

无线局域网

无线局域网(WLAN)是目前很常见的无线计算机网络。其原理、结构、应用和传统的有线计算机网络较为接近,因而本书将 WLAN 作为第一种无线网络类型予以介绍。首先概述其原理和特点,并由浅入深阐述 WLAN 的协议体系结构。然后解读其发展趋势。最后通过 NS2 仿真实例,帮助读者深入分析相关的技术协议。

3.1 无线局域网概述

从本质上讲,WLAN 很像传统的有线计算机局域网,可以是服务器-客户机类型,也可以是无服务器的对等网。其突出特点就是网络链路从传统线缆变成无线,使用户能更为方便地以无线方式发送和接收数据。WLAN 是近几年来局域网技术发展最为迅猛的分支之一。

3.1.1 无线局域网的定义

WLAN 是计算机网络与无线通信技术相结合的产物,通常指采用无线传输介质的计算机局域网。可定义为一种利用无线方式,提供无线对等(如 PC 对 PC、PC 对交换机)或点到点(如 LAN 到 LAN)连通性的数据通信系统。WLAN 放弃了双绞线、同轴电缆或光纤,而通过电磁波传送和接收数据。目前采用的无线传输介质有无线电与红外线。从技术角度分析,WLAN 利用了无线多址信道和宽带调制技术来提供统一的物理层平台,并以此来支持节点间的数据通信,并为通信的移动化、个性化和多媒体应用提供可能。

WLAN 在距离有限的区域内实现无线通信,距离差异使得数据传输的范围不同,导致网络具体的设计和实现方面有所区别。WLAN 能在几十到几千米范围内支持较高数据速率,可采用微蜂窝(Microcell)、微微蜂窝(Picocell)结构,也可采用非蜂窝(如 Ad Hoc)结构。图 3.1 所示是 WLAN 与有线网络的集成部署示意图。图 3.2 所示为常见的 WLAN 设备。

目前 WLAN 领域有两个典型标准: IEEE 802.11、HiperLAN。

IEEE 802.11 系列标准由 802.11 工作组提出,包括 IEEE 802.11、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11i 和 IEEE 802.11n 等多个标准。IEEE 802.11 和 IEEE 802.11b 工作频率为 2.4GHz,传输速率分别为 1~2Mbps 和 5.5~11Mbps。IEEE 802.11a 工作于 5~6GHz 频段,传输速率可达 54Mbps。IEEE 802.11g 工作于 2.4GHz 频段,采用 CCK、OFDM、分组二进制卷积码(PBCC)等技术,可提供 54Mbps 的速率。WiFi 是 IEEE 802.11 的另一种商业名称,由 WiFi 联盟持有,目的是改善基于 IEEE 802.11 标准的 WLAN 产品之间的互通性。很多场合下 WiFi 和 IEEE 802.11 概念相同。

HiperLAN 由欧洲 ETS 开发,包括 HiperLAN1、HiperLAN2、室内无线骨干网络的 HiperLink、室外访问有线基础设施的 HiperAccess 等 4 种标准。目的是实现高速无线局域网连接、减少无线技术复杂性,采用了在 GSM 广泛使用的高斯最小移频键控调制技术。



图 3.1 典型 WLAN 和 LAN 集成部署示意图



图 3.2 WLAN 的常用设备

3.1.2 无线局域网的特点

1. 无线局域网的优点

WLAN 是在有线局域网的基础上发展而来,能使终端摆脱有线介质的束缚,而具有更大的便捷和移动性,并能实现与有线网络之间的互联互通。WLAN 的通信范围与传统有线网络相比受环境限制更小一些,网络传输范围大为拓宽。WLAN 具备一定的抗干扰能力和网络保密性。相对于有线网络,WLAN 的组建、配置和维护更容易。主要特点如下:

(1) 移动性。网络和主机迁移方便。通信范围不再受环境条件的限制,扩大了网络的覆盖范围,为便携式设备提供有效的网络接入功能,用户可随时随地获取信息。

(2) 灵活性。安装简单,组网灵活,可将网络延伸到线缆无法连接的地方。

(3) 可伸缩性。放置或添加接入点(Access Point, AP)或扩展点(Extend Point, EP),可扩展组网。

(4) 经济性。可用于难以实施物理布线的环境,如危险区和古建筑物中,节省了线缆、附件和人工费用。同时省去布线工序,快速组网,快速投入使用,提高了经济效益。可低成本快速实现临时性的网络。而对需频繁布线或更换地方的场合,费用节约更为明显。

2. 无线局域网的局限性

WLAN 尽管有很多优点,也存在一些不足,具体包括:

(1) 可靠性。传统有线局域网的信道误码率小于 10^{-9} ,可靠性和稳定性极高。而 WLAN 采用无线信道,并不十分可靠,存在各种干扰和噪声,会引起信号衰落和误码,进而导致网络吞吐性能下降和不稳定。此外,由于无线传输的特殊性,还可能产生“隐藏节点”、“暴露节点”等现象,影响系统的可靠性。

(2) 兼容性与共存性。兼容性包括:WLAN 要兼容有线局域网;兼容现有网络操作系统和网络软件;多种 WLAN 标准互相兼容;不同厂家无线设备的兼容。共存性包括:同一频段的不同制式或标准共存,如 2.4GHz 的 IEEE 802.11 和蓝牙系统共存;不同频段、制式或标准共存,如 2.4GHz 和 5.8GHz 的 WLAN 共存,WLAN 与 2GHz/3GHz 共存等。

(3) 带宽与系统容量。由于频率资源匮乏,WLAN 的信道带宽远小于有线网络带宽。即使复用,其系统容量也小于有线网络。提高系统传输带宽和系统容量非常重要。

(4) 覆盖范围。WLAN 的低功率和高频率限制了其覆盖范围。为扩大覆盖范围,需引入蜂窝或微蜂窝网络结构,或中继与桥接等措施。

(5) 干扰。外界干扰可影响无线信道和 WLAN 设备,WLAN 内部也会形成自干扰,WLAN 也会干扰其他无线系统。因此规划和使用 WLAN 时,要综合考虑电磁兼容和抗干扰性。

(6) 安全性。包括两方面内容:一是信息安全,即信息传输的可靠性、保密性、合法性和不可篡改性;二是人员安全,即电磁波辐射对人体的影响。不同于有线封闭信道,WLAN 中无线电波可能遭受窃听和恶意干扰。WLAN 系统中也会存在一些安全漏洞。

(7) 节能管理。WLAN 的终端设备是便携设备,如笔记本电脑、PDA 等,为节省电池消耗、延长使用时间和提高电池寿命,网络应有节能管理功能。当站点不是数据收发状态时,应使机内收发处于休眠状态,而要收发数据时,再激活收发功能。

(8) 多业务与多媒体。已有 WLAN 标准和产品主要面向数据业务,而对语音、图像等多媒体业务的适应性较差,需进一步开发保证多媒体服务质量的相关标准和产品。

(9) 移动性。WLAN 虽可支持站的移动,但对大范围移动和高速移动的支持机制还不完善。而小范围的低速移动也会对性能造成一定影响。

(10) 小型化和低成本。其取决于大规模集成电路,尤其是高性能、高集成度技术的进步。目前相关技术已较成熟,已具备了生产小型、低价 WLAN 射频器件的能力。

3.1.3 无线局域网的分类

WLAN 可根据不同层次、不同业务、不同技术、不同标准及不同应用等进行分类。

(1) 根据频段,可分为专用频段和自由频段两类。自由频段又可分为红外线和 2.4GHz/5GHz 频段无线电两种。还可根据采用的传输技术进一步细分,如图 3.3 所示。

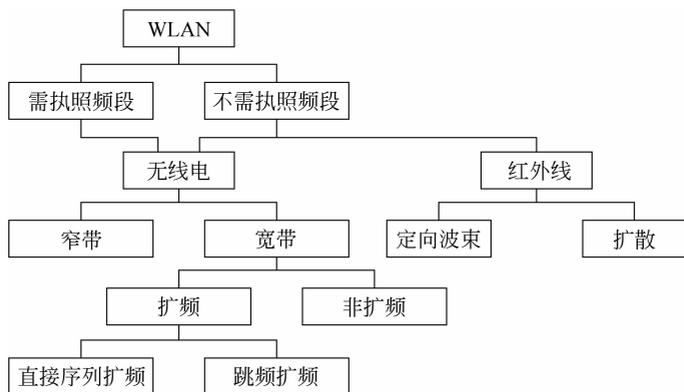


图 3.3 无线局域网分类一

(2) 根据业务类型,可分为面向连接和非连接两类。前者主要用于传输语音等实时性较强的业务,一般基于 TDMA 等技术,如 HiperLAN2 和蓝牙等。而后者主要用于高速数据传输,通常基于 IP 分组,这类是 IEEE 802.11 标准的典型例子,如图 3.4 所示。

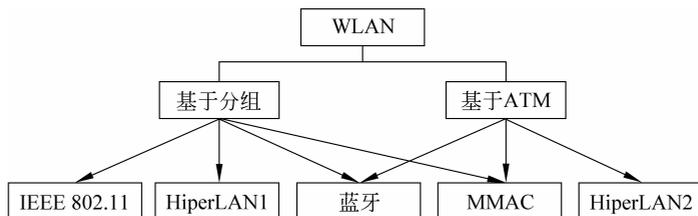


图 3.4 无线局域网分类二

(3) 根据网络拓扑和应用要求,可分为对等、基础架构、接入、中继等。

WLAN 的应用总体可分为室内和室外两类。室内应用包括家庭或小型办公室、大型建筑物、企事业单位、工业或商业等。室外应用包括园区和较远距离的无线网络连接及更远距离的网络中继。某些部门网或专用网会有室内、外的应用。公共 WLAN 接入近年来发展较快,主要部署在热点(hot spots)场所。

另一类适合 WLAN 应用的场合是需临时组网和难以布线的地方,如灾难恢复、短时间商用系统和大型会议等。

WLAN 有 3 种应用目的,即 WLAN 接入、网络无线互联和定位。前两种较普遍,而定位应用近年来才发展起来,与移动通信定位类似。WLAN 定位可与其他应用相结合。

3.2 无线局域网的组成与服务

3.2.1 无线局域网的组成

WLAN 由站、无线介质、无线接入点或基站、分布式系统等组成。

1. 站(STA)

站也称主机或终端,是 WLAN 的基本组成单元。站一般作为客户端,是具备无线网络接口的计算机设备,通常包括终端用户设备、无线网络接口和网络软件 3 部分。

WLAN 中的站如果移动,常称为移动主机或移动终端。按移动性可分为固定站、半移动站和移动站。固定站指位置固定不动,半移动站指经常改变地理位置,但移动时并不要求保持网络连接,而移动站则要求能在移动状态保持连接,典型移动速率为 2~10m/s。

站之间的通信距离由于天线辐射能力有限和应用环境不同而受限制。WLAN 能覆盖的区域范围称为服务区(Service Area, SA),由移动站的无线收发信机及地理环境确定的通信覆盖区域称基本服务区(BSA)或小区(Cell),是网络的最小单元。一个 BSA 内相互联系、相互通信的一组主机组成了基本业务集(BSS)。

2. 无线介质(WM)

无线介质是 WLAN 中站或 AP 间通信的传输介质,空气是无线电波和红外线传播的良好介质。WLAN 中的无线介质由物理层标准定义。

3. 无线接入点(BS)

AP 类似于移动通信网络的基站,通常处于 BSA 的中心,固定不动。其功能包括:

- ① 完成其他非 AP 的站的接入访问和同一 BSS 中的不同功能。
- ② 作为 WLAN 和分布式系统的桥接点,完成 WLAN 与分布式系统间的桥接功能。
- ③ 作为 BSS 的控制中心,控制和管理其他非 AP 站。

无线 AP 是具有无线网络接口的网络设备,一般包括:

- ① 与分布式系统的接口。
- ② 无线网络接口和相关软件。
- ③ 桥接软件、接入控制软件、管理软件等 AP 软件和网络软件。

4. 分布式系统(DS)

单个 BSA 覆盖区域受环境和主机收发信机特性的限制。为覆盖更大区域,需把多个 BSA 通过 DS 连接,形成一个扩展业务区(Extended Service Area, ESA),而通过 DS 互联的属同一 ESA 的所有主机组成一个扩展业务区集(Extended Service Set, ESS)。

用来连接不同 BSA 的通信信道,称为分布式系统介质(Distribution System

Medium,DSM)。DSM 可以是有线或无线信道。无线分布式系统(Wireless DS,WDS)可通过无线通信连接不同 BSS。DS 通过入口(Portal)连接骨干网。WLAN 和有线骨干网的数据传输都需经过 Portal。Portal 必须能识别有线网和 WLAN 的帧,它是一个逻辑接入点,也可以是一个单一设备,或与 AP 集成于同一设备。

3.2.2 无线局域网的拓扑结构

WLAN 的拓扑结构可从几方面分类。根据物理拓扑可分为单区网和多区网;根据逻辑拓扑可分为对等式、基础结构式和线型、星型、环型等;根据控制方式可分为无中心分布式和有中心集中控制式两种;根据与外网的连接性可分为独立 WLAN 和非独立 WLAN。

BSS 是 WLAN 的基本构造模块,有两种基本拓扑结构或组网方式:分布对等式拓扑、基础结构集中式拓扑。单个 BSS 称单区网,多个 BSS 通过 DS 互联构成多区网。

1. 分布对等式拓扑

分布对等式网络是一种独立 BSS(IBSS),至少有两个站。它是一种典型的自治方式单区网。通信范围内的任意站之间可直接通信而无需依赖 AP 转接,如图 3.5 所示。由于没有 AP,站之间是对等、分布式或无中心的。由于 IBSS 网络不必预先计划,可按需要随时构建,因此该模式被称为自组织网络。这种结构中各站点竞争公用信道。站点数过多时,信道竞争会影响网络性能。因此,较适合小规模、小范围的 WLAN。多用于临时组网和军事通信中。注意 IBSS 是一种单区网,但单区网并不一定就是 IBSS。另外 IBSS 不能接入 DS。

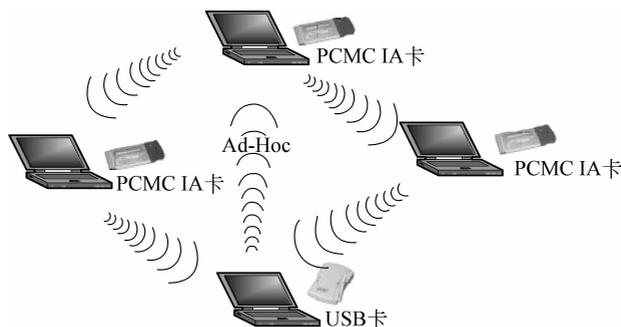


图 3.5 分布对等式工作模式

2. 基础结构集中式拓扑

一个基础结构除 DS 外,至少要有有一个 AP。只包含一个 AP 的单区基础结构网络如图 3.6 所示。AP 是 BSS 的中心控制站,其他站在该中心站的控制下互相通信。

与 IBSS 相比,基础结构 BSS 的可靠性较差,如 AP 遭破坏,整个 BSS 就会瘫痪。此外,中心站 AP 的复杂度较大,成本也较高。

在基础结构 BSS 中,如一个站想与同一 BSS 内的另一站通信,须经源站→AP→目标站的两跳过程,由 AP 予以转接。需较多的传输容量,增加了传输时延,但比各站直接通信仍具备以下优势:

(1) BSS 内的所有站都需在 AP 通信范围之内,而对各站间的距离无限制,即网络中的站点布局受环境限制较小。

(2) 由于各站不需保持邻居关系,其路由的复杂性和物理层实现复杂度较低。

(3) AP 作为中心站,控制所有站点对网络的访问,当网络业务量增大时网络吞吐和时延性能的恶化并不剧烈。

(4) AP 可对 BSS 内站点进行同步、移动和节能管理等,可控性好。

(5) 为接入 DS 或骨干网提供了一个逻辑接入点,并有较大的可伸缩性。可采用增加 AP 数量、选择 AP 位置等方法扩展容量和覆盖区域,即将单区 BSS 扩展成为多区 ESS。

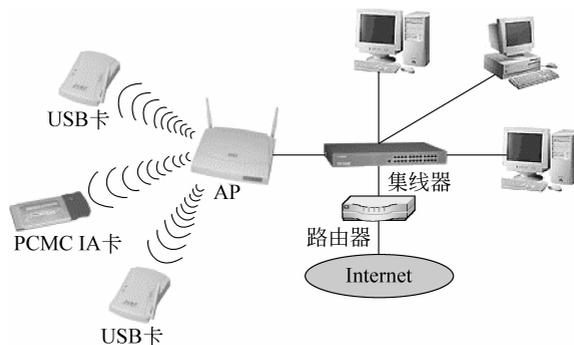


图 3.6 基础结构 BSS 工作模式

3. ESS 网络拓扑

ESA 是多个 BSA 通过 DS 连接形成的扩展区域,范围可达数千米。同一 ESA 的所有站组成 ESS。在 ESA 中,AP 除完成基本功能外,还可确定一个 BSA 的地理位置。ESS 是一种由多个 BSS 组成的多区网,每个 BSS 都获配一个 BSSID。如果一个网络由多个 ESS 组成,每个 ESS 也会有一个 ESSID,所有 ESSID 组成一个网络标识 NID 以区分该网络(子网)。

4. 中继或桥接型网络拓扑

两个或多个网络(LAN 或 WLAN)或网段可通过无线中继器、网桥或路由器等连接和扩展。如果中间只通过一个设备,称单跳网络;如果中间需通过多个设备,则称多跳网络。

3.2.3 无线局域网的服务

WLAN 的不同层次都有相应服务。与 WLAN 体系结构密切相关的服务有 STA 服

务和 DS 服务。这两种服务均在 MAC 层。IEEE 802.11 标准中定义了 9 种服务,3 种用于传送数据,6 种用于管理操作。

1. STA 服务

1) 认证(Authentication)

有线局域网用物理安全性来实现授权接入,而 WLAN 则不行,因为其传输介质没有精确的边界。所以需利用认证服务控制接入,所有 STA 均可用认证获取与其通信 STA 的身份。如果两台 STA 之间未建立交互式认证,则无法建立连接。STA 间的认证可以是链路级认证,也可为端到端或用户到用户的认证。认证过程和方案可自由选择。IEEE 802.11 支持开放系统认证和共享密钥认证,后者执行有线等价保密(Wired Equivalent Privacy,WEP)算法。

2) 解除认证(Deauthentication)

欲终止已存在的认证时,需唤醒解除认证服务。由于认证是连接的先决条件,因此解除认证能使 STA 解除连接。解除认证服务可由任一连接实体(非 AP 的 STA 或 AP)唤醒,它并非请求型,而为通知型服务,且解除认证不能被任何一方拒绝。当 AP 发给已连接的 STA 解除认证通知时,连接将被终止。

3) 保密(Privacy)

有线局域网中只有物理连接的站可侦听局域网通信。而无线共享介质则不同,任何一台符合标准的 STA 均可侦听到其覆盖范围内的所有物理层通信。因此,无保密连接到已存在的有线局域网时会严重降低该有线局域网的安全级别,可用 WEP 服务解决。

2. DS 服务

DS 提供的服务称为 DSS。在 WLAN 中,DSS 通常由 AP 提供,包括以下几种。

1) 连接(Association)

为在 DS 内传送信息,对于给定 STA,DSS 需知道接入哪个 AP。这种信息由连接提供给 DS,支持 BSS 的切换移动,连接是必要非充分条件,仅足以支持无切换的移动。

STA 允许通过 AP 发送数据前,首先连接至 AP。欲建立连接,先唤醒连接服务,该服务提供了 STA 到 DS 的 AP 映射。DS 使用该信息完成其消息分布业务。任一给定瞬间,一台 STA 仅可能和一个 AP 连接。一旦连接完成,STA 就能充分利用 DS(通过 AP)进行通信。连接通常由移动 STA 激活,一个 AP 可同一时间连接多个 STA。

2) 重新连接(Reassociation)

BSS 切换移动需重新连接服务。唤醒的重新连接服务用来完成当前连接从一个 AP 移动到另一 AP。当 STA 在 ESS 内从一个 BSS 移动到另一个 BSS 时,它保持了 AP 与 STA 之间的当前映射。当 STA 保持与同一 AP 的连接时,重新连接还能改变已建连接的属性。重新连接总是由移动 STA 激活。

3) 解除连接(Disassociation)

终止一个已有连接时会唤醒解除连接。在 ESS 中,它告诉 DS 取消已存在的连接消息。连接任一部分(非 AP 的 STA 或 AP)均可唤醒解除连接服务,解除连接是一个通告而非请求型服务,不能被连接的任一方拒绝。AP 可解除 STA 连接,使 AP 从网络中移走。STA 也可试图在需要它们离开网络时解除连接,而 MAC 协议并不依靠 STA 来唤醒解除连接服务。

4) 分布(Distribution)

作为 STA 使用的基本服务,是由来自或发送至工作在 ESS(此时帧通过 DS 发送)中的 WLAN STA 的每个数据消息唤醒,分布借助于 DSS 完成。

5) 集成(Integration)

如果分布式服务确定消息的接收端为集成 LAN 成员,则 DS 的输出点是端口而非 AP。分发到端口的消息使得 DS 唤醒集成功能,集成功能负责完成消息从 DSM 到集成 LAN 介质和地址空间的变换。

3.3 无线局域网协议体系结构

3.3.1 IEEE 802.11 协议标准

1. IEEE 802.11 标准的发展

1990 年 IEEE 802.11 工作组成立。1993 年形成基础协议,1997 年完成该协议。1998 年 IEEE 批准并公布了第一个正式版本,此后,IEEE 802.11 协议标准一直在不断发展和更新中。

IEEE 802.11 标准在 20 多年的发展过程中,形成了许多子集,如表 3.1 所示。

表 3.1 IEEE 802.11 系列标准

协议名称	发布时间/年	简要说明
IEEE 802.11	1997	2.4GHz 微波和红外线标准,初始速率为 1Mbps 和 2Mbps
IEEE 802.11a	1999	5GHz 微波标准,速率达 54Mbps
IEEE 802.11b	1999	2.4GHz 微波标准,增强到 5.5Mbps 和 11Mbps
IEEE 802.11c	2000	IEEE 802.11 网络和普通以太网之间的互通
IEEE 802.11d	2000	国际间漫游的规范
IEEE 802.11e	2005	服务质量控制,包括数据包脉冲
IEEE 802.11f	2003	服务访问点间通信协议
IEEE 802.11g	2003	2.4GHz 微波标准,速率达 54Mbps
IEEE 802.11h	2003	5GHz 微波频谱管理(欧洲)
IEEE 802.11i	2004	增强安全机制
IEEE 802.11j	2004	微波频谱扩展(日本)
IEEE 802.11k	2008	微波测量规范
IEEE 802.11n	2009	使用 MIMO 技术的高吞吐量规范(100Mbps)

续表

协议名称	发布时间/年	简要说明
IEEE 802.11p	2010	车载环境的无线接入
IEEE 802.11r	2008	快速的 BSS 切换
IEEE 802.11s	2010	网状网络的扩展服务集
IEEE 802.11u	2010	和非 IEEE 802 类型的网络协同
IEEE 802.11v	2010	无线网络管理
IEEE 802.11w	2009	被保护的网路管理帧
IEEE 802.11y	2008	3650~3700MHz 微波(美国)
IEEE 802.11z	2011	扩展到直接链路建立
IEEE 802.11aa	2011	音/视频流的鲁棒性
IEEE 802.11ac	2012	使用 MIMO 技术对 IEEE 802.11n 的改进

2. IEEE 802.11 若干子标准简介

先简单介绍一下 IEEE 802.11g, 其载波频率为 2.4GHz, 原始传送速率为 54Mbps, 净传输速度约为 24.7Mbps。其采用了 OFDM 技术, 兼容性和高数据速率弥补了 IEEE 802.11a 和 IEEE 802.11b 的缺陷, 目前已得到广泛使用。表 3.2 对早期的几个子标准进行了比较。

表 3.2 一些 IEEE 802.11 子标准性能比较

子标准	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
物理层	DSSS, FHSS, IR	DSSS	OFDM	OFDM
MAC 层	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA
频带	2.4G/900MHz	2.4GHz	5GHz	2.4GHz
传输速率/Mbps	1,2	1,2,5.5,11	6~54	最高 54
主要缺点	传输速率有限	传输速率有限	通信距离较短	共存网络数有限
主要优点	通信距离较远	通信距离较远	传输速率较高	传输速率较高

IEEE 802.11e 协议加入了服务质量(QoS)功能, 以改进和管理 WLAN 的服务质量, 进行音/视频媒体的传送, 以及增强的安全应用、移动访问应用等。

IEEE 802.11i 针对安全性, 弥补相对薄弱的 WEP 安全加密标准。包括对数据加密与用户身份认证, 它定义了基于 AES 的加密协议 CCMP、向前兼容 RC4 的加密协议 TKIP 等。

IEEE 802.11k 是提供信息以提高无线网络的效率。能实现站点报告, 列出移动客户。实现无破坏连接转移漫游时, 对接入点的有效选择。从而帮助用户实现无间断的网络连接。

IEEE 802.11s 的内容包括网状网络中的拓扑学习、路由与转发、安全性、测量、发现与联系、媒介访问协调、服务兼容性、互联、配置及管理。

IEEE 802.11n 是 IEEE 802.11 家族中较新的成员, 将传输速率从 IEEE 802.11g 的 54Mbps 增至 108Mbps 以上, 最高可达 320Mbps。使 WLAN 能平滑地结合有线网络, 全