ICS 35.110
L 78

中华人民共和国国家标准

GB 15629.11—2003

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)

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

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：5 GHz 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：2.4 GHz 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：2.4 GHz 频段较高速(速率大于 20 Mbit/s)扩展》

《无线局域网媒体访问控制和物理层规范：5 GHz 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第 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、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。

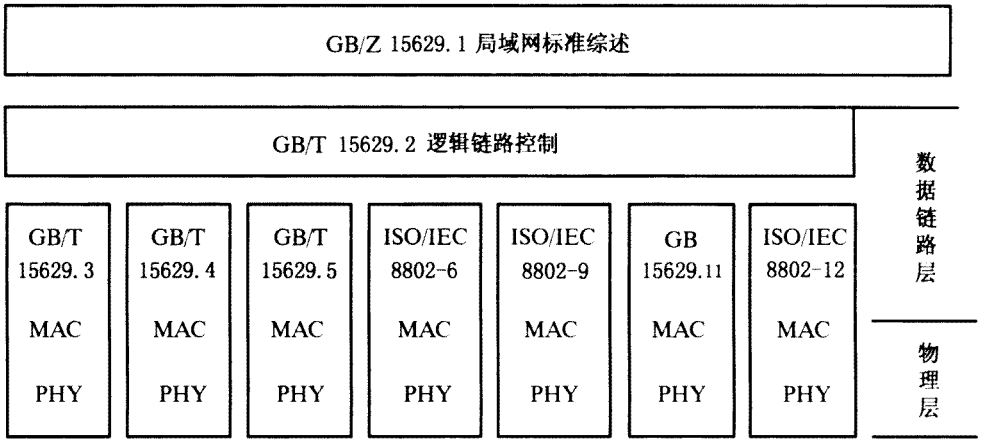
本部分由中国电子技术标准化研究所归口。

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：

a) 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；

b) GB/T 15629.4，利用令牌传递总线作为访问方法；

c) GB/T 15629.5，利用令牌传递环作为访问方法；

d) ISO/IEC 8802-6，利用分布式排队双总线作为访问方法；

e) ISO/IEC 8802-9，为骨干网提供综合业务的统一的访问方法；

f) 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；

g) 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；

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布署的自动装置、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自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　抽象句法表记法一(ASN.1)：基本记法规范

ISO/IEC 8824-2：1995　信息技术　抽象句法表记法一(ASN.1)：信息客体规范

ISO/IEC 8824-3：1995　信息技术　抽象句法表记法一(ASN.1)：限制规范

ISO/IEC 8824-4：1995　信息技术　抽象句法表记法一(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	带码分多址的直接系列扩频(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)

能构成一个自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

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 1024μs 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

与规定的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
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	目的服务访入点
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
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的概念和术语学。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)：

a) 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；

b) 不能避免外界信号；

c) 在媒体上通信的可靠性明显低于有线LAN的PHY；

d) 具有动态拓扑结构；

e) 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。

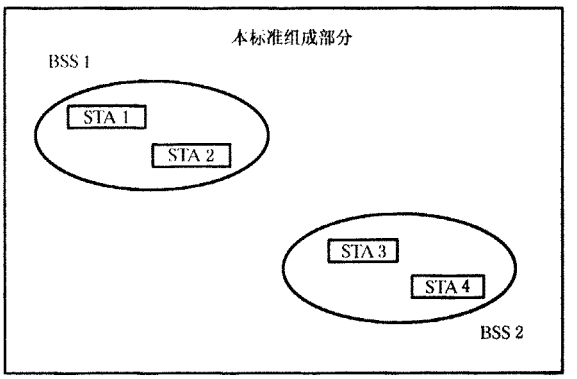


图 1 基本服务集

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。

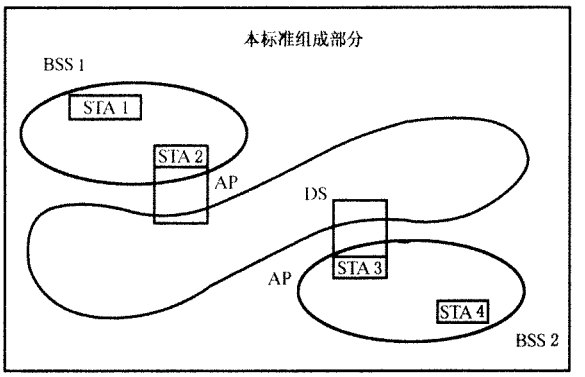


图 2 分布式系统和接入点

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。

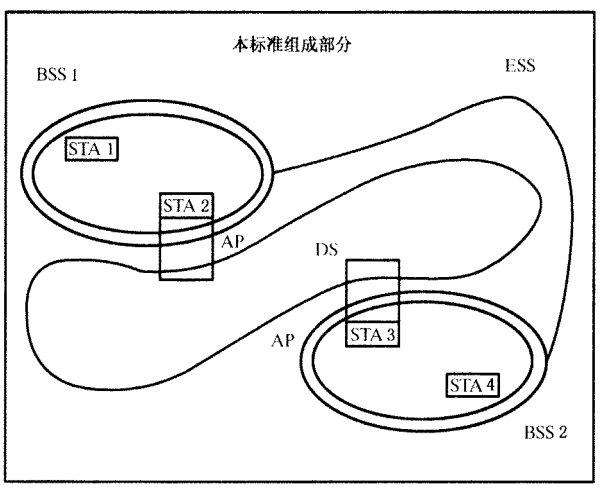


图 3 扩展服务集

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。

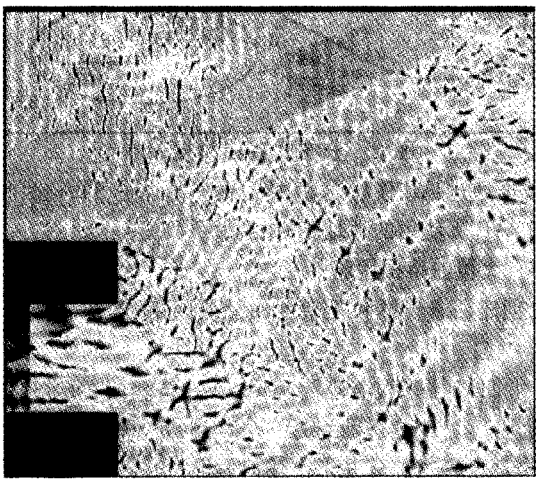


图 4 一个典型的信号强度图

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。

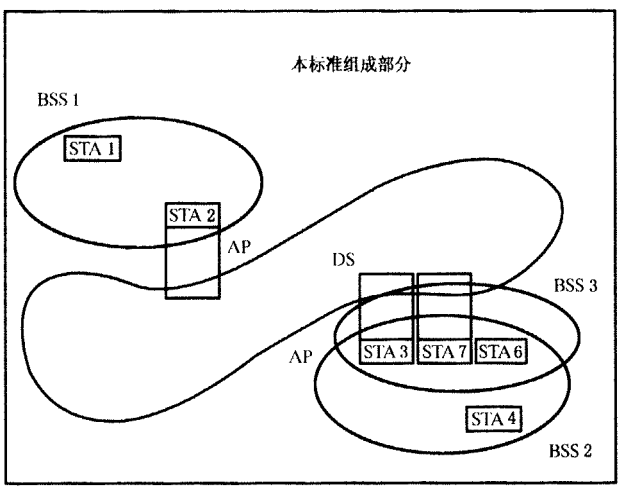


图 5 排列覆盖区

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。

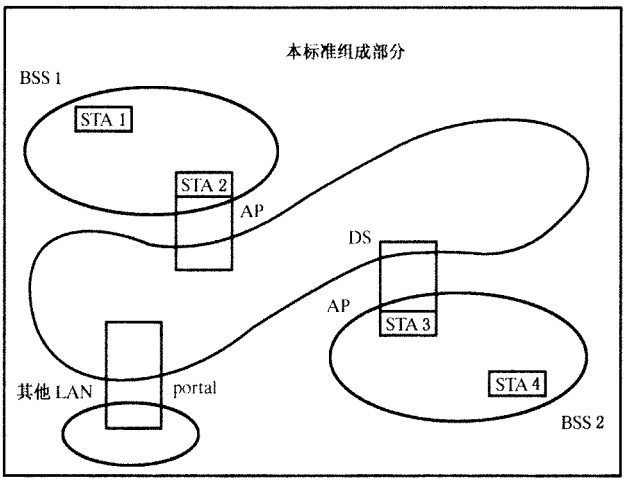


图 6　与其他 GB 15629 LAN 的连接

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 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，在性质上也不限定 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。

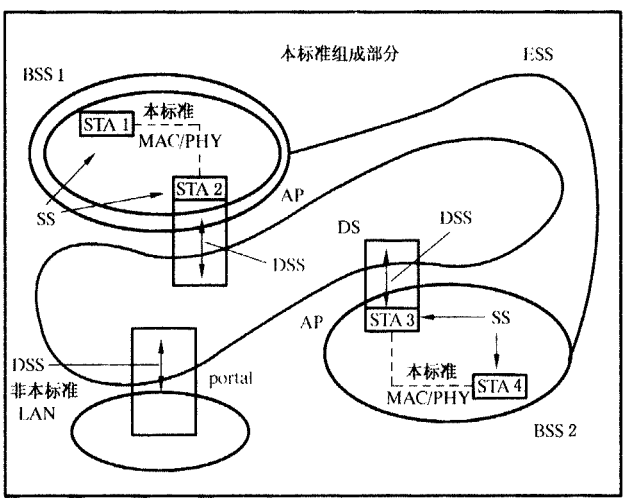


图 7 本部分完整的体系结构

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的地址空间内运行。本部分仅使用和规定 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。

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，通常很难区别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。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。

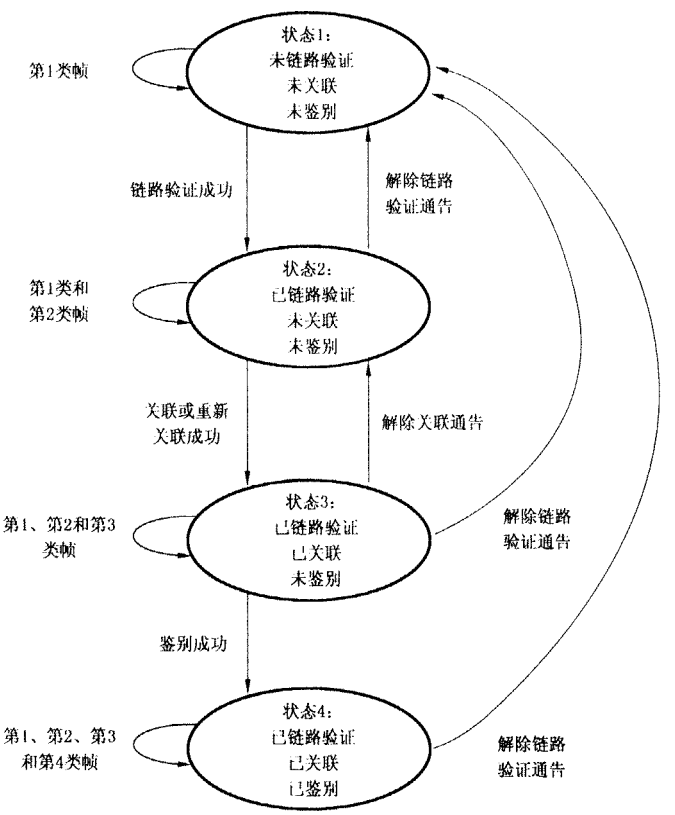


图 8 状态变量与服务间的关系

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;
2) CTS;
3) ACK;
4) CF-End +ACK;
5) CF-End。

b) 管理帧:

1) 探询请求/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。

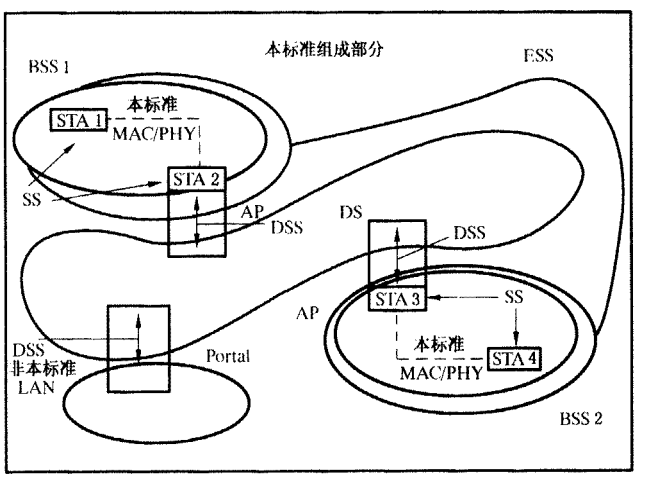


图 9 符合本部分的完整体系结构图

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。

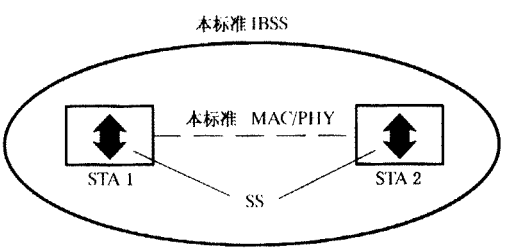


图 10 IBSS 逻辑体系结构

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。

——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(unsuccessful)”。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 和数据链络层的 MAC，这些层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。

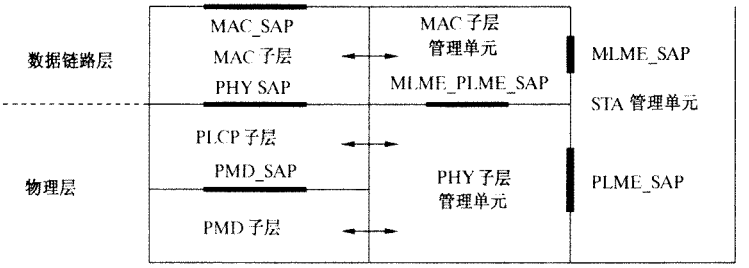


图 11 适用于本部分的基本参考模型构成

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：

a) 机密性；

b) 链路验证；

c) 鉴别；

d) 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 Strictly(Ordered(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 子层实体到传送到 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。

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。

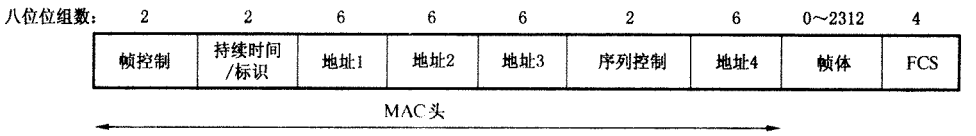


图 12 MAC 帧格式

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。

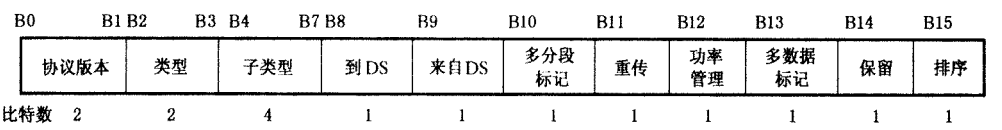


图 13 帧控制字段

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	探询请求
00	管理	0101	探询响应
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

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：

a) 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；

b) 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

表 3（续）

比特 15	比特 14	比特 13～0	用　　途
1	1	0	保留
1	1	1～2 007	PS-Poll 帧中的 AID
1	1	2 008～16 383	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询请求的管理帧的 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

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。

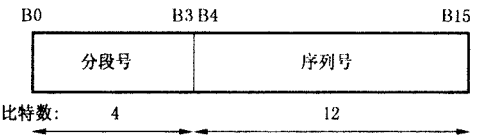


图 14 序列控制字段

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 4 096 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 MMPIDU 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：

a) $x^k \times (x^{31} + x^{30} + x^{29} + \cdots + x^2 + x + 1)$ 除以(模 2 除)$G(x)$ 的余式，k 为计算字段的比特数；

b) 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。

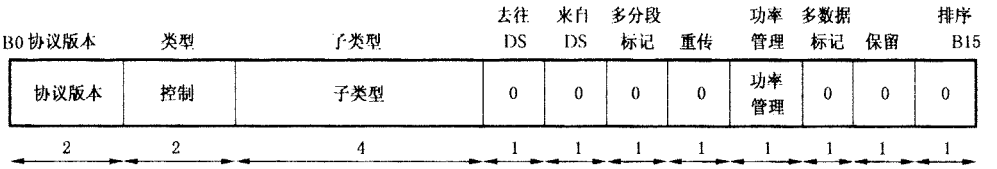


图 15 控制帧中帧控制字段的子字段值

7.2.1.1 请求发送(RTS)帧格式

图 16 定义了 RTS 帧的帧格式。

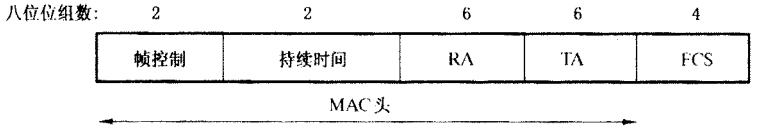


图 16 RTS 帧

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。

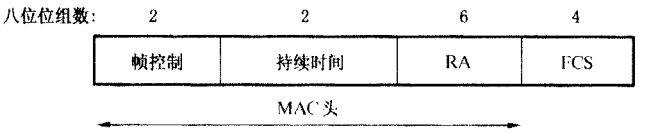


图 17 CTS 帧

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。

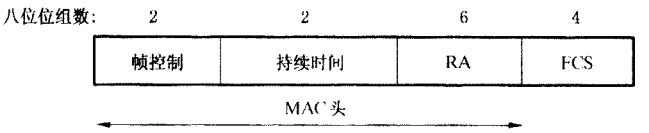


图 18 ACK 帧

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。

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。

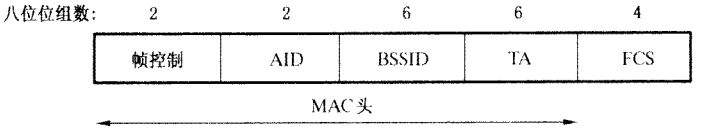


图 19 PS-Poll 帧

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。

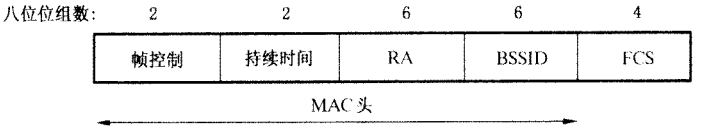


图 20 CF-End 帧

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。

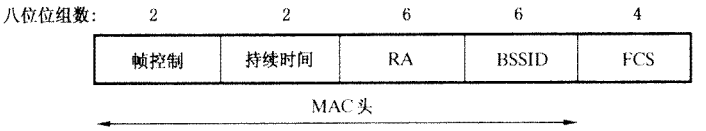


图 21 CF-End＋CF-ACK 帧

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。

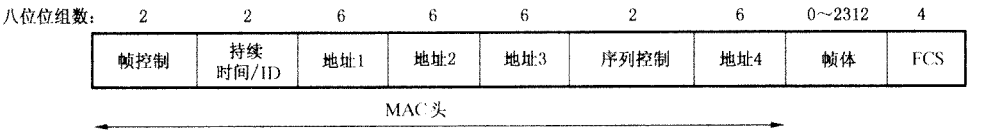


图 22 数据帧

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：

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；

b) 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置为 0；

— 如果帧的帧控制字段的多分段标记比特置为 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多分段标记比特置为 1，且地址 1 字段包含单地址，则持续时间字段的值置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 管理帧

管理帧的帧格式与帧的子类型无关，其定义如图 23 所示。

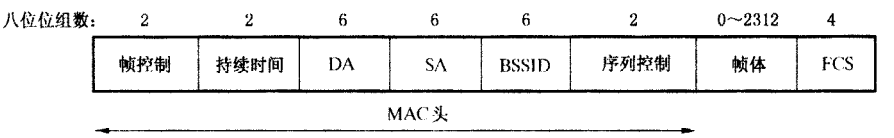


图 23 管理帧格式

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；

b) 如果站为 IBSS 的成员，则 BSSID 就是 IBSS 的 BSSID；

c) 在子类型为探询请求的管理帧中，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多分段标记比特置为 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多分段标记比特置为 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 探询请求帧格式

子类型为探询请求的管理帧的帧体包含的信息如表 11 所示。

表 11 探询请求帧体

顺　　序	信　　息
1	SSID
2	支持的速率

7.2.3.9 探询响应帧格式

子类型为探询响应的管理帧的帧体包含的信息如表 12 所示。

表 12 探询响应帧体

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 产生的探询响应帧中
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 产生的探询响应帧中
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 产生的探询响应帧中
9	IBSS 参数集合	TIM 信息元素仅出现在由 IBSS 中的 AP 产生的探询响应帧中

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。

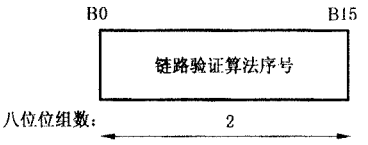


图 24 链路验证算法序号固定字段

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。

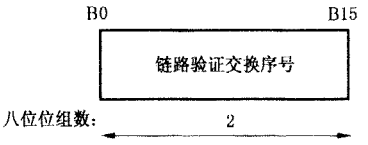


图 25 链路验证交换序号固定字段

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。

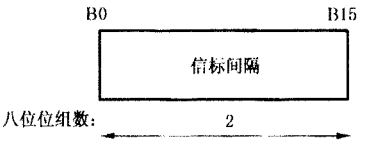


图 26 信标间隔固定字段

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。

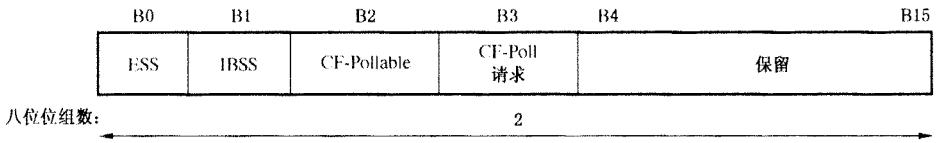


图 27 能力信息固定字段

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。

在发送的信标或探询响应帧中，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、探询响应、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询响应帧中的值相同。

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。

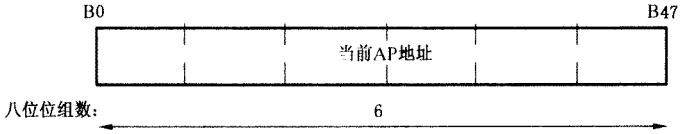


图 28 当前 AP 地址固定字段

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度，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。

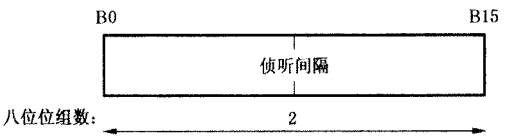


图 29 侦听间隔固定字段

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。

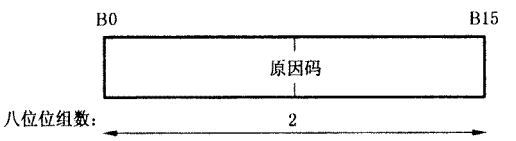


图 30 原因码固定字段

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

表 17（续）

原因码	含　　义
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。

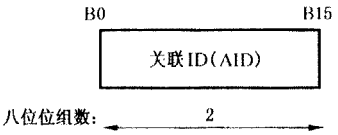


图 31　AID 固定字段

分配的关联 ID 值的变化范围为 1～2 007，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。

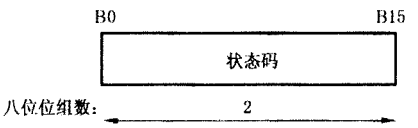


图 32　状态码固定字段

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

表 18（续）

状态码	含　　义
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
19～65 535	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。

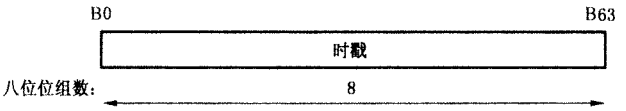


图 33　时戳固定字段

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。

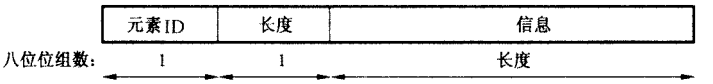


图 34　元素格式

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。

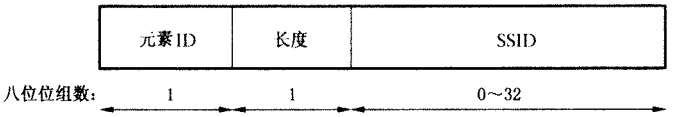


图 35　SSID 元素格式

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、探询响应、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。

信标和探询响应管理帧中的 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。

	元素ID	长度	支持速率
八位位组数：	1	1	1～8

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。

	元素ID	长度	驻留时间(TU)	跳频集合	跳频图案	跳频索引
八位位组数：	1	1	2	1	1	1

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。

	元素ID	长度	当前信道
八位位组数：	1	1	1

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。

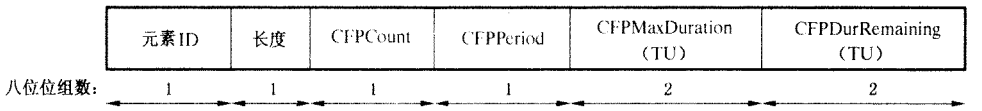


图 39 CF 参数集合元素格式

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。

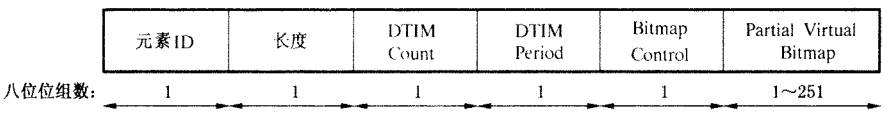


图 40 TIM 元素格式

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 2 008 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[N/8]的八位位组中编号为(N mod 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($N1\times8$)−1 全部为 0 的最大偶数,$N2$ 为能使位图中比特($N2+1$)×8 至比特 2 007全部为 0 的最小数。此时,位图偏移子字段的值包含整数[$N1/2$],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。

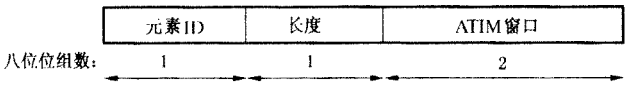


图 41 IBSS 参数集合元素格式

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：

a) 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。

b) 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 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。

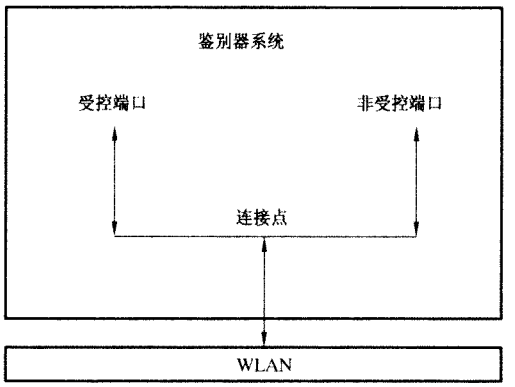


图 42　鉴别器系统示意图

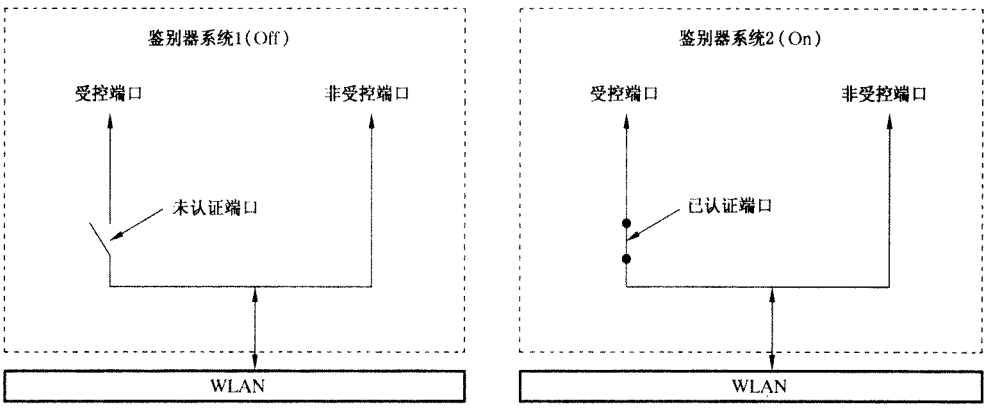


图 43　受控端口的鉴别状态

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：

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。

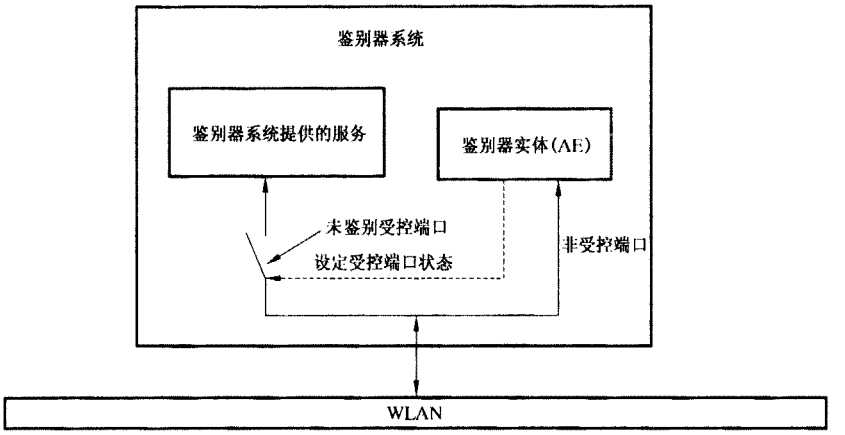


图 44 受控端口和非受控端口的用法

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。

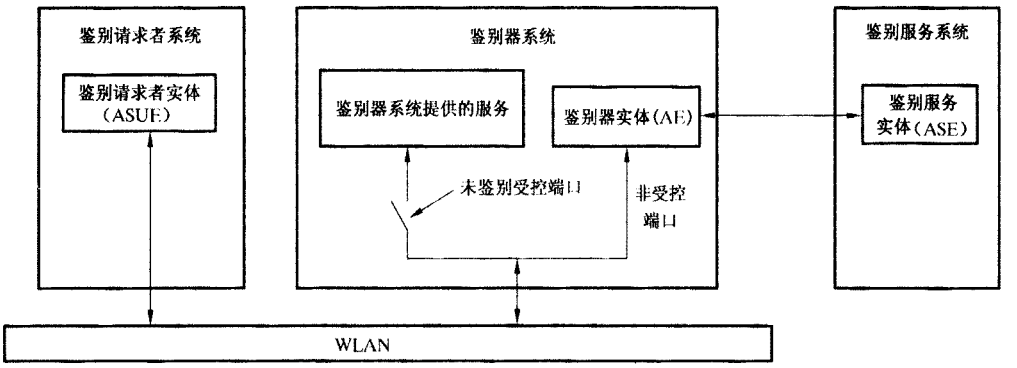


图 45 鉴别系统结构

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 鉴别基础结构中最为重要的组成部分，它的基本功能是实现对 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提供公钥合法性的证明。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。

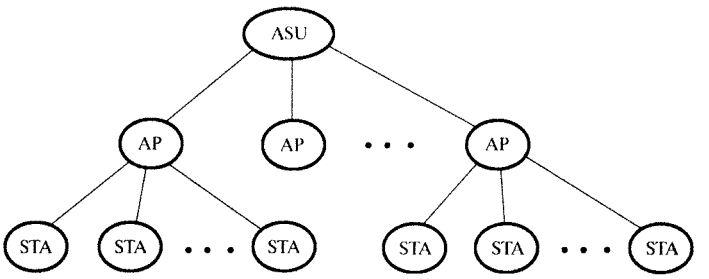


图 46　基于 ASU 的 WAI 逻辑拓扑结构示意图

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

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。

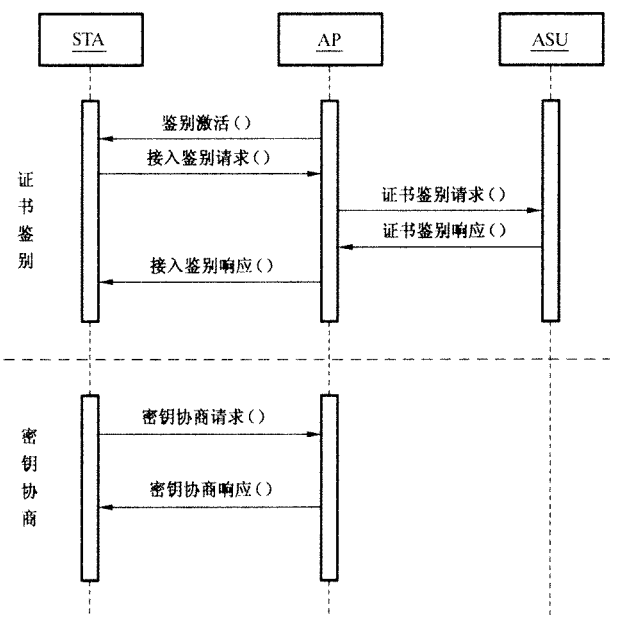


图 48 STA 接入鉴别流程图

8.3.1.1 证书鉴别

图 48 具体定义如下：

a) 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。

b) 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。

c) 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。

d) 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。

e) 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。