第 5 章 无线局域网设计

本章将介绍无线局域网(Wireless Local Area Network，WLAN)技术以及设计规划方法。WLAN 以其灵活性而广泛流行。促进 WLAN 发展的主要原因在于其灵活性以及对用户服务的提升，比有线网络更节约成本。无论用户在哪里，只要无线信号可达的地方，WLAN 都可以让用户访问网络资源。现在越来越多的企业、机构意识到 WLAN 灵活性带来的好处，正在大量部署 WLAN。除了灵活性，WLAN 的另一个优势在于：有些地方部署有线 LAN 的成本较高，而部署 WLAN 的成本却很低。

但是这对 WLAN 的安全和管理提出了更高的要求，这也是 WLAN 设计的重要注意事项。

5.1 无线传输介质

在第 2 章中介绍了两类常见的网络传输介质：铜介质和光介质。除了这些有线介质外，还可以使用无线信号传输。

无线信号是一种能在真空或空气中传播的电磁波，无线电波很容易产生，同时还是全方位传播的，因此发射和接收装置不必在物理上很准确地对准。无线频谱只是电磁频谱中的一部分，所用频率为 3kHz～30GHz。无线电波的特性与频率有关。在较低频率上，无线电波能轻易地通过障碍物，但是其能量随着信号源距离的增大而急剧减小。在高频上，无线电波趋于直线传播但容易受障碍物的阻挡，它们还会被雨水吸收。

WLAN 中常见的无线数据通信种类有窄带、扩频和红外线(IR)。

窄带无线电系统的接收和传送信息者有着特定的无线电频率，并且使信息在尽可能窄的频带中通过。这种系统适用于长距离点到点的应用，但受环境干扰较大，不适合用来进行局域网数据的传送。大部分无线局域网系统使用扩频技术，扩展频谱以牺牲带宽效率换取可靠性、完整性和安全性。与窄带传输相比较，其信号所占有的频带宽度远大于所传信息必需的最小带宽，更多的带宽被消耗，但交换产生的信号能有效地放大，并且因此能轻易地被检测到。有两种常见的无线电扩频技术：跳频扩频(FHSS)和顺序扩频(DSSS)。

无线频段一般由政府机构授权使用，例如中国的无线频段归国家无线电委员会管理。但是，通常各国一般均留出 3 个无须授权的(开放)无线频段：

- 900MHz 频段：范围为 902MHz～928MHz，常用于无绳和蜂窝电话。
- 2.4GHz 频段：范围为 2.42GHz～2.4835GHz，是目前最广泛部署的无线标准。

• 5GHz 频段：范围为 5.725GHz～5.850GHz，常用于高速数据通信装置。

这 3 段无须授权的无线频段也称为 ISM 频段(Industrial Scientific Medical Band，工业科学医学频段)。ISM 频段是国际电联(ITU)为 ISM 设备专门划分的专业频段或与其无线电业务共用的频段。WLAN 通常使用 ISM 频段中的 2.4GHz 频段和 5GHz 频段。

5.2 无线局域网标准

WLAN 采用的标准是 IEEE 802.11 系列。1990 年 7 月，IEEE 802 委员会成立了 IEEE 802.11 WLAN 工作委员会，该委员会负责制定 WLAN 物理层及媒体访问控制(MAC)协议的标准，并于 1997 年 6 月公布了 IEEE 802.11 标准，该标准定义了物理层和 MAC 层协议规范，允许任何 LAN 应用、网络操作系统或协议在遵守 IEEE 802.11 标准的 WLAN 上运行时，就像运行在以太网上一样容易。之后又公布了多版修正的 IEEE 802.11 标准。

5.2.1 IEEE 802.11 系列标准

最初的 IEEE 802.11 标准最高速率仅为 1～2Mb/s，工作在 2.4GHz 频段。随着对 WLAN 性能要求的不断提高，又推出了速度更快的 802.11b、802.11a 和 802.11g 新标准。表 5.1 列出了 IEEE 802.11 系列常用标准的特性。

表 5.1 IEEE 802.11 系列标准

名　　称	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
MAC 协议	CSMA/CA	CSMA/CA	CSMA/CA
工作频段/GHz	5	2.4	2.4
最高速率/Mb/s	54	11	54
安全机制	WEP/WPA	WEP/WPA	WEP/WPA
兼容性	—	—	与 802.11b 兼容
批准时间	1999 年(可用性产品 2001 年出现)	1999 年	2003 年

IEEE 802.11b 的带宽最高可达 11Mb/s，扩大了 WLAN 的应用领域，是目前最流行的 WLAN 协议。IEEE 802.11b 使用的是开放的 2.4GHz 频段，不需要申请就可使用。WLAN 既可作为对有线网络的补充，也可独立组网，从而使网络用户摆脱网线的束缚，实现真正意义上的移动应用。

IEEE 802.11a 工作频段是 5GHz，但是目前已经逐渐被 IEEE 802.11g 取代。

2003 年 7 月，IEEE 批准了一项新标准 802.11g，该技术提升了无线局域网接入速度，传输速率达 54Mb/s，比通用的 802.11b 快近 4 倍，802.11b 标准和 802.11g 标准都在 2.4GHz频率范围内，两者是兼容的，也称为 Wi-Fi(Wireless Fidelity，无线高保真)技术。

5.2.2　MAC 协议

802.11 MAC 子层协议与 IEEE 802.3 以太网的原理类似，都是采用载波侦听的方式来控制网络中信息的传送。不同之处是以太网采用的是 CSMA/CD 技术，网络上所有工作站都侦听网络中有无信息发送，当发现网络空闲时即发出自己的信息，此时只能有一台工作站抢到发出信息权，其余工作站需要继续等待。如果一旦有两台以上的工作站同时发出信息，则网络中会发生冲突，导致这些冲突信息丢失，各工作站则将继续抢夺发出权。802.11b WLAN 引进了冲突避免技术——CSMA/CA（Carrier Sense Multiple Access / Collision Avoid，带冲突避免的载波监听多路访问），从而避免了网络冲突的发生，可以大幅度提高网络效率。

CSMA/CA 协议的工作原理是：如果某站点有数据要发送，它首先侦听信道，并根据下列不同的情形进行相应的处理。

（1）如果信道空闲，继续等待 IFS（InterFrame Space，帧间隔）时间，然后侦听信道；如果信道仍然空闲，立即发送数据。

（2）如果信道忙，该站点继续侦听信道，直到当前传输完全结束。

（3）一旦当前传输结束，站点继续等待 IFS 时间，然后再侦听信道，如果信道仍然保持空闲，站点按指数后退一个随机长的时间后，发送数据。

CSMA/CA 协议的工作流程如图 5.1 所示。

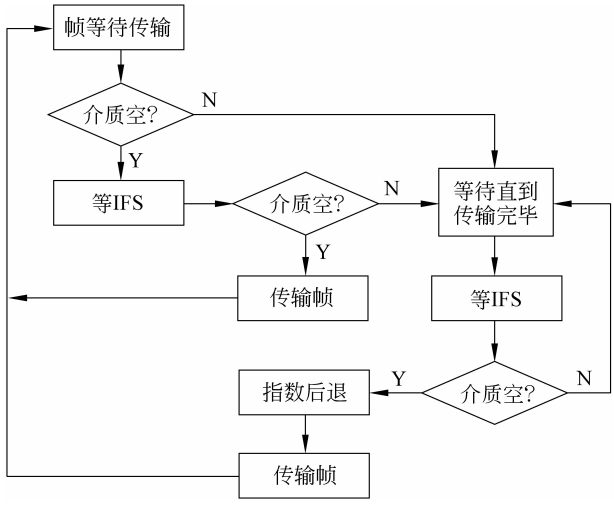

图 5.1　CSMA/CD 协议的工作流程图

按照 CSMA/CA 协议的要求，发送方在发送一数据帧后，接收方正确接收到后必须返回 ACK 给发送方（等待 IFS 时间）。如果发送方没有收到 ACK，则发送方必须重传该帧。如果无线信道的持续空闲时间大于 IFS，则站点可以立即访问无线信道。如果无线信道忙，则站点首先等无线信道变为空闲后继续等待 IFS，然后进入竞争阶段。在竞争阶段，每个无线站点选择一个随机后退时间，延迟这段时间继续侦听无线信道。如果无线信道仍然为空，则该站点可立即发送数据。使用后退算法延迟发送的目的在于避免多个站

点同时发送数据引起的冲突。

5.3 无线局域网设计

进行无线局域网设计具体包括以下几个步骤：了解用户需求、确定相应的组网方式、无线设备选型、无线网络设计、无线网络安全以及无线网络管理等。

5.3.1 组网方式

WLAN由无线接入点(Access Point，AP)和无线客户端设备组成。无线AP在无线客户端设备和有线网络之间提供连通性。无线客户端设备一般需要配备无线网卡(Wireless Network Interface Card，WNIC)，设备使用WNIC进行通信，根据组网方式不同，可能是无线客户端设备之间通信，或者无线客户端设备与无线AP进行通信。

WLAN组网一般采用单元结构，整个系统被分割成许多个单元，每个单元称为基本服务组(Basic Service Set，BSS)，BSS的组成有以下3种方式：独立BSS、有AP的BSS和扩展BSS。

1. 独立BSS

独立BSS是仅由无线客户端设备组成的工作单元，其内部站点可以直接通信并且没有到其他BSS的连接，不需要无线AP，这种类型的独立网络称为自组织网络或对等网络(Ad Hoc)，如图5.2所示。

在一个独立BSS中，因为无线站点没有中继功能，是完全分布式的，所以所有无线站点之间都是直接通信，不通过第三方转发。

2. 有AP的BSS

如果BSS不是独立的，而是通过一个无线AP与有线网相连，则称为是有AP的BSS，如图5.3所示。

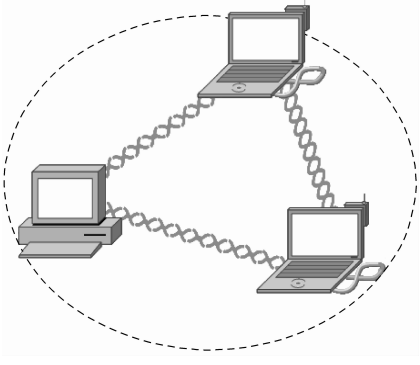

图5.2 独立BSS(Ad Hoc)

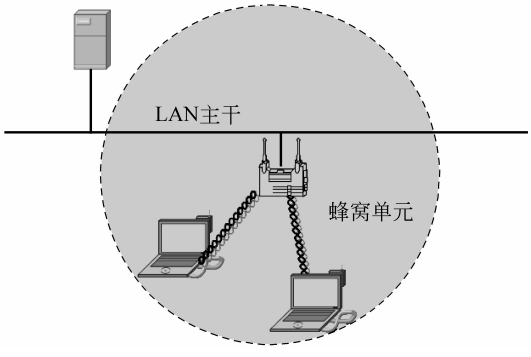

图5.3 有AP的BSS

在有AP的BSS中，无线站点之间不能直接通信，需要通过AP转发。无线站点通过AP接入有线主干网，其中AP起到网桥的作用。

AP使用无线射频(Radio Frequency，RF)代替有线通信，由于无线信号有衰减，每个

AP覆盖范围有限，通常形象地把一个AP覆盖范围称为一个蜂窝单元(Cell)。蜂窝单元的常见距离范围为91.44～152.4m(即300～500英尺)。在进行WLAN设计时，要考虑到蜂窝单元的覆盖范围，通常为了保证通信质量，相邻蜂窝单元覆盖范围应该有20%～30%的重叠，重叠区域内不同AP采用不同的信道区别，如图5.4所示。

在图5.4中，两个AP分别使用信道1和信道6，因此即便是在蜂窝单元的重叠区域，无线客户端设备仍然能区分这两个AP发出的RF信号。

WLAN吞吐量(速度)与发送者和接收者之间的距离成反比。所以，在其他情况相同的情况下，无线客户端距离发送者越近，吞吐量就越大，如图5.5所示。

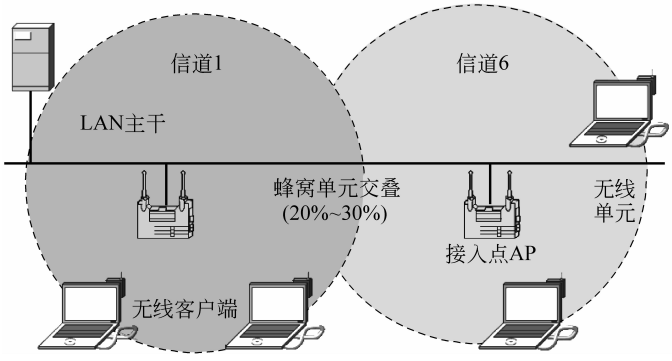

图5.4　相邻蜂窝单元交叠

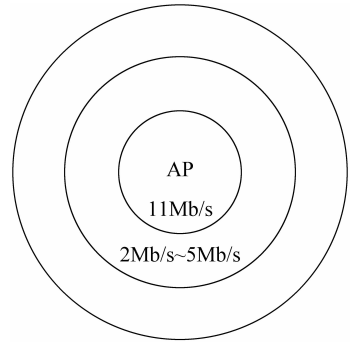

图5.5　吞吐量与发送者距离的关系

因此，在WLAN设计时，如何部署AP点位置也是必须考考虑的重要问题。为了保证吞吐量，安装AP时要保证蜂窝单元重叠，以牺牲覆盖范围(半径)来换取吞吐量的提高。

3. 扩展BSS

扩展BSS是由多个BSS经交换机和有线网络等互连而组成的，如图5.6所示。

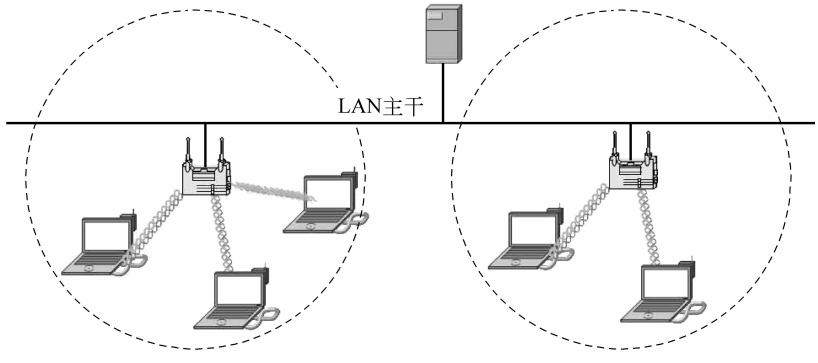

图5.6　扩展的BSS

一般来说，多个BSS常常通过有线骨干网连接，构成一个看起来像一个单独的逻辑LAN。

5.3.2 WLAN 通信原理

WLAN 中传输的帧分成以下几类：

- 数据帧：网络业务数据。
- 控制帧：使用请求发送、清除发送和确认信号控制对介质的访问，类似于调制解调器的模拟连接控制机制。
- 管理帧：类似于数据帧，与当前无线传输的控制有关。

其中只有数据帧与以太网的 802.3 帧相似，但以太网帧的大小不能超过 1518B，而无线网帧的大小可以达到 2346B。

无线站点可以通过两种方法选择 AP 进行数据帧转发：第一种方法是让无线站点主动发送探测帧扫描网络以寻找 AP，这种方法称为主动扫描；第二种方法是让 AP 定期发送一个宣告自己能力的信标帧，这些能力包括该 AP 支持的数据率，这种方法称为被动扫描。

主动扫描的工作过程如下。

(1) 无线站点发送探测帧。

(2) 所有接收到该探测帧的 AP 用探测响应帧来应答。

(3) 无线站点从中选择一个 AP，并向该 AP 发送一个关联请求帧。

(4) 选中的 AP 用关联响应帧来应答。

在被动扫描中，无线站点在接收到 AP 定期发出的信标帧后，只需要向该 AP 发回一个关联请求帧就可以完成站点与 AP 的关联。

5.3.3 WLAN 设计注意事项

设计 WLAN 需要考虑如下事项。

1. 站点测量

站点测量是为了确定所需 AP 的数量和部署位置。认为 AP 价格便宜，可以多多益善，不用进行站点测量，而使无线覆盖达到饱和，其实并不是经济有效的。为了最小化信道干扰，同时最大化覆盖范围，仍应该进行查勘，确定最理想的 AP 部署。

一些 AP 有自动配置选项，通过监听网络，可以使用最少的无线频道来自动完成配置。但这并不总是令人满意的。例如，在一个部署了多个 AP 的多层建筑物内，若在第 6 层安装了一个 AP，该 AP 可能选择一个它感觉可用的信道。如果这个信道已被第 1 层使用了，那么在第 3 层的无线客户端设备就很难保持连线，因为这里出现了信道覆盖的重叠。

在 WLAN 中，信道重叠就与在有线网中由于连续的冲突带来的后果一样，其性能必将受到影响，从而使无线客户端和 AP 之间不能保持持续的连通性。因此必须通过站点测量、AP 部署和信道规划来避免这个问题。①

进行站点测量时要考虑如下问题。

---

① 目前很多网络设备厂商提出了应对此问题的智能无线解决方案：由一个无线控制器来控制多个 AP，统一划分信道，动态规划覆盖范围，以避免信道重叠的问题。

（1）哪一种无线网络更适合企业应用？

（2）在天线之间是否存在可视距离的要求？

（3）为了使 AP 尽可能地靠近客户端设备，应该把 AP 部署在哪里？

（4）建筑物里存在哪些潜在的干扰源？例如，无绳电话、微波炉、天然的干扰或者使用相同信道的访问点。

（5）在部署时是否需要考虑法律法规限制？

2. WLAN 漫游

WLAN 与有线网络相比的最大优势就是可以便于客户端设备自由移动。前面已经介绍过，吞吐量与到 AP 的距离有关，因此设置 AP 时还要考虑用户的漫游范围。

此外，当一个用户离开 AP 时信号强度会减弱，此时连接应该无缝地跳到另一个有较强信号的 AP。

3. 点到点网桥

通常两个建筑物网络互连采用有线网络方式连接居多，如使用光缆、交换机等连接两个建筑物的 LAN 汇聚成一个 3 层广播域。但在有些情况下可能无法进行有线连接，如果此时两个建筑物距离合适并且直接相互可视，那么可以采用无线网桥进行连接，如图 5.7 所示。

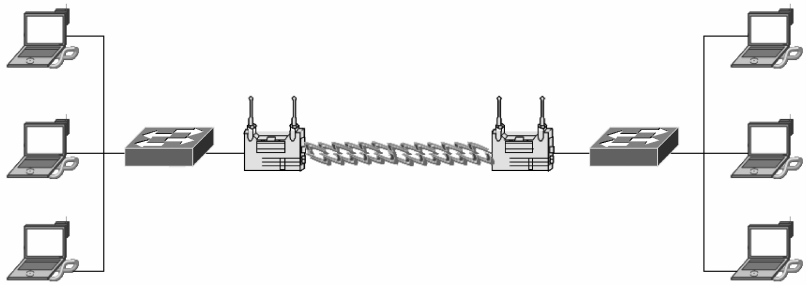

图 5.7　点到点网桥连接

此时，两个 AP 作为一个两端口的逻辑网桥发挥作用，AP 运行在点到点模式下，因此不能再作为无线访问点使用。这种点到点桥接方式可以在没有条件部署有线网络的情况下，作为近距离连接的一种解决方案。

5.4　无线局域网安全

虽然 IEEE 802.11 标准最初包括安全性，但很快就显得不够用了。无线安全问题或缺乏有效的安全管理机制往往是用户不愿意采用 WLAN 的主要原因。因此，在 WLAN 设计中，要根据用户需要考虑不同的安全措施。

WLAN 安全的最大风险就是未经授权就访问网络的业务数据，即查看、显示和记录网络业务数据，又称嗅包。会造成此问题的隐患包括两种：无线窃听和 AP 骗子。在有线网络中，黑客需要物理上处在企业建筑物的内部，通过网络漏洞获取访问权限。而在无线网中，入侵者可以从企业建筑物的外部访问网络。入侵者如果获得无线网访问权限后，

轻则盗用网络带宽,重则盗取资料,危及计算机安全。AP 骗子是指黑客在网络中接入未经授权的 AP。

解决上述安全问题的途径就是使用更安全的无线网协议和网络安全管理策略。具体可以分成以下几类:基本无线安全、增强无线安全、无线入侵检测和管理策略。

5.4.1 基本无线安全

基本无线安全提供的内置功能包括服务组标识符(Service Set Identifier,SSID)、有线等效加密(Wired Equivalent Privacy,WEP)和 MAC 地址验证。

1. SSID

SSID 是识别 AP 的代码,用来区分不同的网络,最多可以有 32 个字符。WLAN 上所有需要与 AP 建立连接的无线设备,都必须使用与 AP 相同的 SSID,无线网卡设置了不同的 SSID 就可以进入不同的网络。

SSID 通常由 AP 广播出来,默认情况下,AP 每隔几秒就广播一次自己的 SSID,主机通过扫描可以相看当前区域内的 SSID。这个广播也可以被停止,因此出于安全考虑可以不广播 SSID,此时用户就要手工设置 SSID 才能进入相应的网络。这样黑客就不能自动地发现 SSID 和 AP。然而,因为每个无线帧的信标中都含有 SSID,所以黑客通过嗅包工具可以很容易地发现 SSID,并且通过欺骗加入网络。

2. WEP

WEP 通过对无线客户端和 AP 之间的流量实施加密可以缓解 SSID 广播问题。使用 WEP 加入无线网称为共享密钥认证,WEP 向无线客户端发送一个“挑战”信息,客户端必须对信息进行加密后回复。如果 AP 可以破译客户端的响应,则 AP 证明客户端拥有合法密钥,因而有权访问无线网。WEP 支持两种加密长度:64 位和 128 位。

然而,WEP 仍然是不安全的:黑客可以首先获取“挑战”信息,然后对加密的响应信息使用逆向工程还原出客户端和 AP 使用的密钥。

3. MAC 地址验证

为了加强无线网的安全性,网络管理员可以使用 MAC 地址过滤功能,把被允许访问无线网的客户端的 MAC 地址配置在 AP 上。当然这种方法也不安全,通过对帧的监听可以发现合法的 MAC 地址,然后黑客就可以假冒这个地址进行访问。

5.4.2 增强型无线安全

在基本无线安全的基础上,还有一些更强壮的安全标准,以弥补一些安全弱点,具体如表 5.2 所示。

表 5.2 无线网安全标准

安全组件	802.11 原始标准	安全增强特性
认证	开放式认证或共享密钥	802.1x
加密	WEP	首先是 WPA,然后是 802.11i 和 802.11n

1. IEEE 802.1x

IEEE 802.1x是一种基于端口的网络访问控制标准，它提供逐个用户、逐个会话和两方强认证机制。如果需要的话，不仅可以用于无线网络，而且还可以用于有线网络。

IEEE 802.1x也可以提供加密，但这取决于认证方法。基于IEEE扩展授权协议(Extensible Authentication Protocol，EAP)，802.1x允许WAP和客户端自动地共享和交换WEP加密密钥。访问点作为代理，承担巨大的加密运算工作量。802.1x标准还支持面向WLAN的集中式密钥管理。

2. 无线保护访问

在IEEE 802.11i标准将要被批准的时候，无线保护访问(Wi-Fi Protected Access，WPA)成为WEP加密和数据完整性不安全的一个中间解决方案。

如果实现了WPA功能，那么只有知道正确密钥的客户端才可以访问AP。虽然WPA比WEP更安全，但是如果共享密钥存储在客户端上而客户端又被偷窃了，那么黑客就可以访问无线网络。

WPA支持认证和加密。通过共享密钥实现的认证称为WPA个人认证。而通过802.1x实现的认证称为WPA企业认证。WPA提供临时密钥完整性协议(Temporal Key Integrity Protocol，TKIP)作为加密算法，还提供另一个新的完整性算法(称为Michael)。WPA是802.11i规范的一个子集。

3. IEEE 802.11i

2004年6月，IEEE批准了802.11i标准的草案，又称为WPA2。从此，802.11i正式取代WEP和最初的802.11标准的其他安全特性。

WPA2是兼容802.11i标准的无线设备的产品证明。WPA2提供对附加强制性802.11i安全特性的支持，而WPA则不包含这些特性。与WPA一样，WPA2也支持企业和个人认证模式。除了要求更严格的加密外，WPA2还增强了对无线客户端快速漫游的支持，允许客户端在保持与即将离开的访问点连接的同时与将要去往的访问点预先完成认证。

4. IEEE 802.11n

IEEE 802.11n是新一代Wi-Fi标准，全面兼容802.11b和802.11g。802.11n扩展了传输范围，可以提供更高速接入，继承了WPA2的优点和缺点，而且配置选项多，配置复杂。

5.4.3　无线入侵检测和管理

很多产品能提供对假冒AP的检测，定期查找非法接入AP也是无线网管理的重要内容。例如，使用专业软件Airmagnet Laptop不但可以查找存在的非法AP，更能定位非法设备的物理位置，并且能够将捕捉到的数据包保存，用免费的Ethereal协议分析软件就能够对无线网络进行更为深入细致的分析。此外WLAN的管理任务还包括RF管理服务、干扰检测、协助站点测量、RF扫描和监控。

5.5 其他无线网标准

除 IEEE 802.11 系列的 WLAN 标准外,还有一些其他的无线通信标准,如 HomeRF 标准、蓝牙技术和 IrDA 红外技术。

5.5.1 HomeRF

HomeRF(家庭无线工作组)是专门为家庭用户设计的一种 WLAN 技术标准,希望实现个人计算机与家用电子设备之间的通信,如电话、传真机和电视等。HomeRF 既可以通过时分复用支持语音通信,又能通过 CSMA/CA 协议提供数据通信服务。同时,HomeRF 提供了与 TCP/IP 良好的集成,支持广播和多播。HomeRF 工作在 2.4GHz 频段上,最大传输速率为 2Mb/s,传输范围超过 100m。但是与 Wi-Fi 相比,HomeRF 已丧失技术优势,正在逐渐消失。

5.5.2 蓝牙技术

蓝牙技术(BlueTooth)是一种用于各种固定与移动的数字化硬件设备之间的低成本、近距离的无线通信连接技术。这种连接是稳定的、无缝的,能够非常广泛地应用于日常生活中。

蓝牙技术首先由瑞典爱立信(Ericsson)公司发明。1998 年,成立了蓝牙 SIG(Special Interest Group)组织,该组织负责创立发展蓝牙技术标准。蓝牙工作于 ISM 的 2.4GHz 频带上,采用跳频扩展技术(FHSS),最高传输速率为 1Mb/s。与其他工作在 2.4GHz 频段上的系统相比,蓝牙跳频更快,数据包更短,这使得蓝牙比其他系统都更稳定。

通信时,多个蓝牙设备之间建立 Ad Hoc 网络,并提供自动同步功能。蓝牙技术的优势在于 30 英尺的短距离内,能去掉两个固定或移动设备之间的线缆,为数据和语音通信提供便利。

5.5.3 IrDA

IrDA(Infrared Data Association,红外线数据标准协会)成立于 1993 年,是非营利性组织,负责建立红外无线通信的国际标准,目前在全世界拥有 160 多个会员,参与的厂商包括计算机及通信硬件、软件及电信公司等。简单地讲,IrDA 是一种利用红外线进行点对点通信的技术,其相应的软件和硬件技术都已经比较成熟。它的主要优点如下。

(1) 体积小,功率低,适合移动设备的需要。

(2) 传输速率高,可达 16Mb/s。

(3) 成本低。

(4) 应用普遍。

目前有 95%以上的笔记本电脑配备了 IrDA 接口,市场上还有可以通过 USB 端口与计算机相连的 USB-IrDA 设备。IrDA 标准也在不断发展中,传输速率由最初 FIR (FastInfrared)标准的 4Mb/s 提高到最新标准 VFIR 的 16Mb/s,接收角度由传统的 30°