其他所有的数据和管理帧。非 CF-Pollable STA 利用 SIFS 期间后发送的 ACK 控制帧对接收的数据与管理帧进行确认。非 CF-Pollable STA 的操作与 DCF 机制下 STA 采用的操作完全相同。

当被 PCF 轮询（Data+CF-Poll、Data+CF-ACK+CF-Poll、CF-Poll 或 CF-ACK+CF-Poll）时，CF-Pollable STA 发送数据帧至任意目的地。直接发往 STA 或通过 PC 的帧，都由 PC 在 SIFS 后发送 CF-ACK 指示（Data+CF-ACK、Data+CF-ACK+CF-Poll、CF-ACK、CF-ACK+CF-Poll 或 CF-End+ACK）来确认。直接发往非 CF-Pollable STA 的帧将通过 SIFS 后发送的 ACK 控制帧加以确认。如果 CF-Pollable STA 被轮询，但它既没有数据帧也没有确认帧要发送时，STA 将在 SIFS 后发送空帧作为响应。如果被轮询的 CF-Pollable STA 在 CFP 结束之前没有充分的时间来发送 MPDU 队列并接收其确认，或者受到当前媒体被占用的限制，则在 SIFS 后发送一个空帧作为响应；如果采用 Data+CF-Poll 或 Data+CF-ACK+CF-Poll 轮询，则发送 CF-ACK 帧作为响应。CF-Pollable STA 可在其响应帧中对多数据比特位进行设置，以允许 PC 将空 STA 队列和由于没有足够时间来传送 MPDU 的响应区分开来。

如果当前 CFP 中没有足够的时间使被轮询的 STA 能发送包含最小长度 MPDU 的数据帧，则 PC 将不发布包括 CF-Poll 的子类型的帧。

### 9.3.4 无竞争轮询列表

如果 PC 支持将 CFP 用于内部帧的传送与帧的交付，则 PC 应维持一个“轮询列表”以选择在 CFP 期间能够合法接收 CF-Poll 帧的 STA。轮询列表的功能特性规定如下。如果 PC 仅仅为帧的交付支持 CFP 的使用，则 PC 不需要轮询列表，并且不会产生包括 CF-Poll 帧的子类型数据帧。PC 提供的无竞争支持的形式在 AP 发出的信标帧、关联响应帧、重新关联响应帧以及探测响应管理帧的能力信息字段标识。如同在非基础结构网络中，由 STA 发出的帧总是将这些比特设置为 0。

轮询列表用于强制性对 CF-Pollable STA 进行轮询, 而不论 PC 是否有挂起的要发送给这些 STA 的通信量。轮询列表用于控制 Data+CF-Poll 和 Data+CF-ACK+CF-Poll 类型帧的使用, PC 使用这些类型帧向 CF-Pollable STA 发送数据帧。轮询列表是一种逻辑结构, 不会暴露在 PC 的外部。轮询列表维护技术的最低要求是: 在由拥有活动的 PC 的任意接入点控制的 BSS 内能保证任意 CF-Pollable STA 之间的互操作性。AP 还可以实现其他的轮询列表维护技术, 这已超出本部分的范围。

#### 9.3.4.1 轮询列表处理

当轮询列表有若干项时, 在每个 CFP 期间 PC 应至少向一个 STA 发送 CF-Poll 帧。在每个 CFP 期间, PC 按照 AID 值递增的顺序依次向轮询列表中的 STA 子集发布轮询。

在 CFP 时间内, 如果所有的 CF 帧已被交付, 且轮询列表中的所有 STA 都已被轮询, 则 PC 可以产生一个或多个 CF-Poll 帧, 并发往轮询列表中的任何 STA。在 CFP 时间内, 如果所有的 CF 帧已被交付, 且轮询列表中的所有 STA 已被轮询, 则 PC 也可以向任何 STA 发送数据或管理帧。

为了从 CFP 中获得最大效率, 也为了在相反方向上的后续数据帧中能够搭载确认, 当在 CFP 期间有充足的时间可以对 CF-Poll 帧响应时, PC 通常将 Data+CF-Poll 和 Data+CF-ACK+CF-Poll 类型用于每个发送的数据帧。

#### 9.3.4.2 轮询列表的更新规程

STA 利用关联请求帧和重新关联请求帧的能力信息字段的 CF-Pollable 子字段来指示它的 CF\_Pollability。如果一个 STA 想改变 PC 的 CF-Pollability 记录, 则 STA 执行重新关联。在关联期间, CF-Pollable STA 也可以请求被列入轮询列表中, 或通过设置能力信息字段的 CF-Poll 请求子字段来实现。如果 CF-Pollable STA 始终不愿被列入轮询列表中, 则该 STA 在执行关联时, 将 CF-Pollable 子字段设置为假, CF-Poll 请求子字段设置为真。对正常使用节能模式的 CF-Pollable STA 而言, 不被轮询是很有用的, 这样可以允许它们在 CFP 期间接收缓存通信量(它们在接收启动 CFP 的 DTIM 时必须保持清醒), 而在它们没有通信量需要发送时无需为了接收 CF-Poll 帧而保持清醒。如果 STA 需要从轮询列表中被移去, 则该 STA 执行重新关联过程。

如果 CF-Pollable STA 不在轮询列表中, 但是在其最近关联期间没有要求不被轮询, 则 PC 可能将 STA 动态地放置在轮询列表中, 以处理该 STA 突发式的帧传送活动。

### 9.4 分段

MAC 对定向 MSDU 或 MMPDU 分段和重组, 分段和重组机制允许分段重传。

除了最后的一个分段可能比较小外, 其他所有 MPDU 分段的八位位组数相同。除了 MSDU 或 MMPDU 的最后一个分段, 其长度可以是偶数也可以为奇数八位位组, 其他 MPDU 分段的长度为偶数八位位组。分段的长度不应大于分段阈值(aFragmentationThreshold)。

在数据被发送前, 分段的八位位组数由 aFragmentationThreshold 和首次构造分段时分配给一个分段的 MPDU 八位位组数共同确定。一旦分段被首次发送, 其帧体的内容和长度就固定不变, 直到它被成功地交付到直接接收方 STA 为止。STA 能够接收任意长度的分段。

如果分段需要重传, 其帧体内容和长度在该 STA 的 MSDU 或 MMPDU 的生存时间内保持不变。一旦分段被发送, 该分段的内容和长度不允许波动以适应驻留时间边界。每个分段包含由序列号和分段号组成的序列控制字段。当 STA 发送 MSDU 或 MMPDU 时, 该 MSDU 或 MMPDU 的所有分段的序列号都保持相同。分段按照分段号由低至高的顺序进行发送, 分段号从 0 开始, 后续分段号依次按 1 递增。帧控制字段还包含一个比特, 即多分段比特, 该比特为 0 时, 表示它是 MSDU 或 MMPDU 的最后一个分段(或惟一分段)。

源 STA 为每个正被发送的 MSDU 维护一个发送 MSDU 定时器, 属性 MaxTransmitMSDULifeTime 规定了允许发送一个 MSDU 的最大时间量。该定时器从试图发送 MSDU 的第一个分段开始计时。若计时超出 aMaxTransmitMSDULifeTime, 则剩余的所有分段被源 STA 丢弃, 并且也不再尝试完成该 MSDU 的发送。

## GB 15629.11—2003

## 9.5 重组

每个分段包含支持从它的组成分段重组为完整的 MSDU 或 MMPDU 的信息。为了目的 STA 对 MSDU 或 MMPDU 进行重组，每个分段的头包含下述信息：

- 帧类型；
- 发送方的地址，从地址 2 字段中得到；
- 目的地址；
- 序列控制字段：该字段允许目的 STA 检验所有接收到的属于同一 MSDU 或 MMPDU 的分段，并且检验用于分段重组的序号；序列控制字段中的序列号对同一 MSDU 或 MMPDU 的所有分段保持相同，而序列控制字段中的分段号对每个分段依次加 1；
- 多分段指示符：向目的 STA 指示本分段不是 MSDU 或 MMPDU 的最后一个分段。只有 MSDU 或 MMPDU 的最后一个分段或惟一分段才将该比特设置为 0，而 MSDU 或 MMPDU 的所有其他分段将该比特设置为 1。

目的 STA 应按照序列控制字段的分段号字段的顺序合并分段重建 MSDU 或 MMPDU。如果还未接收到多分段比特为 0 的分段，则目的 STA 知道 MSDU 或 MMPDU 还没有结束。一旦 STA 接收到多分段比特为 0 的分段，则该 STA 知道该 MSDU 或 MMPDU 不再需要接收更多分段。所有 STA 应支持同时接收至少三个 MSDU 或 MMPDU 分段。注：同时接收超过三个以上的 MSDU 或 MMPDU 分段将显著增加 STA 丢弃帧的数量。

目的 STA 应为每个正被接收的 MSDU 或 MMPDU 维护一个接收定时器，最少可以有三个 MSDU 或 MMPDU。STA 可以使用更多的定时器以能够同时接收更多的 MSDU 或 MMPDU。当 MSDU 或 MMPDU 定时器没有被维护时，正在接收的 STA 将丢弃作为该 MSDU 或 MMPDU 的部分分段。另外，还有一个属性 aMaxReceiveLifeTime 规定了接收一个 MSDU 所允许的最长时间。接收 MSDU 或 MMPDU 定时器从 MSDU 或 MMPDU 的第一个分段接收起开始，如果接收定时器超出 aMaxReceiveLifeTime，则目的 STA 将丢弃所有已接收到的该 MSDU 或 MMPDU 的分段。在超出 aMaxReceiveLifeTime 之后，如果接收到定向的 MSDU 或 MMPDU 的另外的分段，这些分段应被确认并丢弃。

为正确地将 MPDU 重组为 MSDU 或 MMPDU，目的 STA 应丢弃接收到的重复分段，STA 应如 9.2.9 描述的丢弃重复分段。然而，为了响应定向 MSDU 的重复的分段，应发送确认帧。

## 9.6 多速率支持

某些 PHY 具有多数据传送速率能力，为了提高性能，允许动态速率切换。执行速率切换的算法超出了本部分的范围，但是为了确保具有多速率能力的 PHY 之间能够共存和互操作性，本部分定义了一组所有 STA 应遵循的规则。

所有控制帧应以 BSS 基本速率集中的一种速率发送，以使它们能被 BSS 中的所有 STA 理解。

所有组播和广播 RA 的帧应以 BSS 基本速率集中的一种速率发送，无论它们属于何种类型或子类型。

如果带有一个单播 RA 的数据类型和管理类型 MPDU，应以速率切换机制选择的任一种支持的数据速率发送（其输出为一个内部 MAC 变量，称为 MACCurrentRate，该速率用于计算每帧的持续时间/ID 字段）。STA 不应以目的 STA 不支持的速率发送，它在管理帧的支持速率元素中有报告。对于 Data+CF-ACK、Data+CF-Poll+CF-ACK 及 CF-Poll+CF-ACK 类型的帧，选定的用于发送帧的速率必须被接收方 STA 和 ACK 的目的方 STA 支持。

在任何情况下 STA 都不能以高于操作 OperationRateSet 中的最高速率启动数据或管理帧的发送，OperationRateSet 是原语 MLME\_JOIN.request 的一个参数。

为了允许发送的 STA 计算持续时间/ID 字段的内容，响应方 STA 应以与在帧交换序列（如 9.7 中的定义）中最近的帧相同的速率，如果该速率属于 PHY 必备速率，或属于 BSS 基本速率集中

的 PHY 速率的最大可能速率，发送控制响应(CTS 或 ACK)。

### 9.7 帧交换序列

允许的帧交换序列由表 20 和表 21 总结给出，适用于两个表的说明见两表后的表注。

该序列中的每个独立帧均由 SIFS 隔开。

表 20 帧序列

序 列	序列中的帧数	用 途
Data (bc/mc)	1	广播或组播 MSDU
Mgmt (bc)	1	广播 MMPDU
{ RTS-CTS- } [Frag-ACK-] Last-ACK	2	定向 MSDU 或 MMPDU
PS-Poll-ACK	2	缓发的 PS-Poll 响应
PS-Poll-[Frag-ACK-] Last-ACK	3	立即的 PS-Poll 响应
DTIM(CF)-[≤CF-Sequence>-] {CF-End}	2 或更多	CFP 的开始
[<CF-Sequence>-] {CF-End}	2 或更多	在丢失 ACK 或媒体占用边界之后 CFP 继续

注 1: [ ] 内的项在序列中可以不出现或多次出现。  
 注 2: { } 内的项在序列中可以不出现或只出现一次。  
 注 3: 隔离号 “-” 代表帧间的 SIFS 时间间隔。  
 注 4: “Data(bc/mc)” 代表地址 1 字段中为广播或组播地址的任何类型数据帧。  
 注 5: “Mgmt(bc)” 代表 DA 字段中为广播地址的任何管理类型帧。  
 注 6: “RTS” 代表子类型为 RTS 的控制帧。  
 注 7: “CTS” 代表了类型为 CTS 的控制帧。  
 注 8: “ACK” 代表了类型为 ACK 的控制帧。  
 注 9: “Frag” 代表地址 1 字段中为独立地址的数据类型 MPDU 或管理类型 MMPDU，其多分段字段设置为 1。  
 注 10: “Last” 代表地址 1 字段中为独立地址的数据类型 MPDU 或管理类型 MMPDU，其多分段字段设置为 0。  
 注 11: “PS-Poll” 代表子类型为 PS-Poll 的控制帧。  
 注 12: “DTIM(CF)” 代表子类型为信标的管理帧，它包含一个 DTIM 信息元素，且该信息元素的参数集合元素中的 CFPDURRemaining 字段值为非零。  
 注 13: “CF-End” 代表 CF-End 或 CF-End+ACK (若<CF-Sequence>之前的最后一个帧是需要 AP 确认的管理帧或数据帧) 类型的控制帧。

表 21 CF 帧序列

CF 帧序列	序列中的帧数	用 途
Beacon (CF)	1	CFP 期间的信标
Data (bc/mc)	1	广播或组播 MSDU
Mgmt(bc)	1 或 2	广播 MMPDU
Mgmt(dir)-ACK	2 或 3	定向 MMPDU
Data(dir)+CF-Poll {+CF-ACK} - Data(dir)+CF-ACK- {CF-ACK(无数据)}	2	与 MPDU 一起发送的 Poll 与 ACK
Data(dir)+CF-Poll {+CF-ACK} -CF-ACK(无数据)	2	对带有空队列的 STA 进行轮询，没有足够的时间发送队列中的 MPDU，或在驻留时间或媒体占用边界之前所剩时间不足以发送一个排队帧
CF-Poll(无数据) {+CF-ACK} -Data(dir)- {CF-ACK(无数据)}	2	分别轮询，与 MPDU 一起发送的 ACK
CF-Poll(无数据) {+CF-ACK} -Data(dir)-ACK	3	被轮询的 STA 发送给 BSS 中的 STA

表 21 CF 帧序列 (续)

CF-Poll(无数据) {+CF-ACK} -Null(无数据)	2	分别轮询、STA 队列空或者没有足够的时间发送队列中的 MPDU, 或者在驻留时间或媒体占用边界之前所剩时间不足以发送一个排队帧
Data(dir) {+CF-ACK} -ACK	2	若非 CF-Pollable 或未被轮询, 则发送 ACK

注 1: “Beacon(CF)”代表子类型为信标的管理帧, 且它的 CF 参数集合元素的 CFPDURRemaining 字段的值非 0。  
 注 2: “Data(dir)”代表地址 1 字段中为独立地址的数据类型 MPDU。  
 注 3: “Mgmt(dir)”代表地址 1 字段中为独立地址的管理类型 MMPDU。  
 注 4: “CF-ACK (无数据)”代表子类型为 CF-ACK (无数据)的数据帧。  
 注 5: “CF-Poll (无数据)”代表子类型为 CF-Poll (无数据)的数据帧。  
 注 6: “Null (无数据)”代表子类型为无操作 (无数据)的数据帧。  
 注 7: “{+CF-ACK}”指示帧可以包含或不包含无竞争确认。  
 注 8: “+CF-ACK”指示帧包含无竞争确认。  
 注 9: “+CF-Poll”指示帧包含无竞争轮询。  
 注 10: <CF-Sequence> 代表在 CFP 期间发送的一个或多个帧的序列。一个有效的 <CF-Sequence> 由表 21 中的一个帧序列组成。对应于[<CF-Sequence>]的帧交换序列集合在 CFP 期间以任意顺序出现。  
 注 11: 表 20 中的注也适用于本表。

### 9.8 MSDU 传输限制

为了避免在 LLC 实体对之间对 MSDU 重新排序和/或不必要地丢弃 MSDU, 对于能同时处理多个未完成的 MSDU 发送的任何 STA, 必须遵守下述规则。在此, “未完成”是指在某个特定时刻适合被发送的 MSDU 或 MMPDU。在下面条件的限制下, STA 可以同时拥有任意数目 (大于或等于 1) 未完成的合适的 MSDU。

STA 保证在某一时刻从特定 SA 到另一个特定的单独 RA 的 MSDU 或 MMPDU 中最多只有一个特殊的。(简单的说, 限制条件就是: 在某一时刻到特定的单独 RA 的 MSDU 中最多只有一个特殊的。)

对于可选的严格排序服务等级已经被实现的 STA, 应确保不存在具有严格排序服务等级的具有组地址 (多目的) 的 MSDU, 而这些 MSDU 来自任何其他特殊 MSDU (定向的或具有组地址的) 的 SA。这是由于具有组地址的 MSDU 会被寻址到包含任一独立 RA 的对等 STA 的集合中。

建议 STA 在选择 aMaxMSDUTransmitLifeTime 的值时, 要使其足够大, 以使在正常的操作环境下不会由于超出发送 MSDU 定时而丢弃 MSDU。

## 10 层管理

### 10.1 管理模型综述

MAC 层和 PHY 层在概念上包括管理实体, 分别被称为 MAC 子层管理实体 (MLME) 和 PHY 层管理实体 (PLME)。这些实体提供层管理服务接口, 通过这些接口, 可以调用层管理功能。

为了提供正确的 MAC 操作, 站管理实体 (SME) 应存在于每个 STA 中。SME 是与层无关的实体, 可被看作存在于一个独立的管理面中或存在于 “层一侧之外” (off to the side)。SME 的确切功能在本部分中没有规定, 但是该实体通常可被视为负责从不同层管理实体上收集依赖于层的状态, 并类似地设置层特定参数的值。SME 以通用系统管理实体的名义典型地执行这些功能, 并实现标准管理协议。图 11 描绘了管理实体之间的关系。

该模型中的各种实体以各种方式进行交互。借助一个服务访问点 (SAP), 某些交互在本部分中有明确的定义, 定义的原语通过 SAP 进行交换。经由交换已定义的原语的服务访问点 (SAP) 显式地定义。其他交互在本部分中没有显式地定义, 例如 MAC 和 MLME 之间以及 PLCP 和 PLME 之间的接



口，在图 78 内描述为双箭头。这些将 MAC 和 PHY 管理实体集成到整个 MAC 和 PHY 层中的方式未在本部分中规定。

该模型内的管理 SAP 如下：

- SME-MLME SAP
- SME-PLME SAP
- MLME-PLME SAP

后两种 SAP 支持相同的原语，实际上可视为单个 SAP（称为 PLME SAP），它既可以被 MLME 也可以被 SME 直接使用。在这种方式下，该模型反映了所期望的是一种通用的实现途径，其中 PLME 功能受 MLME（以 SME 的名义）控制。特别是不要求 PHY 的实现具有与它们与 MAC 和 MLME 的接口不同的独立接口。

## 10.2 通用管理原语

每层的特定管理信息由该层的管理信息库(MIB)描述。MAC 和 PHY 层管理实体被视为“包含”该层的 MIB。通过管理 SAP 交换的与 MIB 相关的管理原语的通用模型，允许 SAP 用户实体获取(GET)或设置(SET)MIB 属性值。对原语 SET.request 的引用要求该层实体执行特定的规定动作。

图 78 描述了这些通用原语。

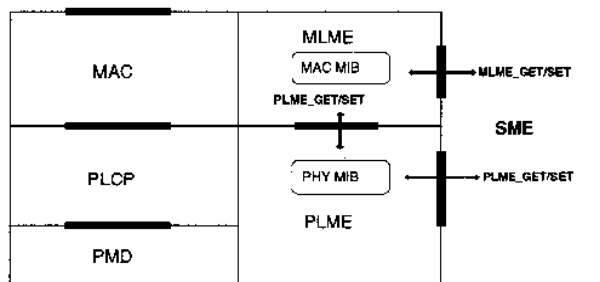


图 78 GET 和 SET 操作

原语 GET 和原语 SET 分别由原语 REQUEST 和相关的原语 CONFIRM 描述。这些原语的前缀为 MLME 或 PLME，取决于涉及到的是 MAC 或 PHY 层管理 SAP。在以下描述中，XX 表示 MLME 或 PLME：

**XX-GET.request(MIBAttribute)**

请求给定的 MIB 属性值。

**XX-GET.confirm(status, MIBAttribute, MIBAttributevalue)**

如果 status="success"，返回适当的 MIB 属性值；否则在状态字段(status)返回一个错误指示。可能的错误状态值包括“无效的 MIB 属性”和“试图获取只写的 MIB 属性”。

**XX-SET.request(MIBAttribute, MIBAttributevalue)**

请求指示的 MIB 属性设置为给定值，如果该 MIB 属性隐含着特定动作，则该原语请求执行该动作。

**XX-SET.confirm(status, MIBAttribute)**

如果 status="success"，该原语证实指定的 MIB 属性已被设置为请求值，否则状态字段 status 返回错误状态。如果 MIBAttribute 隐含着特定动作，则该原语证实该动作已被执行。可能的错误状态值包括“无效的 MIB 属性”和“试图设置只读的 MIB 属性”。

此外，还有某些请求（和相关的证实）能通过给定的 SAP 调用，但并不涉及设置或获取特定的 MIB 属性。每个 SAP 支持的请求如下所示：

- XX-RESET.request：其中 XX 为相关的 MLME 或 PLME
- XX-RESET.confirm

该服务用于初始化管理实体、MIB 及数据通道实体，它可包括一系列被初始化为非默认值的属

## GB 15629.11—2003

性，对应的.confirm 原语指示请求的成功或失败。

其他特定 SAP 原语在 10.3 示出。

## 10.3 MLME SAP 接口

本条规定由 MLME 为 SME 提供的服务。这些服务以抽象的方式描述，因此并不意味任何特定实现或外露接口。MLME SAP 具有通用的原语格式，即原语 ACTION.request 之后紧跟原语 ACTION.confirm。SME 通过 MLME SAP 使用 MLME 提供的服务。

## 10.3.1 功率管理

该机制支持 STA 功率管理模式的建立和维护。

## 10.3.1.1 MLME-POWERMGT.request

## 10.3.1.1.1 功能

该原语请求改变功率管理模式。

## 10.3.1.1.2 服务原语的语义

原语参数如下：

MLME-POWERMGT.request (

PowerManagementMode,

WakeUp,

ReceiveDTIMs

)

名 称	类 型	有效范围	描 述
PowerManagementMode (功率管理模式)	枚举型	ACTIVE POWER_SAVE	描述 STA 期望的功率管理模式的枚举类型
WakeUp (唤醒)	布尔型	真, 假	当值为真时, MAC 被强制立即进入唤醒状态。如果当前功率管理模式为 ACTIVE, 该参数无效
ReceiveDTIMs (接收) DTIM	布尔型	真, 假	值为真时, 该参数唤醒 STA 以接收所有 DTIM 帧; 当值为假时, 对每个 DTIM 帧 STA 不需要被唤醒

## 10.3.1.1.3 产生条件

该原语由 SME 产生，以实施某一实现的节能策略。

## 10.3.1.1.4 收后效果

该请求设置 STA 的功率管理参数。随后 MLME 发布原语 MLME-POWERMGT.confirm 来反映功率管理改变请求的结果。

## 10.3.1.2 MLME-POWERMGT.confirm

## 10.3.1.2.1 功能

该原语确认功率管理模式的改变。

## 10.3.1.2.2 服务原语的语义

原语参数如下：

MLME-POWERMGT.confirm (

ResultCode

)

名 称	类 型	有效范围	描 述
ResultCode	枚举型	SUCCESS INVALID_PARAMETERS NOT_SUPPORTED	指示原语 MLME-POWERMGT.request 的结果

## 10.3.1.2.3 产生条件

该原语是原语 MLME-POWERMGT.request 产生的结果，该原语由 MLME 产生以建立新的功率

管理模式。直到功率管理模式改变完成后才产生该原语。

#### 10.3.1.2.4 收后效果

SME 被通告功率管理模式发生改变。

#### 10.3.2 扫描

该机制支持决定可用 BSS 的特性的过程。

##### 10.3.2.1 MLME-SCAN.request

###### 10.3.2.1.1 功能

该原语请求调查 STA 随后可以尝试加入的潜在的 BSS。

###### 10.3.2.1.2 服务原语的语义

原语参数如下：

```
MLME-SCAN.request (
    BSSType,
    BSSID,
    SSID,
    ScanType,
    ProbeDelay,
    ChannelList,
    MinChannelTime,
    MaxChannelTime
)
```

名 称	类 型	有效范围	描 述
BSSType (BSS 类型)	枚举型	INFRASTRUCTURE INDEPENDENT ANY_BSS	确定扫描过程包括基础结构 BSS 还是独立 BSS，或两者兼而有之
BSSID	MAC 地址	任何有效的单 MAC 地址 或广播 MAC 地址	识别一个特定的或广播 BSSID
SSID	八位位组 串	0~32 八位位组	规定期望的 SSID 或广播 SSID
ScanType (扫描类型)	枚举型	ACTIVE PASSIVE	指示主动或被动扫描
ProbeDelay (探测延迟)	整数型	N/A	在主动扫描期间，发送探测帧之前所用的延迟（单位为 μs）
ChannelList (信道列表)	有序的 整数集	从有效信道范围内选择 每个信道用于适当的 PHY 和载波设置	规定扫描 BSS 时被检查的信道列表
MinChannelTime (最小信道时间)	整数型	≥ProbeDelay	扫描每一信道所用的最小时间 (单位为 TU)
MaxChannelTime (最大信道时间)	整数型	≥MinChannelTime	扫描每一信道所用的最大时间 (单位为 TU)

###### 10.3.2.1.3 产生条件

该原语由 SME 产生，以使 STA 确定是否有其他的 BSS 可以加入。

###### 10.3.2.1.4 收后效果

当前帧交换序列完成时，该原语启动扫描过程。

## GB 15629.11—2003

## 10.3.2.2 MLME-SCAN.confirm

## 10.3.2.2.1 功能

该原语返回对在扫描过程中检测到的 BSS 集合的描述。

## 10.3.2.2.2 服务原语的语义

原语参数如下：

MLME-SCAN.confirm (   
 BSSDescriptionSet,   
 ResultCode   
 )

名 称	类 型	有效范围	描 述
BSSDescriptionSet (BSS 描述集合)	BSSDescription 集合	N/A	返回 BSSDescriptionSet 以指示扫描请求的结果。该值是一个包括零个或多个 BSSDescription 实例的集合
ResultCode (返回值)	枚举	SUCCESS INVALID_ PARAMETERS	指示原语 MLME-SCAN.confirm 的结果

每一个 BSSDescription 包括下列元素：

名 称	类 型	有效范围	描 述
BSSID	MAC 地址	N/A	已发现的 BSS 的 BSSID
SSID	八位位组串	1~32 八位位组	已发现的 BSS 的 SSID
BSSType (BSS 类型)	枚举型	INFRASTRUCTURE INDEPENDENT	已发现的 BSS 的类型
Beacon Period (信标周期)	整数型	N/A	已发现的 BSS 的信标周期(以 TU 为单位)
DTIM Period (DTIM 周期)	整数型	如帧格式中所定义	BSS 的 DTIM 周期(以信标周期为单位)
Timestamp (时戳)	整数型	N/A	从已发现的 BSS 中收到的帧(探测响应/信标)的时戳
Local Time (本地时间)	整数型	N/A	开始接收来自扫描发现的 BSS 的帧(探测响应/信标)的时戳字段的第 1 个八位位组时, STA 的 TSF 定时器值
PHY parameter set (PHY 参数集合)	如帧格式中所定义	如帧格式中所定义	与 PHY 相关的参数集合
CF parameter set (CF 参数集合)	如帧格式中所定义	如帧格式中所定义	CF 周期的参数集合(如果扫描发现的 BSS 支持 CF 模式)
IBSS parameter set (IBSS 参数集合)	如帧格式中所定义	如帧格式中所定义	IBSS 的参数集合(如果扫描发现的 BSS 是 IBSS)
CapabilityInformation (能力信息)	如帧格式中所定义	如帧格式中所定义	已公告的 BSS 的能力
BSSBasicRateSet (BSS 基本速率集)	整数集合	2~127 (对集合中的 每个整数)	期望加入这个 BSS 的所有 STA 都必须支持的数据速率集合。STA 必须能够以集合中列出的每一速率接收和发送

## 10.3.2.2.3 产生条件

该原语作为原语 MLME-SCAN.request 所探知的 STA 的操作环境的结果, 由 MLME 产生。

## 10.3.2.2.4 收后效果

该原语通告 SME 扫描过程的结果。

## 10.3.3 同步

该机制支持在链路验证过程中选择对等方的过程。

## 10.3.3.1 MLME-JOIN.request

## 10.3.3.1.1 功能

该原语请求与一个 BSS 同步。

## 10.3.3.1.2 服务原语的语义

原语参数如下：

MLME-JOIN.request (

BSSDescription,

JoinFailureTimeout,

ProbeDelay,

OperationalRateSet

)

名 称	类 型	有效范围	描 述
BSSDescription (BSS 描述)	BSSDescription	N/A	STA 要加入的 BSS 的 BSSDescription, BSSDescription 是作为原语 MLME-SCAN request 的结果而返回的描述集的成员之一
JoinFailureTimeout (加入失败超时)	整型	$\geq 1$	以信标间隔为单位的时间界限, 在此时间界限后, 终止加入规程
ProbeDelay (探测延迟)	整型	N/A	在主动扫描期间, 发送探测帧之前所用的延迟 (以 $\mu s$ 为单位)
OperationalRateSet (操作速率集)	整数集合	2~127 (对集合中的每个整数)	在 BSS 内, STA 可以用于通信的数据速率集合。STA 必须能够以集合中列出的每一个速率进行接收。该集是由 BSS 公告的 BSS 基本速率集的超集

## 10.3.3.1.3 产生条件

该原语由 SME 产生, 以使 STA 与一个 BSS 建立同步。

## 10.3.3.1.4 收后效果

一旦当前的帧交换序列结束, 该原语启动同步规程。MLME 基于参数 BSSDescription 提供的元素与指定的 BSS 建立时间同步, 随后 MLME 发布一个反应结果的原语 MLME-JOIN.confirm。

## 10.3.3.2 MLME-JOIN.confirm

## 10.3.3.2.1 功能

该原语用于确认与一个 BSS 的同步。

## 10.3.3.2.2 服务原语的语义

原语参数如下：

MLME-JOIN.confirm (

ResultCode

)

名 称	类 型	有效范围	描 述
ResultCode (返回值)	枚举型	SUCCESS INVALID_PARAMETERS TIMEOUT	指示原语 MLME-JOIN.request 的结果

## 10.3.3.2.3 产生条件

该原语由 MLME 产生, 作为原语 MLME-JOIN.request 建立与 BSS 的同步的结果。

## 10.3.3.2.4 收后效果

## GB 15629.11—2003

通告 SME 同步规程的结果。

## 10.3.4 链路验证

该机制支持与对等 MAC 实体建立链路验证关系的过程。

## 10.3.4.1 MLME-LINKVERIFY.request

## 10.3.4.1.1 功能

该原语请求与一个规定的对等 MAC 实体建立链路验证关系。

## 10.3.4.1.2 服务原语的语义

原语参数如下：

```
MLME- LINKVERIFY.request (
    PeerSTAAddress,
    LinkVerifyFailureTimeout
)
```

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单 MAC 地址	规定与之建立链路验证过程的 对等 MAC 实体的地址
LinkVerifyFailureTimeout (链路验证失败超时)	整数型	$\geq 1$	规定终止链路验证规程的时间 界限 (单位为 TU)

## 10.3.4.1.3 产生条件

该原语由 SME 产生, STA 用于同一个特定的对等 MAC 实体建立链路验证关系, 以便允许在两个 STA 之间交换第 2 类帧。在链路验证规程中, SME 可能产生额外的原语 MLME-LINKVERIFY.request。

## 10.3.4.1.4 收后效果

该原语启动链路验证过程。随后 MLME 发布一个反映结果的原语 MLME-LINKVERIFY.confirm。

## 10.3.4.2 MLME-LINKVERIFY.confirm

## 10.3.4.2.1 功能

该原语报告与指定的对等 MAC 实体尝试建立链路验证关系的过程结果。

## 10.3.4.2.2 服务原语的语义

原语参数如下：

```
MLME- LINKVERIFY.confirm (
    PeerSTAAddress,
    ResultCode
)
```

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定试图与之建立链路验证过程的对等 MAC 实体的地址。该值必须与相应的原语 MLME-LINKVERIFY.request 中的参数 PeerSTAAddress 相匹配
ResultCode (返回值)	枚举型	SUCCESS INVALID_PARAMETERS TIMEOUT TOO_MANY_ SIMULTANEOUS_ REQUESTS REFUSED	指示原语 MLME- LINKVERIFY.request 的结果

## 10.3.4.2.3 产生条件

该原语由 MLME 产生，是用于同规定的对等 MAC 实体建立链路验证的原语 MLME-LINKVERIFY.request 的结果。

## 10.3.4.2.4 收后效果

通知 SME 链路验证规程的结果。

## 10.3.4.3 MLME-LINKVERIFY.indication

## 10.3.4.3.1 功能

该原语报告与规定的对等 MAC 实体建立链路验证关系的情况。

## 10.3.4.3.2 服务原语的语义

原语参数如下：

MLME-LINKVERIFY.indication (   
 PeerSTAAddress   
 )

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之建立链路验证关系的对等 MAC 实体的地址

## 10.3.4.3.3 产生条件

该原语由 MLME 产生，作为与规定的对等 MAC 实体建立链路验证关系的结果。而该链路验证关系的建立源于由指定的对等的 MAC 实体启动的链路验证过程。

## 10.3.4.3.4 收后效果

通知 SME 链路验证关系的建立。

## 10.3.5 解除链路验证

该机制支持使与一个对等的 MAC 实体之间的链路验证关系变为无效。

## 10.3.5.1 MLME-DELINKVERIFY.request

## 10.3.5.1.1 功能

该原语请求与一个对等的 MAC 实体之间的链路验证关系变为无效。

## 10.3.5.1.2 服务原语的语义

原语参数如下：

MLME-DELINKVERIFY.request (   
 PeerSTAAddress,   
 ReasonCode   
 )

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	任一有效的单个 MAC 地址	任一有效的单个 MAC 地址	规定与之解除链路验证关系的对等 MAC 实体的地址
ReasonCode (原因代码)	如帧格式所定义	如帧格式所定义	规定启动解除链路验证过程的原因

## 10.3.5.1.3 产生条件

该原语由 SME 产生，STA 用于使与一个规定的对等 MAC 实体之间的已建立的链路验证关系变为无效，以阻碍在两个 STA 之间交换第 2 类帧。在解除链路验证过程中，SME 可能产生额外的原语 MLME-DELINKVERIFY.request。

## 10.3.5.1.4 收后效果

该原语启动一个解除链路验证过程。随后 MLME 发布一个反应结果的原语 MLME-DELINK-VERIFY.confirm。

## GB 15629.11—2003

## 10.3.5.2 MLME-DELINKVERIFY.confirm

## 10.3.5.2.1 功能

该原语报告试图与指定的对等 MAC 实体解除链路验证关系的结果。

## 10.3.5.2.2 服务原语的语义

原语参数如下：

MLME-DELINKVERIFY.confirm (   
 PeerSTAAddress,   
 ResultCode   
 )

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定试图与之解除链路验证关系的对等 MAC 实体的地址
ResultCode (返回代码)	枚举	SUCCESS INVALID_PARAMETERS TOO_MANY_ SIMULTANEOUS_ REQUESTS	指示原语 MLME-DELINKVERIFY.request 的结果

## 10.3.5.2.3 产生条件

该原语由 MLME 产生，作为与规定的对等 MAC 实体解除链路验证关系的原语 MLME-DELINKVERIFY.request 的结果。

## 10.3.5.2.4 收后效果

通知 SME 解除链路验证过程的结果。

## 10.3.5.3 MLME-DELINKVERIFY.indication

## 10.3.5.3.1 功能

该原语报告与一个规定的对等 MAC 实体之间的链路验证关系无效。

## 10.3.5.3.2 服务原语的语义

原语参数如下：

MLME-DELINKVERIFY.indication (   
 PeerSTAAddress,   
 ReasonCode   
 )

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之解除链路验证关系的对等 MAC 实体的地址
ReasonCode (原因代码)	如帧格式中所定义	如帧格式中所定义	规定启动解除链路验证过程的原因

## 10.3.5.3.3 产生条件

该原语由 MLME 产生，作为与规定的对等 MAC 实体解除链路验证关系的结果。

## 10.3.5.3.4 收后效果

通知 SME 指定的链路验证关系的解除情况。

## 10.3.6 关联

下列原语描述 STA 如何与接入点(AP)进行关联。

## 10.3.6.1 MLME-ASSOCIATE.request

## 10.3.6.1.1 功能

该原语请求与充当 AP 的指定的对等 MAC 实体进行关联。



## 10.3.6.1.2 服务原语的语义

原语参数如下:

MLME-ASSOCIATE.request (

PeerSTAAddress,

AssociateFailureTimeout,

CapabilityInformation,

ListenInterval

)

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之执行关联过程的对等的 MAC 实体地址
AssociateFailureTimeout (关联失败超时)	整数型	$\geq 1$	规定终止关联过程的时间界限(单位 为 TU)
CapabilityInformation (能力信息)	如帧格式中所定义	如帧格式中所定义	规定 MAC 实体所用的操作能力定义
ListenInterval (侦听间隔)	整数型	$\geq 0$	规定在 STA 唤醒并侦听下一个信标 之前可以经过的信标间隔数

## 10.3.6.1.3 产生条件

当 STA 期望与 AP 进行关联时, 该原语由 SME 产生。

## 10.3.6.1.4 收后效果

该原语启动关联过程。随后 MLME 发布一个反映结果的原语 MLME-ASSOCIATE.confirm。

## 10.3.6.2 MLME-ASSOCIATE.confirm

## 10.3.6.2.1 功能

该原语报告试图与充当 AP 的指定的对等 MAC 实体进行关联的结果。

## 10.3.6.2.2 服务原语的语义

原语参数如下:

MLME-ASSOCIATE.confirm (

ResultCode

)

名 称	类 型	有效范围	描 述
ResultCode (返回值)	枚举型	SUCCESS INVALID_PARAMETERS TIMEOUT REFUSED	指示原语 MLME-ASSOCIATE.request 的结 果

## 10.3.6.2.3 产生条件

该原语由 MLME 产生, 作为与充当 AP 的指定的对等 MAC 实体进行关联的原语 MLME-ASSOCIATE.request 的结果。

## 10.3.6.2.4 收后效果

通知 SME 关联过程的结果。

## 10.3.6.3 MLME-ASSOCIATE.indication

## 10.3.6.3.1 功能

该原语报告与规定的对等 MAC 实体建立关联。

## 10.3.6.3.2 服务原语的语义

MLME-ASSOCIATE.indication (

PeerSTAAddress

)

## GB 15629.11—2003

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之建立关联的对等 MAC 实体的地址

## 10.3.6.3.3 产生条件

该原语由 MLME 产生, 作为与规定的对等 MAC 实体建立关联的结果。而此关联源于由规定的对等 MAC 实体启动的关联过程。

## 10.3.6.3.4 收后效果

通知 SME 关联关系的建立。

## 10.3.7 重新关联

下列原语描述 STA 如何与另外一个 AP 进行关联。

## 10.3.7.1 MLME-REASSOCIATE.request

## 10.3.7.1.1 功能

该原语请求关联关系改变至一个规定的新的充当 AP 的对等 MAC 实体。

## 10.3.7.1.2 服务原语的语义

原语参数如下:

MLME-REASSOCIATE.request (

NewAPAddress,

ReassociateFailureTimeout,

CapabilityInformation,

ListenInterval

)

名 称	类 型	有效范围	描 述
NewAPAddress (新的 AP 地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之执行重新关联过程的对等 MAC 实体的地址
ReassociateFailureTimeout (重新关联失败超时)	整数型	$\geq 1$	规定终止重新关联过程的时间界限 (以 TU 为单位)
CapabilityInformation (能力信息)	如帧格式中定义	如帧格式中定义	规定 MAC 实体所用的操作能力定义
ListenInterval (侦听间隔)	整数型	$\geq 0$	规定在 STA 唤醒并侦听下一个信标 帧前可以经过的信标间隔数

## 10.3.7.1.3 产生条件

该原语由 SME 产生, STA 用于将关联关系改变至一个规定的新的充当 AP 的对等 MAC 实体。

## 10.3.7.1.4 收后效果

该原语启动一个重新关联过程, 随后 MLME 发布反映结果的原语 MLME-REASSOCIATE.confirm。

## 10.3.7.2 MLME-REASSOCIATE.confirm

## 10.3.7.2.1 功能

该原语报告试图与充当 AP 的规定对等 MAC 实体取得重新关联的结果。

## 10.3.7.2.2 服务原语的语义

原语参数如下:

MLME-REASSOCIATE.confirm (

ResultCode

)

## GB 15629.11—2003

名 称	类 型	有效范围	描 述
ResultCode (返回值)	枚举型	SUCCESS INVALID_PARAMETERS TIMEOUT REFUSED	指示原语 MLME-REASSOCIATE.request 的结果

## 10.3.7.2.3 产生条件

该原语由 MLME 产生，作为试图与一个规定的充当 AP 的对等 MAC 实体进行重新关联的原语 MLME-REASSOCIATE.request 的结果。

## 10.3.7.2.4 收后效果

通知 SME 重新关联过程的结果。

## 10.3.7.3 MLME-REASSOCIATE.indication

## 10.3.7.3.1 功能

该原语报告与一个规定的对等 MAC 实体建立重新关联。

## 10.3.7.3.2 服务原语的语义

MLME-REASSOCIATE.indication (   
 PeerSTAAddress  
 )

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之建立重新关联的对等 MAC 实体的地址

## 10.3.7.3.3 产生条件

该原语由 MLME 产生，作为与规定的对等 MAC 实体建立重新关联的结果。而此重新关联源于规定的对等 MAC 实体启动的重新关联过程。

## 10.3.7.3.4 收后效果

通知 SME 重新关联已经建立。

## 10.3.8 解除关联

## 10.3.8.1 MLME-DISASSOCIATE.request

## 10.3.8.1.1 功能

该原语请求解除与充当 AP 的指定的对等 MAC 实体之间的关联关系。

## 10.3.8.1.2 服务原语的语义

原语参数如下：

MLME-DISASSOCIATE.request (   
 PeerSTAAddress,  
 ReasonCode  
 )

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之进行解除关联过程的 对等 MAC 实体
ReasonCode (原因码)	如帧格式中所 定义	如帧格式中所定义	规定启动解除关联过程的原因

## 10.3.8.1.3 产生条件

该原语由 SME 产生，用于使 STA 解除与 AP 之间的关联关系。

## 10.3.8.1.4 收后效果

该原语启动一个解除关联过程。随后 MLME 发布反映结果的原语 MLME-DISASSOCIATE

confirm.

#### 10.3.8.2.1 功能

该原语报告与一个规定的充当 AP 的对等 MAC 实体解除关联的过程的结果。

原语参数如下:

```
MLME-DISASSOCIATE.confirm (  
    ResultCode  
)
```

名 称	类 型	有效范围	描 述
ResultCode (返回值)	枚举型	SUCCESS INVALID_PARAMETERS TIMEOUT REFUSED	指示原语 MLME-DISASSOCIATE.request 的结果

10.3.8.2.3 产生条件

该原语由 MLME 产生，作为用于与一个指定的充当 AP 的对等 MAC 实体解除关联的原语 MLME-DISASSOCIATE.request 的结果。

#### 10.3.8.2.4 收后效果

通知 SME 解除关联过程的结果。

#### 10.3.8.3 MLME-DISASSOCIATE.indication

#### 10.3.8.3.1 功能

该原语报告与一个指定的对等 MAC 实体解除关联。

#### 10.3.8.3.2 服务原语的语义

```
MLME-DISASSOCIATE.indication (
    PeerSTA Address,
    ReasonCode
)
```

名 称	类 型	有效范围	描 述
PeerSTAAddress (对等的 STA 的地址)	MAC 地址	任一有效的单个 MAC 地址	规定与之解除关联关系的对等 MAC 实体的地址
ReasonCode (原因码)	如帧格式中所定义	如帧格式中所定义	规定启动解除关联过程的原因

### 10.3.8.3.3 产生条件

该原语由 MLME 产生，作为与一个规定的对等 MAC 实体解除关联关系的过程的结果。

#### 10.3.8.3.4 收后效果

通知 SME 指定的关联关系无效。

### 10.3.9 重新設置

该机制支持重新设置 MAC 的过程。

#### 10.3.9.1 MLME-RESET.request

#### 10.3.9.1.1 功能

该原语请求重新设置 MAC 实体。

### 10.3.9.1.2 服务原语的语义

原语参数如下:

MLME-RESET.request (

STAAddress,  
SetDefaultMIB  
)

名 称	类 型	有效范围	描 述
STAAddress (STA 地址)	MAC 地址	任 何 有 效 的 MAC 地址	规定正在被重新设置的 MAC 实体要使用的 MAC 地址。该值可用于提供本地管理的 STA 地址
SetDefaultMIB (设置默认的 MIB)	布尔型	真, 假	若为真, 所有的 MIB 属性被置为默认值, 具体的默认值依具体的实现而定。 若为假, 虽然 MAC 被重新设置, 但所有 MIB 属性仍保持原语 MLME-RESET.request 产生之前的值不变

#### 10.3.9.1.3 产生条件

该原语由 SME 产生, 用以将 MAC 重新设置为初始状态。原语 MLME-RESET.request 必须在原语 MLME-START.request 之前使用。

#### 10.3.9.1.4 收后效果

该原语将 MAC 设置为初始状态, 即将所有内部变量清至默认值。通过设置标志 SetDefaultMIB 为真, MIB 属性可被重新设置为依实现而定的默认值。随后 MLME 发布一个反映结果的原语 MLME-RESET.confirm。

#### 10.3.9.2 MLME-RESET.confirm

##### 10.3.9.2.1 功能

该原语报告重新设置过程的结果。

##### 10.3.9.2.2 服务原语的语义

原语参数如下:

MLME-RESET.confirm (   
                      ResultCode  
 )

名 称	类 型	有效范围	描 述
ResultCode (返回值)	枚举型	SUCCESS	指示原语 MLME-RESET.request 的结果

#### 10.3.9.2.3 产生条件

该原语由 MLME 产生, 作为用于重新设置 MAC 实体的原语 MLME-RESET.request 的结果。

#### 10.3.9.2.4 收后效果

通知 SME 重新设置过程的结果。

#### 10.3.10 启动

该机制支持创建一个新的 BSS 的过程。

##### 10.3.10.1 MLME-START.request

##### 10.3.10.1.1 功能

该原语请求 MAC 实体启动一个新的 BSS。

##### 10.3.10.1.2 服务原语的语义

原语参数如下:

MLME-START.request (   
                      SSID,  
                      BSSType,  
                      BeaconPeriod,  
                      DTIMPeriod,  
                      CF parameter set,

## GB 15629.11—2003

PHY parameter set,  
 IBSS parameter set,  
 ProbeDelay,  
 CapabilityInformation,  
 BSSBasicRateSet,  
 OperationalRateSet  
 )

名 称	类 型	有效范围	描 述
SSID	八位位组串	1~32 八位位组	BSS 的 SSID
BSSType (BSS 类型)	枚举型	INFRASTRUCTURE INDEPENDENT	BSS 的类型
BeaconPeriod (信标周期)	整数型	$\geq 1$	BSS 的信标周期(以 TU 为单位)
DTIMPeriod (DTIM 周期)	整数型	如帧格式中所定义	BSS 的 DTIM 周期(以信标周期为单位)
CF parameter set (CF 参数集合)	如帧格式中所定义	如帧格式中所定义	若 BSS 支持 CF 模式, 则为 CF 期间的参数集合。由于发布原语 MLME-START.request 的副作用, aCFPPeriod 被修改
PHY parameter set (PHY 参数集合)	如帧格式中所定义	如帧格式中所定义	与 PHY 有关的参数集合
IBSS parameter set (IBSS 参数集合)	如帧格式中所定义	如帧格式中所定义	适用于 IBSS 的参数集合(若 BSS 为 IBSS)
ProbeDelay (探测延迟)	整数型	N/A	在主动扫描过程中, 在发送探测帧之前所用的延迟(单位为 $\mu s$ )
CapabilityInformation (能力信息)	如帧格式中所定义	如帧格式中所定义	向 BSS 通告的能力
BSSBasicRateSet (BSS 基本速率集)	整数集	2~127(对集合中的 每个整数)	所有加入本 BSS 的 STA 都必须支持的数据速率集(以 500kbit/s 为单位), 该 BSS 中的 STA 必须能以集合中列出的每一速率发送和接收数据
OperationalRateSet (操作速率集)	整数集	2~127(对集合中的 每个整数)	BSS 内的 STA 通信时可以使用的数据速率集。STA 必须能以集合中列出的每一速率接收数据。该集是由 BSS 通告的 BSS 基本速率集的超集

## 10.3.10.1.3 产生条件

该原语由 SME 产生, 以启动一个基础结构 BSS(MAC 实体充当 AP), 或者启动一个独立的 BSS(MAC 实体充当 IBSS 中的第一个 STA)。

原语 MLME-START.request 的产生时间必须在用原语 MLME-RESET.request 重新设置 MAC 实体之后和用原语 MLME-JOIN.request 成功加入一个已存在的基础结构 BSS 或独立的 BSS 之前。

如果没有原语 MLME-RESET.request 介入, 则在成功使用原语 MLME-START.request 或原语 MLME-JOIN.request 之后, 不能使用原语 MLME-START.request。

## 10.3.10.1.4 收后效果

一旦当前帧交换序列结束, 该原语启动 BSS 初始化过程。随后 MLME 发布反映创建过程结果的原语 MLME-START.confirm。

## 10.3.10.2 MLME-START.confirm

## 10.3.10.2.1 功能

该原语报告创建 BSS 过程的结果。

## 10.3.10.2.2 服务原语的语义

原语参数如下：

MLME-START.confirm (   
 ResultCode   
 )

名 称	类 性	有效范围	描 述
ResultCode (返回值)	枚举型	SUCCESS INVALID_PARAMETERS BASS_ALREADY_ STARTED_OR_JONED	指示原语 MLME-START.request 的结果

## 10.3.10.2.3 产生条件

该原语由 MLME 产生，作为用于创建一个新的 BSS 的原语 MLME-START.request 的结果。

## 10.3.10.2.4 收后效果

通知 SME 创建 BSS 的过程的结果。

## 10.4 PLME SAP 接口

PHY 管理服务接口包括以前所述的基于 PHY MIB 属性的通用原语 PLMEGET 和 PLMESET，以及原语 PLME-RESET、PLME-CHARACTERISTICS 和以下指定的原语。

## 10.4.1 PLME-RESET.request

## 10.4.1.1 功能

该原语是 LME 为复位 PHY 发出的请求。PHY 应总被复位为接收状态以避免偶然的数据发送。

## 10.4.1.2 服务原语的语义

原语语义如下：

PLME-RESET.request ( )

该原语无参数。

## 10.4.1.3 产生条件

该原语可在任意复位 PHY 时产生。

## 10.4.1.4 收后效果

PHY 子层收到该原语后应使 PHY 实体的发送和接收状态机复位，并置 PHY 为接收状态。

## 10.4.2 PLME-CHARACTERISTICS.request

## 10.4.2.1 功能

该原语是 LME 的请求原语，用于请求提供 PHY 操作特性。

## 10.4.2.2 服务原语的语义

原语语义如下：

PLME-CHARACTERISTICS.request ( )

该原语无参数。

## 10.4.2.3 产生条件

在初始化时刻，LME 产生该原语，请求 PHY 实体提供其操作特性。

## 10.4.2.4 收后效果

PHY 实体接收到该原语后应产生一个原语 PLME-CHARACTERISTICS.confirm，以运送该 PHY 实体的操作特性。

## 10.4.3 PLME-CHARACTERISTICS.confirm

## 10.4.3.1 功能

## GB 15629.11—2003

该原语提供 PHY 的操作特性。

## 10.4.3.2 服务原语的语义

原语参数如下：

PLME-CHARACTERISTICS.confirm (

- aSlotTime,
- aSIFSTime,
- aCCATime,
- aRxTxTurnarounTime,
- aTxPLCPDelay,
- aRxPLCPDelay,
- aRxTxSwitchTime,
- aTxRampOnTime,
- aTxRampOffTime,
- aTxRFDelay,
- aRxRFDelay,
- aAirPropagationTime,
- aMACProcessingDelay,
- aPreambleLength,
- aPLCPHeaderLength,
- aMPDUDurationFactor,
- aMPDUMaxLength,
- aCWmin,
- aCWmax

)

名 称	类型	描 述
aSlotTime (时隙时间)	整数型	MAC 用于定义 PIFS 和 DIFS 的时隙时间 (单位为 $\mu\text{s}$ )。见 9.2.10
aSIFSTime (SIFS 时间)	整数型	MAC 和 PHY 在空中接口接收到帧的最后一个符号到处理该帧并以空中接口中的最早的可能的响应帧的第一个符号作为响应所需要的额定时间 (单位为 $\mu\text{s}$ )。见 9.2.10
aCCATime (CCA 时间)	整数型	CCA 机制在每个时隙内评估媒体以确定媒体是忙或闲所需要的最小时间 (单位为 $\mu\text{s}$ )
aRxTxTurnaroundTime (接收发送转换时间)	整数型	PHY 从接收状态转换到发送第一个符号所需的最大时间 (单位为 $\mu\text{s}$ )。以下方程可导出 aRxTxTurnaroundTime: $\text{ATxPLCPDelay} + \text{aRxTxSwitchTime} + \text{aTxRampOnTime} + \text{aTxRFDelay}$
aTxPLCPDelay (PLCP 发送延迟)	整数型	PLCP 把一个符号从 MAC 接口传送到 PMD 的发送数据通路上所需要的额定时间 (单位为 $\mu\text{s}$ )
aRxPLCPDelay (PLCP 接收延迟)	整数型	PLCP 把一个比特从 PMD 接收通路上传送到 MAC 所需要的额定时间 (单位为 $\mu\text{s}$ )
aRxTxSwitchTime (接收发送切换时间)	整数型	PMD 从接收切换到发送所需要的额定时间 (单位为 $\mu\text{s}$ )
aTxRampOnTime (发送坡升时间)	整数型	PMD 打开发射器所需要的时间 (单位为 $\mu\text{s}$ )
aTxRampOffTime (发送坡降时间)	整数型	PMD 关闭发射功率放大器所需要的额定时间 (单位为 $\mu\text{s}$ )



## GB 15629.11—2003

aTxRFDelay (RF 发送延迟)	整数型	在原语 PMD-DATA.request 的发布和该原语在空中接口上对应的符号的开始之间的额定时间 (单位为 $\mu\text{s}$ )。符号的开始定义为: 对 FH 为符号中心位置前 1/2 符号周期; 对 DS 为符号的第一个码片中心位置前 1/2 码片周期, 对 IR 为对应时隙中心位置前 1/2 时隙
aRxRFDelay (RF 接收延迟)	整数型	在空中接口的最后符号结束和向 PLCP 发布原语 PMD-DATA.indicate 之间的额定时间 (单位为 $\mu\text{s}$ )。符号的结束定义为: 对 FH 为符号中心位置后 1/2 符号周期, 对 DS 为符号的最后一个码片中心位置后 1/2 码片周期, 对 IR 为对应时隙中心位置后 1/2 时隙
aAirPropagationTime (空中传播时间)	整数型	从发送站发送一个信号到接收站所预期的时间 (单位为 $\mu\text{s}$ )
aMACProcessingDelay (MAC 处理延迟)	整数型	MAC 处理一帧并准备对该帧进行响应所用的额定时间 (单位为 $\mu\text{s}$ )
aPreambleLength (前导码长度)	整数型	当前 PHY 的前导码长度 ( $\mu\text{s}$ )。如果已调制的前导码的实际长度值不足微秒的整数倍, 应向上取整
aPLCPHeaderLength (PLCP 头的长度)	整数型	当前 PHY PLCP 头的长度 (单位为 $\mu\text{s}$ )。如果已调制的 PLCP 头的实际长度值不是微秒的整数倍, 则向上取整
aMPDUDurationFactor (MPDU 的持续时间因子)	整数型	MPDU 通过无线媒体进行传输时 PHY 加给 MPDU 的开销, 可用 MPDU 的比特数乘以一个比例因子来表示。aMPDUDurationFactor 的值通过以下方程产生: 向下取整 $[(\text{PPDU 比特数}/\text{PSDU 比特数}) - 1] \times 10^9$ 。 在空中传输 PPDU 的总时间由以下方程产生 (并向上取整至下一个 $\mu\text{s}$ ): $\text{aPreambleLength} + \text{aPLCPHeaderLength} + ((\text{aMPDUDurationFactor} \times 8 \times \text{PSDU 八位位组数})/10^9) + (8 \times \text{PSDU 八位位组数})/\text{数据速率}$ 其中, 数据速率的单位为 Mbit/s。 从前导码的第一个符号到 PPDU 的任一八位位组开始的总时间 (单位为 $\mu\text{s}$ ) 可由以下方程中的持续时间因子计算: 向下取整 $[\text{aPreambleLength} + \text{aPLCPHeaderLength} + ((\text{aMPDUDurationFactor} \times 8 \times N)/10^9) + (8 \times N)/\text{数据速率}] + 1$ 其中, 数据速率单位为 Mbit/s, N 表示在期望的八位位组之前 PPDU 中的八位位组数, 但不包括前导码和 PLCP 头中的八位位组数
aMPDUMaxLength (MPDU 最大长度)	整数型	能被 PLCP PPDU 运送的 MPDU 的最大八位位组数
ACWmin	整数型	竞争窗口的最小长度, 单位为 aSlotTime
ACWmax	整数型	竞争窗口的最大长度, 单位为 aSlotTime

## 10.4.3.3 产生条件

该原语由 PHY 实体产生, 以响应原语 PLME-CHARACTERISTICS.request。

## 10.4.3.4 接收后效果

收到该原语提供 PHY 实体的操作参数。

## 10.4.4 PLME-DSSSTESTMODE.request

## 10.4.4.1 功能

该原语请求 DSSS PHY 实体进入测试模式操作。推荐使用与该原语相关联的参数, 在特定实现时这些参数是可选的。

## 10.4.4.2 服务原语的语义

原语参数如下:

PLME-DSSSTESTMODE.request (

TEST\_ENABLE,

TEST\_MODE,

SCRAMBLE\_STATE,

SPREADING\_STATE,  
DATA\_TYPE,  
DATA\_RATE  
)

名 称	类 型	有效范围	描 述
TEST_ENABLE (测试使能)	布尔型	真, 假	若为真, 根据余下的参数使能 PHY 测试模式
TEST_MODE (测试模式)	整数型	1, 2, 3	TEST-MODE 选择以下三种操作状态之一: 01=透明接收 02=持续发送 03=50%占空比
SCRAMBLE-STATE (加扰状态)	布尔型	真, 假	若为真, 将加扰器的操作状态置为 ON
SPREADING-STATE (扩展状态)	布尔型	真, 假	若为真, 选择码片生成操作状态
DATA-TYPE (数据类型)	整数型	1, 2, 3	选择三种数据模式中的一种用于测试的发送部分
DATA-RATE (数据速率)	整数型	2, 4	在 1Mbit/s 和 2Mbit/s 之间选择: 02=1Mbit/s 04=2Mbit/s

#### 10.4.4.3 产生条件

该原语应在任何进入 DSSS PHY 测试模式时产生。

#### 10.4.4.4 收后效果

PHY 子层收到该原语后应将 DSSS PHY 实体进入操作的测试模式。

#### 10.4.5 PLME-DSSSTESTOUTPUT.request

##### 10.4.5.1 功能

该可选原语应是 LME 的请求原语, 用于使能从 PHY 中选定的测试信号, 推荐使用与该原语相关联的参数, 在特定实现中这些参数是可选的。

##### 10.4.5.2 服务原语的语义

原语参数如下:

PLME-DSSSTESTOUTPUT.request (   
TEST\_OUTPUT  
)

名 称	类 型	有效范围	描 述
TEST_OUTPUT (测试输出)	布尔型	真, 假	若为真, 使能选择测试信号, 以测试 DS PHY

TEST\_OUTPTU 使被选定的信号能和不能用于调试和测试 PHY。可用于输出的一些信号为: PHY-TXSTART.request、PHY-RXSTART.indicate(RXVECTOR)、PHY-CCA.indicate、码片生成时钟、数据时钟、符号时钟、发送数据和接收数据。

##### 10.4.5.3 产生条件

当 DSSS PHY 处于测试模式时, 该原语可在任何以使能测试输出信号时产生。

##### 10.4.5.4 收后效果

DSSS PHY 子层收到该原语后, 应使 DSSS PHY 实体使能测试输出, 这些输出使用了由最近的原语 PLME-DSSSTESTMODE.request 所设置的模式。

## 11 MAC子层管理实体

### 11.1 同步

在单个 BSS 内的所有 STA 应采用这里定义的机制与一个公共时钟同步。

#### 11.1.1 基本方法

定时同步功能(TSF)使同一 BSS 内的所有 STA 的定时器保持同步。所有的 STA 均应维护一个本地的 TSF 定时器。

##### 11.1.1.1 基础结构网络的 TSF

在一个基础结构网络中, AP 应为定时控制器, 并应执行 TSF。AP 应以与任何同时启动的其他 AP 无关的方式初始化其 TSF 定时器, 以使多个 AP 中的 TSF 定时器的同步问题最小化。AP 应周期性地发送称为信标的特殊帧, 该帧包含一个 TSF 定时器的副本, 用于同步 BSS 中的其他 STA。接收 STA 应总是接受为 BSS 服务的 AP 发送的信标中的定时信息。如果接收 STA 的 TSF 定时器与收到的信标中的时戳不同, 则其应将其本地定时器的值设置为接收到的时戳值。

信标应由 AP 生成, 每个 BeaconPeriod (信标周期) 时间单元发送一次。

##### 11.1.1.2 独立 BSS(IBSS)中的 TSF

IBSS 中的 TSF 应通过分布式算法来实现, 该分布式算法由 BSS 中的所有成员来执行。BSS 中的每个 STA 都根据在本章中描述的算法来发送信标。如果 IBSS 中的 STA 接收到的信标或探测响应中的 TSF 值比其本身的 TSF 定时器更新, 则 STA 应采用从信标或探测响应中收到的定时。

#### 11.1.2 维持同步

每个 STA 维持一个以微秒递增模  $2^{64}$  的 TSF 定时器。STA 期望以额定的速率接收信标。信标之间的时间间隔由 STA 的参数 BeaconPeriod 定义。发送信标的 STA 应设置信标的时戳, 该值等于在时戳的第一个比特被发送到 PHY 的时刻 STA 的 TSF 定时器的值加上 STA 通过本地 PHY 从 MAC\_PHY 接口到 STA 与无线媒体接口(天线、LED 发射面等)的发送延迟。本章的算法定义了一种机制, 使得在  $4\mu s$  加上在 PHY 上为 1Mbit/s 或更高速的 PHY 的最大传播延迟的时间段内维持 BSS 内的各个 TSF 定时器同步。

##### 11.1.2.1 基础结构网络中信标的产生

AP 应根据自身的 aBeaconPeriod 属性, 通过发送信标为整个 BSS 定义定时。这里准确定义了一系列相隔 aBeaconPeriod 时间单元的目标信标传输时间(TBTT)。零时刻定义为一个 TBTT, 信标作为 DTIM, 且在 CFP 的起始时刻发送。在每一个 TBTT 处, AP 准备一个信标作为下一帧发送。如果载波侦听机制(见 9.2.1)判断媒体为不可用, AP 应根据第 9 章中规定的基本媒体访问规则来延迟实际的信标发送。信标周期包含在信标和探测响应帧中, STA 在加入 BSS 时应采用该信标周期。

注: 尽管信标帧的发送可能由于 CSMA 的延期而延迟, 但后续的信标帧应以额定的信标时间间隔进行发送, 如图 79 示出。

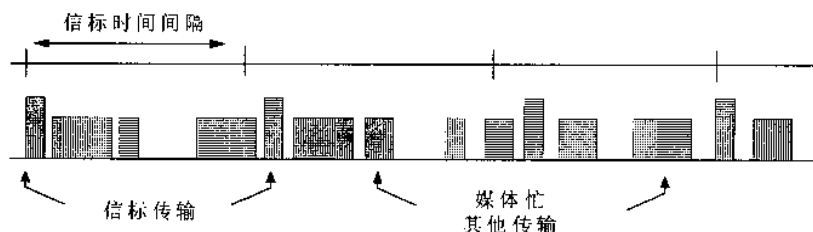


图 79 在忙网络上的信标传输

##### 11.1.2.2 IBSS 中信标的产生

在 IBSS 中信标的产生是分布式的。信标周期包含在信标和探测响应帧中, STA 在加入 IBSS 时应采用该信标周期。IBSS 的所有成员都参与信标的产生。每一个 STA 维护自己的 TSF 定时器, 用

## GB 15629.11—2003

于对 aBeaconPeriod 定时。IBSS 内的信标时间间隔由发起 IBSS 的 STA 建立。这准确定义了一系列相隔 aBeaconPeriod 时间单元的 TBTT。零时刻被定义为一个 TBTT，在每个 TBTT，STA 应

- 延缓对任何待发的非信标或非 ad hoc 指示(ATIM)发送的退避计时器的递减；
- 计算一个随机延迟，它均匀分布于零到两倍的  $aCW_{min} \times aSlotTime$  之间；
- 等待随机延迟周期，用与退避算法相同的算法递减随机延迟定时器；
- 如果信标在随机延迟定时器溢出前到达，则取消剩余的随机延迟和待发的信标的发送，并且 ATM 退避定时器应恢复递减；
- 如果随机延迟定时器溢出，并且在延迟期间没有信标到达，则发送一个信标（见图 80）。信标的传输应总是发生在以低功率模式操作的 STA 的唤醒周期内，这在 11.2 有更详细的描述。

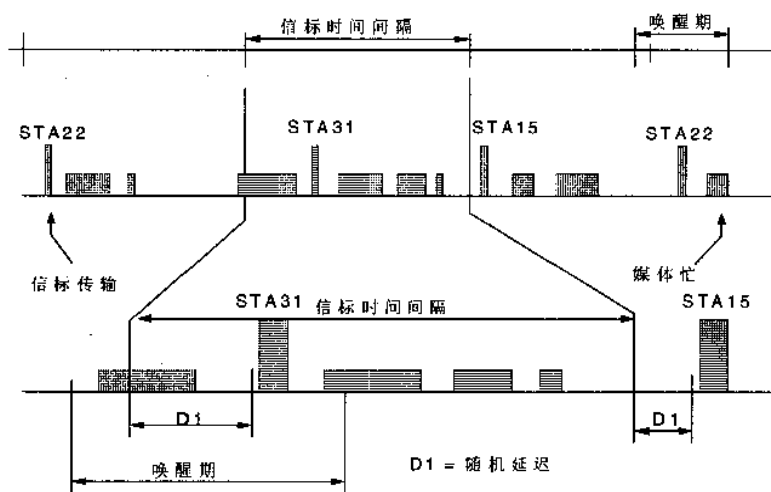


图 80 IBSS 中信标帧的传输

#### 11.1.2.3 信标的接收

STA 应使用所有接收到的信标的 CF 参数集合元素的信息来更新他们的 NAV，具体规定在 9.3.2.2。

如果 BSSID 字段与包含在 BSS 的 AP 中的 STA 当前使用的 MAC 地址相同，基础结构网络中的 STA 应仅使用接收到的信标帧中的其他信息。

在 IBSS 中，如果在该信标帧能力 Capability 字段的 IBSS 子字段被置为 1，并且 SSID 元素的内容与 IBSS 的 SSID 相同时，STA 应使用任何接收到的信标帧中的其他信息。信息的使用在 11.1.4 中规定。

#### 11.1.2.4 TSF 定时器的精确度

如 11.1.2.3 所描述，当接收到 FCS 字段和 BSSID 或 SSID 字段均有效的信标帧时，STA 按照以下算法更新其 TSF 定时器：通过加上一个等于接收方 STA 通过其 PHY 部分的延迟量与从时戳的第一个比特在 MAC/PHY 接口被接收的时刻算起所经过时间的和，来调整接收的时戳值。在基础结构 BSS 中，STA 的 TSF 定时器应设为调整后的时戳值。在 IBSS 中，如果调整后的时戳值晚于 STA 的 TSF 定时器的值，则 STA 的 TSF 定时器的值会校准到调整后的接收时戳值上。TSF 定时器的准确度应为  $\pm 0.01\%$ 。

#### 11.1.3 获取同步、扫描

STA 应根据当前的原语 MLME-SCAN.request 中参数 ScanMode 的值，操作以被动扫描模式或主动扫描模式操作。

当接收到原语 MLME-SCAN.request，STA 应扫描。参数 SSID 指示了要扫描的 SSID。要使用被动扫描方式成为一个特定 ESS 的成员，STA 应扫描包含该 ESS 的 SSID 的信标帧，返回所有与相应

的原语 MLME-SCAN.confirm 的参数 BSSDescriptionSet 中期望的 SSID 相匹配的信标帧。其中,能力信息字段中的适当比特会指示该信标帧来自基础结构 BSS 还是 IBSS。在主动扫描中,STA 会发送包含期望的 SSID 的探测帧。扫描一旦完成,MLME 就发布一个原语 MLME-SCAN.confirm,以指示所有接收到的 BSS 信息。

当接收到原语 MLME-JOIN.request, STA 会通过采用该请求中规定的 BSSID、TSF 定时器值、PHY 参数以及信标周期的值来加入到一个 BSS 中。

当接收到带广播 SSID 的原语 MLME-SCAN.request, STA 应根据参数 ScanMode 的值,被动扫描任何信标帧,或者主动地发送包含广播 SSID 的探测帧。扫描一旦完成,MLME 就发布一个原语 MLME-SCAN.confirm 以指示所有接收到的 BSS 信息。

如果 STA 不能扫描到具有期望的 SSID 和期望类型的 BSS,或不能发现任何 BSS,STA 在收到原语 MLME-START.request 后可启动一个 IBSS。

STA 可以启动它自己的 BSS,而不用先扫描 BSS 来加入它。

当 STA 启动一个 BSS 时,STA 应确定 BSS 的 BSSID。如果 BSSType 指示为基础结构 BSS,则 STA 应启动一个基础结构 BSS,并且 BSSID 应等于 STA 的 dot11StationID 值。即使在原语 MLME-START.request 完成后 dot11StationID 的值发生了变化,BSSID 的值也保持不变。如果 BSSType 指示为 IBSS,STA 应启动一个 IBSS,并且 BSSID 应为一个单个的本地管理的符合 IEEE Std 802-1990 规定的 MAC 地址。MAC 地址中剩余的 46 比特应是一个选定的数字,具体的选择方式使得即使多个 STA 在相同的初始条件的情况下,STA 生成相同数字的可能性也会被最小化。SSID 参数的值应被用作新的 BSS 的 SSID。设计者们能意识到在 STA 中对随机数据流的统计独立性的需求是很重要的。

#### 11.1.3.1 被动扫描

如果 ScanType 是被动的,STA 应在不超过由参数 ChannelTime 确定的最大时间内侦听每个被扫描的信道。

#### 11.1.3.2 主动扫描

主动扫描包括探测帧的产生和随后对接收到的探测响应帧的处理过程,主动扫描规程如后续条中规定。

##### 11.1.3.2.1 发送探测响应

按照下面的准则,只有当探测请求中的 SSID 是广播 SSID 或与 STA 中的特定的 SSID 相匹配时,接收探测请求帧的 STA 才会以探测响应帧作为响应。探测响应帧应作为定向帧被发送到产生探测请求的 STA 的地址。探测响应帧应使用正常的帧发送规则来发送。AP 应对所有符合上述准则的探测请求作出响应。在 IBSS 中产生最后一个信标帧的 STA 是对探测请求帧作出响应的 STA。

在每个 BSS 中,在任一给定时刻最少有一个 STA 处于唤醒状态以响应探测请求。发送信标的 STA 应保持 Awake (唤醒) 状态并应对探测请求作出响应,直到接收到带有当前 BSSID 的信标帧为止。如果 STA 是 AP,它应一直保持 Awake 状态并对探测请求作出响应。特别地,在 IBSS 中由于先前的信标帧没有被成功接收,或者由于在发送的信标之间产生了碰撞而导致在最近的 TBTT 之后不止有一个 STA 发送信标帧时,对任一给定的探测请求而言,可能不止有一个的 STA 对其作出响应。

##### 11.1.3.2.2 主动扫描规程

一旦接收到 ScanType 指示为主动扫描的原语 MLME-SCAN.request, STA 应采用如下规程:

对每个被扫描的信道:

- 等待直到 ProbeDelay 时间到期或者收到原语 PHY-RxStart.indication 为止;
- 执行 9.2.5.1 中定义的基本访问规程;
- 发送一个带有广播目的地址、SSID 和广播 BSSID 的探测;
- 清除并启动一个探测定时器 ProbeTimer;

## GB 15629.11—2003

- e) 在探测定时器 ProbeTimer 到达 MinChannelTime 之前, 如果还没有监测到 PHY-CCA.indication(忙), 则清除 NAV 并扫描下一信道, 否则当探测定时器到达 MaxChannelTime 时, 则处理所有收到的探测响应;
- f) 清除 NAV 并扫描下一信道。

见图 81。

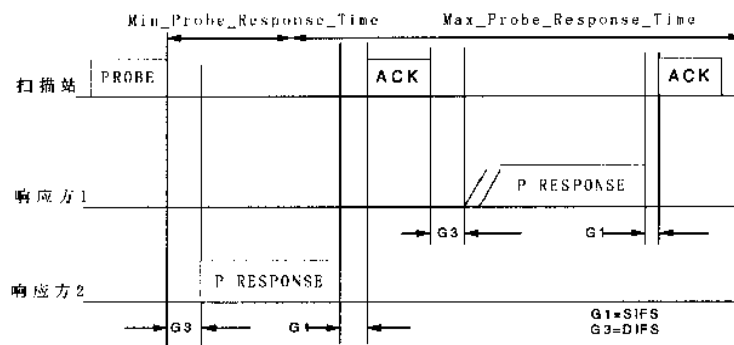


图 81 探测响应

在扫描完 ChannelList 中的所有信道后, MLME 应发布原语 MLME-SCAN.confirm, 并用 BSSDescriptionSet 参数包含在扫描期间内收集到的所有信息。

#### 11.1.3.3 初始化 BSS

一旦接收到原语 MLME-Start.request, STA 应确定 BSS 的 BSSID (如 11.1.3 中所描述), 选择信道同步信息, 选择信标周期, 初始化并启动 TSF 定时器, 并且开始发送信标。

#### 11.1.3.4 与 BSS 同步

一旦接收到原语 MLME-Join.request, STA 应在请求原语中采用参数: BSSID、信道同步信息和 TSF 定时器值。一旦从 BSS 中接收到信标帧, MLME 应发布原语 MLME-Join.confirm 以指示操作成功。如果在从 BSS 收到信标帧之前 JoinFailureTimeout 到期, 则 MLME 应发布原语 MLME-Join.confirm 以指示操作未成功。

#### 11.1.4 调整 STA 定时器

在基础结构 BSS 中, STA 总是采用来自其所属 BSS 中的 AP 的信标或探测响应中的定时器。

在 IBSS 中, 当信标帧或探测响应帧中包含一个匹配的 SSID 并且时戳的值迟于 STA 的 TSF 定时器时, STA 应总是采用该帧中的信息。作为对原语 MLME-Join.request 的响应, STA 应将其 TSF 定时器初始化为 0, 并且直到 STA 从带有匹配的 SSID 的 IBSS 成员中听到一个信标或探测响应时, 才发送一个信标或探测响应。

所有的信标和探测响应帧都带有一个时戳 Timestamp 字段。STA 从具有相同 SSID 的 IBSS 中的另一个 STA 接收到这样的帧后, 应将帧中的时戳字段与自身的 TSF 时间比较, 如果时戳字段比自身的 TSF 时间要迟, STA 应采用信标帧中的所有参数。

#### 11.1.5 频率跳变(FH)物理层定时同步

注: 本条仅适用于使用 FH PHY 的 STA。

这里所描述的 TSF 为在 FH 系统中的 STA 从一个信道转移到另一个信道 (他们的“跳”) 的同步提供了一种机制。每一个 STA 应维护一个表, 表中有系统中所有的跳变序列。在一个 BSS 中, 所有 STA 应采用相同的跳变序列。每一个信标和探测响应包含必要的信道同步信息, 以确定 BSS 的跳频图案和定时。

STA 使用其 TSF 定时器来为 aCurrentDwellTime 定时。aCurrentDwellTime 是 STA 在跳变序列的每个频率上应停留的时间长度, 在若干个 STA 同步后, 它们具有相同的 TSF 定时值。

只要满足下述条件, BSS 中的 STA 就应给正在使用的 PHY 发布一个合适的 PLME 服务原语,