

无线局域网技术白皮书

目录

第 1 章、前言	4
第 2 章、无线网络概述.....	4
1. 无线网络概述.....	4
2. 无线网络的特点	4
3. 无线数据网络种类	6
第 3 章、无线局域网.....	6
1. 无线局域网（WLAN）概述	6
2. 无线局域网的益处.....	9
3. 典型的无线局域网应用	10
第 4 章、无线局域网技术	11
1. 无线局域网标准概述.....	11
802.11a 标准.....	11
802.11g 标准.....	12
802.11 系列新标准.....	14
2 无线局域网标准进展	15
3. 三种流行无线网络技术的比较.....	15
4. 下一代无线网络技术：HIPERLAN/2	17
5. 无线局域网频道分配与调制技术	22
6. 无线局域网拓扑结构.....	23

7. 无线局域网的几个主要工作过程	24
8. 影响无线局域网性能的因素	25
9. 无线局域网络的安全性.....	25
1. 无线局域网 (WLAN) 面临哪些威胁?	25
2. 常见的无线网络安全分类.....	25
3. 如何保障无线局域网安全.....	26
4. 保护企业无线网络.....	27
第 5 章、无线局域网络产品的兼容性.....	28
第 6 章、CISCO 无线局域网络解决方案	28
1. 思科无线局域网技术指南	28
下一代无线局域网.....	28
无线技术的到来.....	28
无线移植方案的选择.....	29
802.11a 标准.....	29
802.11g 标准.....	30
兼容性.....	30
双频 Cisco Aironet 1200: 全球最佳.....	30
今天的无线应用.....	30
计算的新纪元.....	31
2. 思科无线安全解决方案指南.....	31
第 8 章、CISCO AIRONET 扩频无线网络产品	39
一、扩频收发工作站.....	39
二、扩频天线馈线系统.....	44
第 9 章、无线网络典型联接方式与实例	45
一、CISCO AIRONET	46
二、其它无线网案例.....	48
第 10 章、无线联网的现状与发展前景	49
一、无线网络的需求及实现.....	49
二、计算机无线网络的应用现状.....	50
三、计算机无线网络目前存在的问题和解决.....	50
四、计算机无线网络的标准化.....	51
五、计算机无线网络的发展与应用的前景.....	51
第 11 章、计算机无线网技术应用介绍	51

一、计算机无线网技术适用范围:51

二、应用介绍.....52

第 12 章、总结54

第八章、无线网络产品选购指南54

附录一、无线局域网常用品牌及产品简介56

附录一、AIRONET 无线网产品安全性说明60

附录二、国家无线电委员会对 2.4GHZ 频段的管理办法60

附录三、AIRONET 无线网产品参考报价（部分）62

第 1 章、前言

信息革命到今天，我们越来越离不开计算机网络，无论是信息共享、合作伙伴交流、还是移动用户办公，都有网络价值的体现。网络已经渗透到了个人、企业以及运营商。现在的网络建设已经发展到无所不在，不论你在任何时间、任何地点都可以轻松上网。网络无所不在其实并不简单，光靠光纤、铜缆是不够的，毕竟在许多场合不允许铺设线缆。因此，需要推广一种新的解决方案，使得网络的无所不在能够得以实现。这种解决方案就是无线数据网络。

第 2 章、无线网络概述

1. 无线网络概述

无线网络由于无需借助电缆和光缆即可实现计算机之间的通讯，因此，已经被广泛应用于无法铺设线缆、不便铺设线缆或需要频繁移动的场合。利用无线网络的这一特点，也可以使用户迅速建立 Internet 连接。

无线网络不仅可以用于连接局域网络，而且还可以直接连接至 Internet，用户甚至可以借助 Internet 及其他公用通信网络建立自己的虚拟专网，实现网络之间的互联。无线网络可以提供的带宽高达 11Mbit/s，比 ADSL 还要快，无疑是 Internet 宽带接入的又一理想选择。

无线网络标准采用 CSMA/CA（带有回避冲突的载波侦听多路存取）的 MAC 方式，同时 IEEE802.11 标准还提供漫游功能等多方面优势，允许一台客户机在多个无线子网中漫游，同时还可以工作承同一或不同的信道中，从而使得无线网络终端如同手机一样能在各网间进行漫游。为了能够实现多个供应商产品之间的漫游，多家公司合作开发了“接入点互连协议”（IAPP，Inter Access Point Protocol）规范，以实现多家产品的互通、互联、互相兼容，使得漫游能够在不同厂商提供产品的网络间平滑地实现。

2. 无线网络的特点

下面我们将从**传输方式**、**网络拓扑**、**网络接口**等几个方面来描述无线网的特点。

一、传输方式

传输方式涉及无线网采用的传输媒体、选择的频段及调制方式。

目前无线网采用的传输媒体主要有两种，即无线电波与红外线。在采用无线电波做为传输媒体的无线网依调制方式不同，又可分为扩展频谱方式与窄带调制方式。

1、扩展频谱方式

在扩展频谱方式展频谱方式中，数据基带信号的频谱被扩展至几倍-几十倍后再被搬移至射频发射出去。这一作法虽然牺牲了频带带宽，却提高了通信系统的抗干扰能力和安全性。由于单位频带内的功率降低，对其它电子设备的干扰也减小了。

采用扩展频谱方式的无线局域网一般选择所谓 ISM 频段，这里 ISM 分别取于 Industrial、Scientific 及 Medical 的第一个字母。许多工业、科研和医疗设备辐射的能量集中于该频段，例如美国 ISM 频段由 902MHz-928MHz，2.4GHz-2.48GHz，5.725GHz-5.850GHz 三个频段组成。如果发射功率及带宽辐射满足美国联邦通信委员会（FCC）的要求，则无须向 FCC 提出专门的申请即可使用 ISM 频段。

2、窄带调制方式

在窄带调制方式中，数据基带信号的频谱不做任何扩展即被直接搬移到射频发射出去。

与扩展频谱方式相比，窄带调制方式占用频带少，频带利用率高。采用窄带调制方式的无线局域网一般选用专用频段，需要经过国家无线电管理部门的许可方可使用。当然，也可选用 **ISM** 频段，这样可免去向无线电管理委员会申请。但带来的问题是，当临近的仪器设备或通信设备也在使用这一频段时，会严重影响通信质量，通信的可靠性无法得到保障。

3、红外线方式

基于红外线的传输技术最近几年有了很大发展。目前广泛使用的家电遥控器几乎都是采用红外线传输技术。做为无线局域网的传输方式，红外线的最大优点是这种传输方式不受无线电干扰，且红外线的使用不受国家无线电管理委员会的限制。然而，红外线对非透明物体的透过性极差，这导致传输距离受限。

二、网络拓扑

无线局域网的拓扑结构可归结为两类：无中心或对等式（**Peer to Peer**）拓扑和有中心（**HUB-Based**）拓扑。

1、无中心拓扑

无中心拓扑的网络要求网中任意两个站点均可直接通信。

采用这种拓扑结构的网络一般是用公用广播信道，各站点都可竞争公用信道，而信道接入控制（**MAC**）协议大多采用 **CSMA**（载波监测多址接入）类型的多址接入协议。

这种结构的优点是网络抗毁性好、建网容易、且费用较低。但当网中用户数（站点数）过多时，信道竞争成为限制网络性能的要害。并且为了满足任意两个站点可直接通信，网络中站点布局受环境限制较大。因此这种拓扑结构适用于用户相对减少的工作群网络规模。

2、有中心拓扑

在中心拓扑结构中，要求一个无线站点充当中心站，所有站点对网络的访问均由其控制。

这样，当网络业务量增大时网络吞吐性能及网络时延性能的而恶化并不剧烈。由于每个站点只需在中心站覆盖范围之内就可与其它站点通信，故网络中点站布局受环境限制亦小。此外，中心站为接入有线主干网提供了一个逻辑接入点。

有中心网络拓扑结构的弱点是抗毁性差，中心点的故障容易导致整个网络瘫痪，并且中心站点的引入增加了网络成本。

在实际应用中，无线网往往与有线主干网络结合起来使用。这时，中心站点充当无线网与有线主干网的转接器。

三、网络接口

这涉及无线网中站点从哪一层接入网络系统。一般来讲，网络接口可以选择在 **OSI** 参

考模型的物理层或数据链路层。

所谓物理层接口指使用无线信道替代通常的有线信道，而物理层以上各层不变。这样做的最大优点是上层的网络操作系统及相应的驱动程序可不做任何修改。这种接口方式在使用时一般做为有线网的集线器和无线转发器以实现有线局域网间互连或扩大有线局域网的覆盖面积。

另一种接口方法是从数据链路层接入网络。这种接口方法并不沿用有线局域网的 **MCA** 协议，而采用更适合无线传输环境的 **MAC** 协议。在实现时，**MAC** 层及其以下层对上层是透明的，配置相应的驱动程序来完成域上层的接口，这样可保证现有的有线局域网操作系统或应用软件可在无线局域网上正常运转。

目前，大部分无线局域网厂商都采用数据链路层接口方法。

3. 无线数据网络种类

无线数据网络解决方案包括：无线个人网（**WPAN**）、无线局域网（**WLAN**）、无线 LAN-to-LAN 网桥、无线城域网（**WMAN**）和无线广域网（**WWAN**）。

无线个人网：主要用于个人用户工作空间，典型距离覆盖几米，可以与计算机同步传输文件，访问本地外围设备，如打印机等。目前主要技术包括蓝牙（**Bluetooth**）和红外（**IrDA**）。

无线局域网：主要用于宽带家庭、大楼内部以及园区内部，典型距离覆盖几十米至上百米。目前主要技术为 802.11 系列。

无线 LAN-to-LAN 网桥：主要用于大楼之间的联网通讯，典型距离几公里。许多无线网桥采用 802.11b 技术。

无线城域网和广域网：覆盖城域和广域环境，主要用于 **Internet/email** 访问，但提供的带宽比无线局域网技术要低很多。

各种无线数据网络技术的比较见下表：

第 3 章、无线局域网络

1. 无线局域网（WLAN）概述

无线局域网或者 **WLAN** 是利用无线信号而不是有线线缆连接客户设备和无线集线器的一种以太网（**ethernet-based network**）。无线集线器也称“访问点”是连接无线客户设备到有线网络的桥梁。访问点和无线集线器之间的通信遵循 IEEE802.11 无线以太网标准，该标准使用 WEP 协议（**Wired Equivalent Privacy**，有线对等私有协议）支持基本的验证和加密。

什么是无线局域网？

最简单地讲，无线局域网（**WLAN**）正如其名称所说的那样，可以提供传统 LAN 技术（如以太网和令牌网）和所有功能和好处，但不会受到线缆的限制。但是仅从不需要线缆这一角度来看待 **WLAN** 则是没有抓住其本质：**WLAN** 使我们重新定义对 LAN 的看法。连通性不再仅仅意味着连接。局域的概念不再以英尺或

米来度量，而是以英里或公里来度量。系统的基础结构不再需要埋在地下或藏在墙里，它可以是移动性的，也可以随组织的成长发生变化。这一技术可以立即被应用于一些领域。包括：

- 希望在企业内部获得传统有线网络之外的移动功能的 IT 专业人士或高级商业管理人员。
- 需要能够在整个站点内或选定的区域内灵活且频繁地改变 LAN 布线的公司所有者和 IT 董事。
- 任何其地点因建筑物或预算的限制（如建筑物是老旧的、空间是租赁性的或地点是临时性的）而不适于使用 LAN 布线的公司。
- 任何需要视野内建筑物到建筑物桥接设备所能提供的灵活性和成本节省的公司，这些公司可以通过这些设备避免昂贵的挖沟布线、线路租赁或走线问题。

目前的纵向市场包括：

- 培训
- 金融
- 系统健康照管
- 促销和零售
- 制造和生产

WLAN 使用的传输手段与有线 LAN 不一样。WLAN 不是使用双绞线或光纤，它使用的是红外线（IR）或射频（RF）。在这两者之中，RF 因其作用距离长、带宽大及覆盖范围更广而更加受到欢迎。今天的大多数无线 LAN 都在使用 2.4 千兆赫（GHz）的频率波段，这是世界范围内 RF 频谱中为非许可保留的唯一波段。无线网络的自由性和灵活性既可用于建筑物内部也可用于建筑物之间。

建筑物内 WLAN

WLAN 技术可以替代传统的有线网络，还可以对其可达范围和功能进行扩展。与有线 LAN 非常相似的是，建筑物内 WLAN 设备也是由 PC 卡、个人计算机接口（PCI）、产业标准结构（ISA）客户机适配器以及接入点组成的¹，接入点所执行的功能与有线网络中的集线器类似。与有线 LAN 的小型安装或临时安装类似，WLAN 可以在仅使用客户机适配器的点对点拓扑或临时拓扑²中使用。

为实现更多的功能和获得更大的作用范围，可以插入接入点并将其作为星型拓扑的中心，还可以将其作为与以太网连接的桥接设备。

在建筑物内部，无线功能既可支持移动计算，也可支持连接计算。通过安装在笔记本电脑或手持 PC 上的 PC 卡客户机适配器，用户可以在整个设施内自由移动，同时维持对网络的访问能力。

将无线 LAN 技术应用于桌面系统可以为一个组织提供传统 LAN 所不能提供的灵活性。桌面客户机系统可以被放置在不可能进行或不适于进行布线的地方。桌面 PC 可以根据需要在设施内的任何地方进行重新部署，这一特性使无线方案成为临时工作组或快速成长组织的理想选择。

建筑物到建筑物的 WLAN

商业无线电信号在任何天气下都可以在距离发射器数英里之遥的地方接收，WLAN 利用无线电波的方式与此非常类似，正是通过这一方式 WLAN 重新定义了 LAN 的“局域”概念。通过无线桥接设备，相距数英里的建筑物中的网络可以被集成为一个单一的局域网。当使用传统的铜线或光纤连接建筑物时，公路、湖泊甚至当地政府都有可能成为不可逾越的障碍。一个无线网桥就可以使这些东西统统变得不相干，它可以通过空气传输数据，无需获得许可，也无所谓正确的走线。

如果没有无线方案，组织将不得不频繁求助于广域网技术以实现分离的局域网之间的连接。通过与本地电话供应商签订合同来获得租赁线路将带来很多问题。一般情况下安装会很昂贵，而且几乎不可能很快使用。带宽的月租费常常很高，而这样的带宽以 LAN 的标准来衡量又很低。一个无线网桥可在一个下午的时间里购买和安装完毕，其费用一般仅相当于单独的 T1 安装费用。一旦投资完成，将不再需要承担重复性费用。而且，今天的无线网桥所提供的带宽技术植根于数据而非语音、通信。

无线 LAN 标准

在有线世界里，以太网已经成为主流的 LAN 技术，其发展不仅与无线 LAN 标准的发展并行，而且也确实预示了后者的发展方向。通过电气和电子研究所（IEEE）802.3 标准的定义，以太网提供了一个不断

发展、高速、应用广泛且具备互操作特性的网络标准。这一标准还在继续发展，以跟上现代 LAN 在数据传输速率和吞吐量方面要求。以太网标准最初仅提供 10 兆位/秒 (Mbps) 的数据传输速率，现在已经发展成为可以提供网络主干和带宽密集型应用所要求的 100 兆位/秒的数据传输速率。IEEE 802.3 标准是开放性的，减少了市场进入的障碍，并导致了大量可供以太网用户选择的供应商、产品 and 价值点的产生。最重要的是，只要符合以太网标准就可以实现到操作性，从而使用户能够选择多个供应商提供的一种产品，同时确保这些产品能够共同使用。

第一代无线 LAN 技术是低速的 (1-2 兆位/秒) 专有产品提供。尽管有这些缺点，无线所带来的自由性和灵活性还是在纵向市场上为这些早期产品占据了一席之地，如零售业和仓储业，这些行业的移动工人使用手持设备进行存货管理和数据采集。随后，医院使用无线技术将病人的信息直接传送到病床边。随着计算机进入课堂，学校和大学开始安装无线网络，以避免布线成本和共享 Internet 接入。打头阵的无线供应商不久就认识到，为使这一技术获得市场的广泛接受，需要建立一种类似以太网的标准。供应商们在 1991 年联合到一起，第一次建议并随后建立了一个基于各自技术的标准。1997 年 6 月，IEEE 发布了用于无线局域网的 802.11 标准。

正象 802.3 标准允许数据通过双绞线和同轴电缆进行传输一样，802.11 WLAN 标准允许通过不同的介质进行数据传输。可以使用的介质包括红外线和两种在无需获得许可的 2.4 千兆赫频段上的无线电传输：跳频扩频 (FHSS) 和直序扩频 (DSSS)。传播频谱是 40 年代开发的一种调制技术，可以在一个很宽的无线电频率波段内传播信号。这一技术是数据通信的理想选择，因为它对无线电干扰不很敏感，而且几乎不产生干扰。FHSS 受限于 2 兆位/秒的数据传输速率，仅推荐在非常特殊的应用如某些类型的水运工具中使用。对于其它所有的无线 LAN 应用，DSSS 是更好的选择。最近发布的 IEEE 演化版本 802.11b 可以通过 DSSS 提供与以太网相当的 11 兆位/秒的数据传输速率。FHSS 不支持 2 兆位/秒以上的数据传输速率。

无线局域网的未来

有线 LAN 的技术发展历史可用一句话来概括，“更快、更好、更便宜”。无线 LAN 技术已经开始沿着同一道路发展：数据传输速率从 1 兆位/秒增加到 11 兆位/秒，随着 IEEE 802.11b 标准的出现互操作性已经成为事实，而且价格已经大大降低。改进在目前看来还只是刚刚开始。

性能

IEEE 802.11b 标准的 11 兆位/秒 WLAN 工作在 2.4 千兆赫兹频段，这一频段还有增加带宽的空间。使用 802.11b 规格中所包含的光调制技术，可以将目前的数据传输速率提高一倍。Cisco 已经将 22 兆位/秒的数据传输速率列入将来的发展计划。无线 LAN 制造商从 900 兆赫波段转换到 2.4 千兆赫波段，以提高数据传输速率。这一模式还将继续发展下去，在 5 千兆赫波段将出现能够支持更大带宽的更宽的频率波段。IEEE 已经发布了一个针对工作在 5 千兆赫波段、可支持 54 兆位/秒数据传输速率的设备的技术规格 (802.11a)。这一代技术在 2001 年的某个时候进入市场时将很可能获得很大利润。与典型情况一样，这一利润将随时间减少，而数据传输速率将增加：5.7 千兆赫波段有望将数据传输速率提高一个新的突破性的水平—100 兆位/秒。在性能毫无疑问地将继续得到提高的同时，客户们将继续要求获得可靠的合作伙伴，以将这些动态发展的技术无缝地集成入现有的网络之中。Cisco 能够提供实现这类集成所需的稳定性和网络专业知识。

安全性

802.11 标准中与有线系统相当的保密性 (WEP) 选项只是满足客户安全需要的第一步。Cisco 能够提供目前无线网络可以达到的最高级别的安全性，可以提供 128 位加密功能，并可支持 802.11 标准的加密和身份验证选项。按照标准中的规定，Cisco 使用了具有 40 或 128 位密钥的 RC4 算法。当实现 WEP 支持时，每个台站 (客户机和接入点) 最多可以有 4 个密钥。密钥用于在使用无线电波对数据进行传输之前对其进行加密。如果一个台站接收的数据包没有经过适当密钥的加密，该数据包将被丢弃，永远也不会被发送到主机上。

尽管 802.11 为确保 WLAN 的安全性而提供了强大的加密服务，但安全密钥的授权、取消和更新方法还没有被定义。幸运的是，在企业中可以采用一些关键的管理结构。大型网络的最佳方式是集中的密钥管理，

这一方式使用集中的加密密钥服务器。Cisco 目前的战略包括了添加加密密钥服务器，确保有价值的数据可以得到保护。加密密钥服务器可以提供集中的密钥生成、密钥的分配以及进行中密钥循环功能。密钥服务器使网络管理员能够在客户级别上命令 RSA 公共/私有密钥的生成，这一功能是客户身份鉴定所必需的。Cisco 密钥服务器还将为客户提供数据包加密所需要的 RC4 密钥的生成和分配功能。这一工具简化了管理并有助于避免机密密钥的损坏。Cisco 将继续提高安全尺度，以确保贯穿企业网络的最好的安全保护。

移动服务

WLAN 的主要优点是移动性，但目前在其管理信息库（MIB）中还没有针对移动设备的跟踪和管理的产业标准。这一遗漏使用户不能在覆盖一个公共区域（如一座建筑物的完整的一层）的无线接入点之间进行漫游。Cisco 已经解决了这一问题，提供了自己的移动算法，该算法便于在一个 IP 域（如一层楼）内进行漫游，同时注意了对跨 IP 域的漫游进行优化（如一个企业厂区）。

管理

无线接入点共享集线器和交换机的功能。与接入点关联的无线用户共享无线 LAN，其方式与集线器功能的共享类似，但是接入点还可以跟踪客户在自己的域的范围内的移动，并能够允许或拒绝特定的通信流或客户通过自己进行通信。对于希望利用这些优点的网络经理来说，能够象配置集线器或交换机那样对接入点进行配置是很必要的。

Cisco 的 WLAN 设备可以通过公共的 Telnet 或 SNMP（I 或 II）服务程序进行管理，一个 Web 浏览器可以为其进行监视和控制提供便利。除了桥接设备的统计信息和计数器，接入点还可以提供附加的功能以使其更加强大和易于管理，这些功能包括无线接入点和与其相关的客户的映射以及客户统计的监视和报告。通过介质访问控制（MAC）和协议级的访问列表，接入点还可以控制通过无线 LAN 的通信流的接入和流动。可以对配置参数和接入点的代码图象进行集中的配置和管理，以促进 WLAN 网络政策的一致性。

价格

不断下降的无线 LAN 设备价格开创了一个全新的市场。随着数量的持续增加，制造效率得到提高，成本下降，价格将进一步下跌。尽管无线客户机适配器的价格不太可能与有线的客户机适配器相提并论（已计入布线 and 人工成本），但价格上的差别将变得越来越不重要。

结论

今天，WLAN 已经对连接这一概念作出了重新的定义，它扩展了局域网的边界，并使基础结构可根据需要进行动态的改变。所有这些仅仅是开始：标准的制定只有三年，高速 802.11b 标准诞生不过一年。通过标准和可以实现互操作的产品，LAN 的规模可以达到有线基础结构所无法想象的程度。只需传统广域网技术成本的一部分，WLAN 就可以建立高速的互连。在无线世界中，用户不仅可以在校园内漫游，也可以在城市内漫游，同时保持与外部网、内部网和 Internet 的高速连接。无线局域网的将来从现在开始——从 Cisco 开始。

2. 无线局域网网络的益处

无线局域网可以作传统有线网络的延伸，在某些环境也可以替代传统的有线网络。对比于传统的有线网络，无线局域网的显著特点包括：

移动性：在大楼或园区内，局域网用户不管在任何地方都可以实时的访问信息。

安装的快速性和简单性：安装无线局域网系统即快速又简单，同时消除了穿墙或过天花板布线的繁琐工作。

安装的灵活性：无线技术可以使网络遍及有线所不能到达的地方。

减少投资：尽管无线局域网硬件的初始投资要比有线硬件高，但一方面无线网络减少了布线的费用，另一方面在需要频繁移动和变化的动态环境中，无线局域网的投资更有回报。

扩展能力：无线局域网可以组成多种拓扑结构，可以十分容易地从少数用户的对等网络

模式扩展到上千用户的结构化网络。

3. 典型的无线局域网应用

典型的无线局域网应用包括：医院、学校、金融服务、制造业、服务业、公司应用、公共访问等。

第 4 章、无线局域网技术

1. 无线局域网标准概述

无线通信的发展日新月异，从“蓝牙”到第三代移动通信，新技术层出不穷，尤其是无线局域网技术以比人们的预料快得多的速度向前发展着。过去，无线 LAN 仅限于工厂和仓库使用，现在已进入办公室、家庭，乃至其他公共场所

IEEE 802.11b 的用户在 2001 年初只是凤毛麟角，而现在已超过 1500 万，这个数字与蜂窝电话和有线以太网相比还显得太小，但增长速度却是扶摇直上。而且在 IEEE 802.11b 推出后，IEEE 又制定了 IEEE 802.11a 和 IEEE 802.11g，这两个标准的数据率比 IEEE 802.11b 高得多。这两个标准的出台以及其他标准的推出（见表 1），将推动无线 LAN 以更快的速度向前发展，并有可能对铜线和光纤网络构成威胁。

电气和电子工程师协会（IEEE）在 1999 年批准了 802.11b 标准，它可以提供最高每秒 11B 位（Mbps）的数据传输速率——近似于很多以太网工作小组所使用的 10-Mbps 连接。无线局域网首次开始适用于大部分工作环境和办公室应用。很多厂商随后立即开始支持 802.11b 标准——这迅速地降低了成本，带来了更多的需求和更加广泛的厂商支持。另外，802.11b 标准确保了用户可以获得设备互操作能力。无线以太网兼容性联盟（WECA）是一个非盈利性的国际组织，它的宗旨是检验基于 802.11b 标准的无线局域网产品的互操作能力，并在所有市场中推广该标准。随着 802.11b 标准的迅速普及，用户开始可以选择多种可互操作的、低成本的、高性能的无线设备。

可能最重要的是，各种类型的企业现在都可以通过将无线技术加入自己的企业局域网而获得巨大的利益。多年以来，膝上型电脑和笔记本电脑一直承诺可以随时随地进行计算。但是，随着对局域网和互联网的访问日益成为开展业务的不可或缺的组成部分，人们需要通过无线连接来真正实现随时随地进行计算的承诺。无线设备让用户几乎从任何地方都可以接入网络：办公桌、会议室、咖啡厅，或者企业园区和校园中的另外一个建筑物。这种能力为用户提供了最大限度的灵活性、生产率和效率，同时可以极大地促进同事、商业伙伴和客户之间的合作。此外，无线技术还可以为难以铺设电缆或者布线成本过高的场所提供局域网访问。

无线移植方案的选择

像其他任何技术一样，无线技术一直在不断地发展——提供更高的速度、带宽、安全性等。无线技术最近在技术上发展到了重要的转折点。

工作在不需许可的 2.4GHz 频段的 802.11b 标准是全球应用最广泛的无线标准，它可以提供最高 11Mbps 的数据传输速率。对于一部分企业来说，这样的速度已经足以满足他们目前的需求。但是其他企业仍然希望通过新一代的设备获得更高的吞吐量、访问速度和功能，以满足他们迅速增长的无线用户的需要。

无线厂商对这种需求做出了积极的响应。目前，IEEE 任务小组正在集中精力制定两项更高性能的标准——802.11a 和 802.11g。在移植到更高性能的无线技术的过程中，用户必须了解每种无线标准的优点和缺点，并在此基础上判断哪种技术或者哪些技术最符合他们自身的无线网络需求。

802.11a 标准

IEEE 于 1999 年批准了 802.11a 标准，但是直到 2001 年 12 月市场上才出现第一款兼容 802.11a 的产

品。802.11a 标准最高可以提供 54Mbps 的数据传输速率和 8 个不重叠的频率通道——从而可以增加网络容量，提高可扩展性，并能够在不干扰相邻单元的情况下创建微型单元式结构。802.11a 工作在不需申请的 5GHz 频段，因为不会受到来自于工作在 2.4GHz 频段的设备的干扰，例如微波炉、无绳电话和蓝牙（一种短距离、低速、点对点、个人局域网无线标准）设备。但是，802.11a 标准并不能与现有的支持 802.11b 的设备兼容。已经采用了 802.11b 设备，并希望获得 802.11a 技术所提供的更高通道数和网络速度的企业必须安装一整套全新的 802.11a 基础设施，以及 802.11a 接入点和客户端适配器。需要指出的是，2.4GHz 和 5GHz 设备可以在互不干扰的情况下在同一个物理环境下工作。

要在全球范围内普及 802.11a，一个重要的障碍是该标准尚未被全球各国的相关法规制定部门批准使用。到目前为止，802.11a 还未在欧洲获得批准；但是，IEEE 和欧洲通信标准委员会（ETSI）目前正在设法通过 IEEE 802.11h 任务小组达成一项协议，解决 802.11a 的电源问题和通道设置问题。

推广 802.11a 的另外一个障碍是缺乏对互操作性的认证。目前，各个厂商的产品之间的互操作性还没有保障。WECA 将为 802.11a 产品提供互操作性测试，并致力于进一步推广该技术。但是，只有在两家芯片厂商开始制造相应的芯片，并至少有三家厂商在这些芯片的基础上制造产品以后，WECA 才会开始进行这样的测试。WECA 期望认证工作将从 2002 年下半年开始。

802.11g 标准

802.11g 标准从 2001 年 11 月就开始草拟，但是预计到 2003 年之前不大可能最终完成。802.11g 可以提供与 802.11a 相同的 54Mbps 数据传输速率，但是它还可以提供一种重要的优势——对 802.11b 设备向后兼容。这意味着 802.11b 客户端卡可以与 802.11g 接入点配合使用，而 802.11g 客户端卡也可以与 802.11b 接入点配合使用。因为 802.11g 和 802.11b 都工作在不需许可的 2.4GHz 频段，所以对于那些已经采用了 802.11b 无线基础设施的企业来说，移植到 802.11g 将是一种合理的选择。需要指出的是，802.11b 产品无法“软件升级”到 802.11g，这是因为 802.11g 无线收发装置采用了一种与 802.11b 不同的芯片组，以提供更高的数据传输速率。但是，就像以太网和快速以太网的关系一样，802.11g 产品可以在同一个网络中与 802.11b 产品结合使用。由于 802.11g 与 802.11b 工作在同一个无需申请的频段，所以它需要共享三个相同的频段，这将会限制无线容量和可扩展性。

兼容性

802.11a 和 802.11g 都可以大幅度地改进现有的 802.11b 标准，因为它们所带来的更高的数据传输速率可以为无线局域网上的设备提供更高的性能和可用性。但是一个不足之处是由于 802.11a 和 802.11g 标准使用的频段不同，所以不能相互兼容。而且，802.11a 不能与现有的 802.11b 设备兼容。

802.11a 优于 802.11b

IEEE 802.11b 于 2000 年推出，它采用直接序列扩频(DSSS)，其技术比较简单。IEEE 802.11a 在 2001 年到 2002 年推出，它采用较为复杂的正交频分复用(OFDM)技术。技术越复杂，数据率越高。IEEE 802.11b 的数据率为 11Mbps（物理层额外开销使数据率下降 40%，实际数据率最多为 6Mbps），而 IEEE 802.11a 的数据率却高达 54Mbps。

所有的无线 LAN 都使用未注册频谱，因此，它们易受干扰，并引起传输出错。当传输出现差错时，所传输的信息必须重发，势必浪费带宽。如果差错率达到 50%，则会使数据率减少三分之二。就 802.11b 而言，6Mbps 的实际数据率减去差错重发开销后只剩下 2Mbps，在网络上只能实现每个节点共享的半双工通信。

表 1 现有和未来的无线 lan 标准

无线 lan 系统	物理层数据率	实际数据率	最大传输距离	频率	qos	推出时间
802.11b	11mbps	6mbps	100 米	2.4ghz	无	2000 年
802.11a	54mbps	31mbps	80 米	5ghz	无	2001 年
802.11g	54mbps	12mbps	150 米	5ghz	无	2002 年底
homeRF2	10mbps	6mbps	50 米	2.4ghz	有	现在
hiperlan2	54mbps	31mbps	80 米	5ghz	有	2003 年
5-up	108mbps	72mbps	80 米	5ghz	有	2003 年

802.11a 除数据率较高外，它还使用 5GHz 的较高频段，而 802.11b 则使用 2.4GHz 频段，而且与无绳电话、微波炉和“蓝牙”等装置共用这一频段。从频宽和频谱拥挤角度看，802.11a 优于 802.11b，因为频段较宽，意味着更多的无线信道可以在无干扰的环境下共存。每个无线信道相当于一个独立的网络，或同一个网上的一个交换式分系统，而且把两个 802.11a 信道整合在一起，可使数据率倍增。

尽管 5GHz 频段有许多优点，但也存在一些问题，其中最主要的问题是兼容性，即频率不同意味着 802.11a 的产品不能与 802.11b 的互通。为了解决这个问题，IEEE 制定出了 802.11g，该标准将提高 802.11b 的数据率，并增大传输距离，以使它与 802.11a 兼容。但由于受干扰的影响，目前 802.11g 的传输速度还是不如 802.11a 快，因此，该标准要推迟到 2002 年秋季才能出台。

802.11g 增大传输距离

大多数 802.11b 网络的传输距离能够达到 100 米，但这只是粗略估算，功率较高的发射机可以扩大传输距离，而干扰和信号阻塞有可能减少传输距离。由于无线 LAN 是用在室内环境中，安全要求、墙壁阻挡和其他信号干扰，都可能限制传输距离。

在任何一种无线系统中，频率越高，传输信号被大气或其他物体吸收的可能性就越大。这就使得大多数人以为 802.11a 的覆盖范围比 802.11b 小。据测试，实际情况并不是这样。例如，据美国一家公司测试显示，当在典型的办公环境应用时，802.11a 在每一种测试距离上都能提供较高的数据率，其原因是采用 OFDM 技术能够抗多径干扰，从而使传输距离与 802.11b 相当。

802.11g 与 802.11a 一样也采用 OFDM 技术，但使用的频段与 802.11b 相同(2.4GHz)，因而其传输距离更远。由于 802.11g 是新标准，还没有人实际测试过采用该标准的无线系统；但如果在 2.4GHz 频段实现 OFDM 技术，其传输距离要比 802.11a 和 802.11b 增大 50%。而且，与任何其他系统相比，802.11g 的接入点少一半，而覆盖范围却相同，因此，802.11g 的覆盖能力可能是其长期的最大的销售点。

802.11g 由于接入点比其他系统少，用在用户较少、覆盖密度较低，或用户不要求高速连接的地方如仓库、货栈等，不失为最佳选择。在人员拥挤的地方，如会议中心、机场等地，要求覆盖密度最高，最终将向 802.11a 看齐。

802.11 系列新标准

尽管 802.11b 是最流行的无线 LAN 标准，但安全性较差，且不支持 QoS，802.11a 和 802.11g 也尚有不足之处。因此，除 802.11b 、802.11a 和 802.11g 这 3 个主要的无线 LAN 标准外，IEEE 还在制定一系列新的标准，使之更加完善(见表 2)。

表 2 ieee 新的标准系列	
标准名称	主要内容
802.11d	旨在制定在其他频率上工作的多个 802.11b 版本，使之适合于世界上现在还未使用 2.4ghz 频段的国家。
802.11e	该标准将对 802.11 网络增加 qos 能力，它将用时分多址（tdma）方案取代类似以太网的 mac 层，并对重要的业务
	增加额外的纠错功能。
802.11f	该标准旨在改进 802.11 的切换机制，以使用户能够在两个不同的交换分区(无线信道)之间，或在加到 2 个不同的网络上
	的接入点之间漫游的同时保持连接。
802.11h	该标准意在对 802.11a 的传输功率和无线信道选择增加更好的控制功能，它与 802.11e 相结合，适用于欧洲地区。
802.11i	该标准消除 802.11 的最明显的缺陷：安全问题。除 wep 外，它将是基于高级加密标准(aes)，即美国政府“官方”
	加密算法的一个完整的新标准。
802.11j	这是个新的标准，目前只是一个草案，尚未组成特别工作组进行讨论。预计，该标准将使 802.11a 和 hipervlan2 这两
	个标准在同一频率共存。

就最为突出的安全而言，目前，所有的 802.11b 产品都采用“有线等效保密”系统，用 40 位长的密钥给所有的传输信号加密。有些新产品采用 WEP2 加密系统，IEEE 将该系统重新命名为临时密钥完整性协议(TKIP)。该协议使用 128 位密钥，且完全与 WEP 兼容。使用 WEP 的用户都使用相同的密钥；如果一台机器被盗，将殃及整个网络，而且容易受“黑客”的攻击。WEP2 同样易受“黑客”的攻击，因为它与 WEP 兼容，所使用的口令常常被“黑客”运行简单的攻击程序推测出。

为解决上述问题，IEEE 正在制订新的标准 802x，并得到了许多厂商的支持。但是，该标准只解决认证问题，并未解决所有的安全问题，而且还不完整。因此，业界有关人士建议用防火墙保护接入点，通过与 5GHz 合作工程远程 Internet 接入同一种类型的虚拟专用网运行所有的业务。

5GHz 合作工程

目前，在 5GHz 频率上，欧洲电信标准学会(ETSI)制定了 HiperLAN2 标准。该标准使用 OFDM 技术，在物理层上几乎与 802.11a 相同，甚至数据率也相同，但与以太网相比协议栈高一级，更接近 ATM(异步传送模式)。

日本 DoCoMo 公司已把 HiperLAN2 与无绳电话结合在一起, 建立一个双模系统(即无线局域网和无绳电话两种方式可同时使用)。

爱立信是公开演示 HiperLAN2 样机的厂商。爱立信看中 HiperLAN2 的原因是, HiperLAN 不是真正的 LAN 协议, 而是为宽带移动数据业务设计的, 它可能成为 4G 的基础。

在欧洲, 蓝牙和 HiperLAN 系统都能保证移动装置之间“特设”网络的 QoS。欧洲各电信管理机构主张采用 HiperLAN2 标准, 不愿采用 802.11a。

现在, IEEE 正在解决未来在欧洲推行 802.11a 新版本的问题。在 IEEE 和 ETSI 之间还成立了一个称为 5GPP 工作组(即 5GHz 合作伙伴工程组), 旨在将 802.11a 和 HiperLAN2 整合成单一标准。该标准暂时称为 5-UP 协议, 即 5GHz 一体化协议, 它将 2 个甚至 3 个信道捆绑在一起, 能够提供比现有的系统更高的数据率。3 个信道的实际数据率将高达 100Mbps。采用 5-UP 协议的新系统将于 2003 年开始面市。

2 无线局域网标准进展

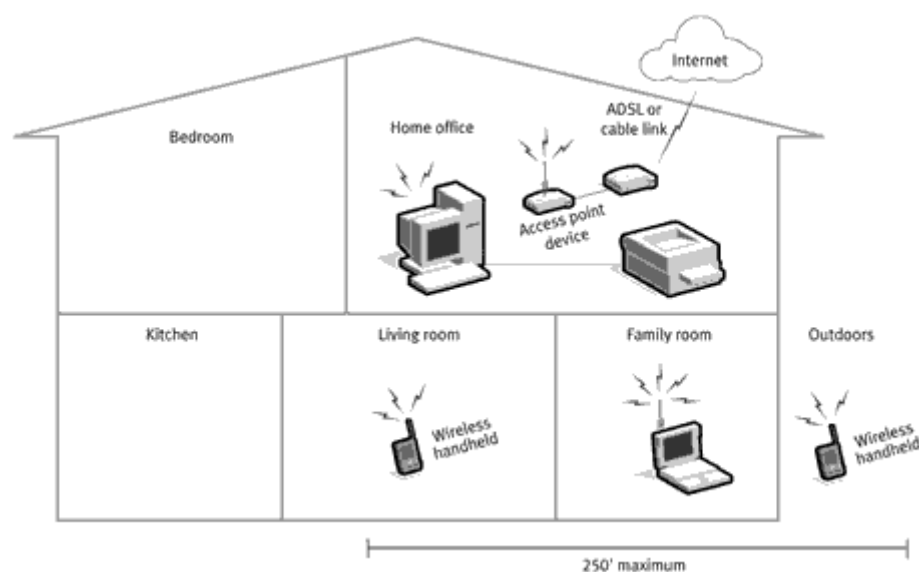
IEEE 802.11 是在 1997 年由大量的局域网以及计算机专家审定通过的标准。IEEE 802.11 规定了无线局域网在 2.4GHz 波段进行操作, 这一波段被全球无线电法规实体定义为扩频使用波段。

1999 年 8 月, 802.11 标准得到了进一步的完善和修订, 包括用一个基于 SNMP 的 MIB 来取代原来基于 OSI 协议的 MIB。另外还增加了两项内容, 一是 802.11a, 它扩充了标准的物理层, 频带为 5GHz, 采用 QFSK 调制方式, 传输速率为 6Mb/s—54Mb/s。它采用正交频分复用(OFDM)的独特扩频技术, 可提供 25Mbps 的无线 [ATM](#) 接口和 10Mbps 的 [以太网](#) 无线帧结构接口, 并支持语音、数据、图像业务。这样的速率完全能满足室内、室外的各种应用场合。但是, 采用该标准的产品目前还没有进入市场。另一种是 802.11b 标准, 采用 2.4GHz 频带和补偿编码键控(CCK)调制方式。该标准可提供 11Mb/s 的数据速率, 大约是现有 IEEE 标准无线 LAN 速度的 5 倍。还能够支持 5.5 Mbps 和 11 Mbps 两个新速率。而且 802.11b 可以根据情况的变化, 在 11 Mbps、5.5 Mbps、2 Mbps、1 Mbps 的不同速率之间自动切换。它从根本上改变 WLAN 设计和应用现状, 扩大了 WLAN 的应用领域, 现在, 大多数厂商生产的 WLAN 产品都基于 802.11b 标准。

除了 IEEE 802.11 委员会以外, 其他一些组织在推动无线局域网市场方面也做了许多工作。无线局域网联盟(WLANA)是由无线局域网厂商建立的非营利性组织, 它主要是进行无线局域网市场和产品使用方面的培训等工作。由 3Com、Aironet、Intersil、朗讯科技、诺基亚以及 Symbol 科技公司等厂商组建的无线 [以太网](#) 兼容联盟(WECA)则主要通过在同一无线结构内对不同厂商的产品进行验证, 以实现真正意义上的多厂商产品的互操作。

3. 三种流行无线网络技术的比较

如今, 无线网络技术日趋火热, 以蓝牙, IEEE 802.11 等为代表的一批无线网络连接技术正得到日益普及的应用。



上图所示为无线网络的组网结构。每一台计算机都安装了外部网卡，打印机或其它外设通过所连接的计算机实现共享。所有的设备都通过预先设定的无线电频率在实现相互之间的通信，并且通过接入点设备共享与外界互联网的连接。

一般来说，无线网络的有效传输距离在 250 英尺左右，不需要固定设备的具体位置。

无线网络具有以下优势：

- 支持移动联网。用户可以象使用移动电话那样灵活的移动计算设备的位置，保持持续的网络连接。
- 不需要使用物理线路，安装非常简便。
- 因为无线网络所使用的高频率无线电波可以穿透墙壁或玻璃窗，所以网络设备可以在有效范围内任意放置。
- 多层安全防护措施可以充分确保用户隐私
- 改动网络结构或布局时，不需要对网络进行重新设置。

常见的无线网络接入技术有下面三种：

1、IEEE802.11 家族

IEEE802.11 是 IEEE 最初制定的一个无线局域网标准，主要用于解决办公室局域网和校园网中，用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到 2Mb/s。

由于 IEEE802.11 在速率和传输距离上都不能满足人们的需要，因此，IEEE 小组又相继于 1999 年推出了 IEEE802.11b 和 IEEE802.11a 两个新标准。三者之间技术上的主要差别在于 MAC 子层和物理层。

IEEE802.11b 物理层支持 5.5Mb/s 和 11Mb/s 两个新速率，IEEE802.11 标准在扩频时是一个 11 位调制芯片，而 IEEE802.11b 标准采用一种新的调制技术 CCK 完成。IEEE802.11b 使用动态速率漂移，可因环境变化，在 11Mb/s、5.5Mb/s、2Mb/s、1Mb/s 之间切换，且在 2Mb/s、1Mb/s 速率时与 IEEE802.11 兼容。

IEEE802.11a 工作在 5GHz U-NII 频带，物理层速率可达 54Mb/s，传输层达 25Mb/s。采用正交频分复用 (OFDM) 的独特扩频技术；可提供 25Mb/s 的无线 ATM 接口和 10Mb/s 的以太

网无线帧结构接口，以及 TDD/TDMA 的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。但是，芯片没有进入市场、设备昂贵、空中接力不好、点对点连接很不经济、不适合小型设备。值得庆幸的是，Radiata 的低成本 COMS 无线引擎芯片装置可支持 IEEE802.11a。

2、蓝牙新贵

蓝牙（IEEE802.15）是一项最新标准，对于 IEEE802.11 来说，它的出现不是为了竞争而是相互补充。蓝牙比 IEEE802.11 更具移动性，比如，IEEE802.11 限制在办公室和校园内，蓝牙能把一个设备连接到 LAN 和 WAN，甚至支持全球漫游。此外，蓝牙成本低、体积小，可用于更多的设备。但是，蓝牙主要是点对点的短距离无线发送技术，本质上要么是 RF 要么是红外线。而且，蓝牙被设计成低功耗、短距离、低带宽的应用，严格来讲，不算是真正的局域网技术。

3、家庭网络的 HomeRF

HomeRF 主要为家庭网络设计，是 IEEE802.11 与 DECT 的结合，旨在降低语音数据成本。HomeRF 也采用了扩频技术，工作在 2.4GHz 频带，能同步支持 4 条高质量语音信道。但目前 HomeRF 的传输速率只有 1~2Mb/s。FCC 建议增加到 10Mb/s。

通过比较分析可以看出，各种标准都是根据不同的使用场合，不同的用户需求而制定的。有的是为了增加带宽和传输距离，有的则是考虑移动性和经济性，局部最优不等于全局最优。因此，用户应视实际需求选择适合自己的标准。

表 2 几种无线网络接入技术的比较

	IEEE802.11	IEEE802.11b	IEEE802.11a	Bluetooth	HomeRF
频率	2.4GHz	2.4GHz	5GHz	2.4GHz	2.4GHz
带宽	1~2Mb/s	可达 11Mb/s	可达 54Mb/s	1Mb/s	1~2Mb/s，可增至 10Mb/s
距离	100m	100m，功率增加可扩展	5~10km	10~100m	100m
业务	数据	数据/图像	语音/数据/图像	语音/数据	语音/数据

4. 下一代无线网络技术：HiperLAN/2

由于不受物理线路的限制，无线网络具有了有线网络所不可比拟的优势。针对无线 LAN 应用的需求，各厂商都推出了一系列基于 802.11 标准的无线 LAN（WLAN）产品，这些产品提供的带宽从 1Mbps 到 11Mbps 不等。但是，现在这些无线网络产品在性能上还远远不能与传统的固定网络产品相比，这就使得如今的无线网络在性能方面与采用 GSM、AMPS 等技术的广域蜂窝网络似乎并没有实质性的区别。尽管也支持一些速率较低（10kbps 左右）的数据通信，但这些无线网络的最主要的应用还是支持语音服务。为了满足未来的 Internet/Intranet 访问的需求，业界正在开发新一代的 WLAN 和蜂窝网络技术，这些新一代的技术将在 QoS（以便创建多服务网络）、安全及性能方面进行改进。

本文介绍了由 HiperLAN/全球论坛 (H2GF) 开发的被称为 HiperLAN/2 的下一代无线 LAN 技术 (WLAN)。H2GF 是由 Bosch Telcom、Dell、Ericsson、Nokia、Telia Mobile 和 Texas Instruments 等公司发起的，其宗旨就是要推动 HiperLAN/2 技术的标准化。HiperLAN/2 最引人注目之处是它能够在 5GHz 的频段上运行，而传统的无线 LAN 技术大多使用 802.11 标准的 2.4GHz 频段。HiperLAN/2 标准已经在去年底被最终确定下来。

网络结构及功能

图 1 显示了一个 HiperLAN/2 网络的拓扑结构。移动终端 (MT) 通过一个由 HiperLAN/2 标准确定的无线接口与访问点 (AP) 进行通信。MT 的用户可以在 HiperLAN/2 网络中自由地移动，HiperLAN/2 可以确保用户和 MT 得到最佳的传输性能。一个 MT 在某个时刻只与一个 AP 进行通信，不管用户移动到哪里，HiperLAN/2 无线网络能够检测到每个时刻能够为该 MT 提供最佳性能的 AP，并自动建立与该 AP 的联系。据介绍，在两个 MT 之间也可以不通过无线接口直接进行通信，但这种技术还处于研发阶段，具体细节现在还未公开。

HiperLAN/2 定义了检测功能和转换信令，以支持许多无线网络功能，包括动态频率选择 (DFS) 功能、链路自适应、无线信元转换、多束天线和功率控制等。

● 动态频率选择

该功能允许几个网络提供商共享可用的频谱，并且可以用来避免频率之间的相互干扰。每个 AP 是通过由 AP 以及和它相关的 MT 执行的过滤干扰计量来进行频率选择的。

● 链路自适应

为了满足各种无线传输服务质量的需要，在信扰比 (C/I) 方面，HiperLAN/2 使用了一个链路自适应方案。C/I 的变化范围根据 HiperLAN/2 系统部署的位置而定，而且，根据周围无线信元中的通信状况，C/I 可以进行变化。链路自适应方案根据链路的质量计量它适应物理层的程度。因此，网络可以动态地为每一个被发射的 MAC 帧选择 SCH (短传输信道) 和 LCH (长传输信道)。

● 天线

HiperLAN/2 中支持多束天线，这样可以增加无线网络的 C/I 比，提高无线网络的性能。HiperLAN/2 中的 MAC 协议和帧结构允许使用 7 束天线。

● 转换

转换方案是由 MT 启动的，也就是说，每一个 MT 都对周围的 AP 进行必要的检测，并选择最适合的 AP 进行通信。转换检测方法并没有在 HiperLAN/2 标准中进行定义，因此，有的厂商根据信号的强度进行转换，也有的厂商根据其他的质量标准进行转换。HiperLAN/2 标准定义了必要的信令来完成这种转换。

● 功率控制

HiperLAN/2 在 MT（上行链路）和 AP（下行链路）中都支持发射机功率控制。MT 功率控制主要用于简化 AP 接收机的设计。AP 功率控制是 HiperLAN/2 标准的一部分。

工作原理

图 2 表示了具有一个 MT 和三个支持具有优先权指示 Q 标记（Q tag）的 AP 的 HiperLAN/2 方案。

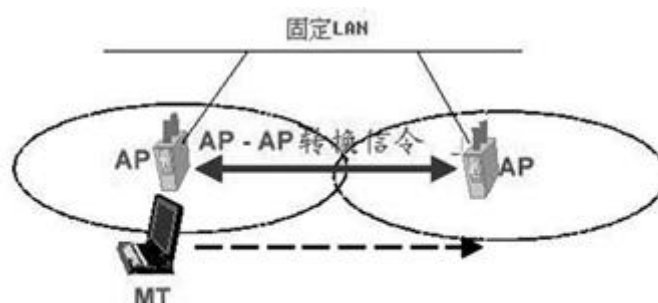


图2 通过固定LAN连接的HiperLAN/2网络

在 HiperLAN/2 中，每一个 AP 都使用 DFS 算法选择合适的频率。首先，MT 将检测信号强度，并选择要与它建立联系的最适当的 AP。MT 从选中的 AP 中接收一个 MAC 号（MAC ID），紧接着交换链路功能并据此决定使用什么样的认证过程和加密算法，以及使用哪一个聚合层用于用户的通信。在密钥交换和认证之后，MT 与 AP 就可以建立联系。最后，在数据链路控制层（DLC）建立用户连接，此时用户就可以进行通信了。

MT 将通过两个建立的连接（在 HiperLAN 中缺省值是 2 个）收发数据，这两个连接支持两种不同的带有 Q 标记映射的优先权排队（当然，也可以支持更多的优先级排队）。以太网聚合层确保每个以太网帧的优先级根据预先定义的映射方案被映射到适当的数据链路层用户连接中。

MT 可以决定加入一个或多个多路广播小组。HiperLAN/2 网络可以被配置来使用 N 个单路广播，以得到最理想的传输质量，也可以为每个加入的小组分配一个单独的 MAC 号（MAC ID）以便为其保留带宽。如果一个单独的 MAC 号被分配给一个多路广播小组，那么映射方案就是：IP 地址——IEEE 地址——MAC 号。

当 MT 移动时，如果它检测到有一个 AP 更适合于进行通信（如具有更好的信号强度），那么它会执行一次转换。所有已经建立的连接将使用 AP-AP 信令，通过固定 LAN 自动转换到新的 AP 上。当 MT（更确切地讲是用户）想与 LAN 断开连接时，MT 将请求断开了联系，这样就断开了 MT 和 AP 之间的所有连接。当 MT 移动到超出 HiperLAN/2 的覆盖范围时，也会断开 MT 和 AP 之间的所有连接。

主要特点

HiperLAN/2 技术的主要特点包括以下几个方面：

● 高传输速率

HiperLAN/2 具有很高的传输速率，它的物理层传输速率最高可达到 54Mbps，第三层的传输速率最高可达到 25Mbps。为了实现这样高的速率，HiperLAN/2 利用一种被称为正交频率数字复用（Orthogonal Frequency Digital Multiplexing, OFDM）的调制方法来发射模拟信

号。OFDM 在时间分散的环境（如办公室中）是非常有效的，这些地方发射的无线信号可能会被许多点反射，使得它们在最终到达接收方以前会产生不同的传播时间。在物理层上面，HiperLAN/2 使用了全新的媒体控制层（MAC）协议，它使用一种动态时分双工技术来最有效地利用无线资源。

● 面向连接

传统的无线网络都是非连接的。在 HiperLAN/2 网络中，需要先使用 HiperLAN/2 控制板的信令功能，在 MT 和 AP 之间建立连接，然后才能进行数据传输。连接是使用无线接口时分多址复用技术建立的。HiperLAN/2 中使用的连接有两类，即点对点的连接和单点对多点的连接。点对点连接是双向的，而单点对多点的连接是单向的，即只指向移动终端 MT。除此之外，还有一个专用的广播信道用于从一个 AP 将数据发射到所有的终端 MT。

● QoS 支持

HiperLAN/2 的面向连接的特性使它很容易满足 QoS 要求，可以为每个连接分配一个指定的 QoS，确定这个连接在带宽、延迟、拥塞、比特错误率等方面的要求。在 HiperLAN/2 中还有可能使用一个更加简单的方法，即每个连接可以分配一个不同的优先级标记。这种 QoS 支持与高传输速率一起保证了不同的数据序列（如视频、语音和数据等）可以同时进行高速传输。

● 自动频率分配

在 HiperLAN/2 网络中，不需要像在蜂窝网络（如 GSM 中）那样手工规划频率。无线基站（在 HiperLAN/2 中被称为访问点 AP）本身支持为每个 AP 在覆盖范围内进行的传输选择最适当的无线信道。（上接第 D26 版）每一个 AP 都监视邻近的 AP 以及 HiperLAN/2 环境中的其他无线资源，并且根据无线信道已经被其他 AP 占用和对无线网络环境的干扰降到最低这两个原则，选择最适当的传输信道。

● 安全支持

HiperLAN/2 支持认证和加密。通过使用认证机制，AP 和 MT 可以相互进行认证，以确保对网络的授权访问（从 AP 的角度看），或者确保对有效的网络提供商的访问（从 MT 的角度看）。HiperLAN/2 中的认证机制要依赖一些其他支持功能（如目录服务等），但这些支持功能本身并不包括在 HiperLAN/2 技术里。

用户在已经建立的连接上进行通信时，可以使用加密技术来防止实时窃听和中间人的攻击。

● 移动性支持

MT 将能够自动从最近的 AP 发射和接收数据。更确切地讲，MT 使用的 AP 所提供的无线信号具有最佳的信噪比。因此，当用户和 MT 移动时，MT 有可能检测到有另外一个比当前正在使用的 AP 具有更好的无线传输性能的 AP。此时，MT 将自动转换到这个 AP 上。所有原来

已经建立的连接都将被转移到这个新的 AP 上，使得 MT 仍然处于 HiperLAN/2 网络上，因此不会导致通信的中断。不过，在转换期间可能会发生一些丢包现象。

如果一个 MT 在某段时间里超出了无线 HiperLAN/2 的覆盖范围，MT 可能断开与 HiperLAN/2 网络的联系，这会使得所有原有的连接都被释放出来。

●网络和应用独立

HiperLAN/2 协议栈具有一个灵活的结构，因此很容易与多种固定网络进行适配和集成。如一个 HiperLAN/2 网络可以被用于一个交换式以太网的一段，但它也可能被用于其他的配置，如作为对第三代蜂窝网络的一个访问网络。所有今天可以在固定网络中运行的应用都可以在 HiperLAN/2 网络中运行。

●功耗低

在 HiperLAN/2 中，MT 节省功耗的机制是基于 MT 启动的休眠期状态。MT 可以在任意时刻请求 AP 进入一种低功率休眠状态，而且可以确定这一状态的时间。当协商好的休眠期满时，MT 搜索是否有 AP 发出的唤醒指示。如果没有搜索到唤醒指示，MT 将重新转换到低功率状态进入下一个休眠期。在休眠期间，AP 将延迟所有等待的数据传输任务，直到 MT 中结束相应的休眠期为止。HiperLAN/2 支持不同的休眠时间，这样可以满足用户对短延迟或低功率等不同的需求。

应用领域

HiperLAN/2 的应用领域非常广泛，下面是一些最典型的应用领域。

●企业 LAN

图 3 表示了使用以太网 LAN 和 IP 路由器建立的企业网络，在这个网络中，一个 HiperLAN/2 网络被用作 MT 和 LAN 之间的最后一段。HiperLAN/2 网络支持同一个 LAN/子网 (Subnet) 中的移动性。在子网之间移动就意味着 IP 具有可移动性。

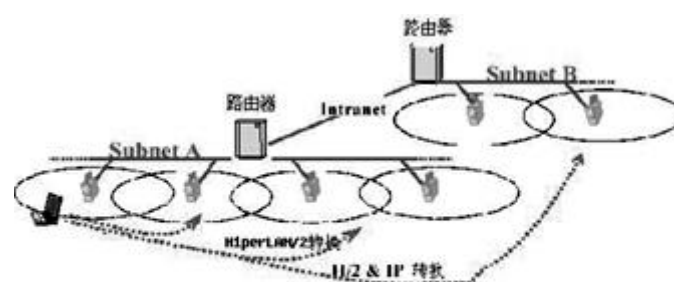


图3 在企业网络中使用的HiperLAN/2

●重要地点

HiperLAN/2 可以部署在一些重要地点（如机场、宾馆等），以便为正在旅行的用户提供远程访问和 Internet 服务。与 HiperLAN/2 连接的访问服务器允许点对点连接，也可以访问特定的企业网络（可能需要通过特定的 ISP）。

●访问第三代蜂窝网络

用户可以通过 HiperLAN/2 访问第三代蜂窝网络（如 WCDMA 等）。将来，HiperLAN/2 和 WCDMA 技术覆盖的地区必将越来越广泛，而用户可以从中得到最大的好处，他们不仅可以使使用 HiperLAN/2 提供的服务，而且在没有 HiperLAN/2 的地方仍然可以使用 WCDMA 蜂窝网络服务。当用户在两类网络之间移动时，核心网络可以保证用户无缝地自动在两类网络之间进行转换。

●家庭网络

HiperLAN 可以为家庭环境创建一个无线基础设施，用于家用设备（如家用 PC、VCR、照相机和打印机等）的联网。HiperLAN/2 的高输出和 QoS 特性可以满足各种家用设备视频传输与数据通信的要求。在这种情况下，AP 可能会提供一个到公众 Internet 的“上行”链路。

5. 无线局域网频道分配与调制技术

无线局域网采用电磁波（RF）作为载体传送数据信息。对电磁波的使用分两种常见模式：窄带和扩频。窄带技术以微波为主，适用于长距离点到点的应用，可以达到 40 公里。由于它采用的频道较宽以及定向信号天线，因此其最大带宽可达 10Mbps，但受环境干扰较大。

无线局域网采用无线扩频(spread spectrum)技术，也称 SST，早期由军事部门研发，确保安全可靠的军事通讯。常见的扩频技术包括两种：调频扩频（FHSS）和直序扩频（DSSS），它们工作在 2.4-2.4835GHz。

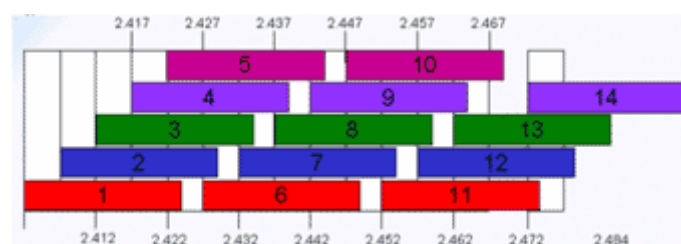
调频技术将 835MHz 的频带划分成 79 个子频道，每个频道带宽为 1MHz。信号传输时在 79 个子频道间跳变，因此传输方与接受方必须同步，获得相同的条变格式，否则，接受方无法恢复正确的信息。调频过程中如果遇到某个频道存在干扰，将绕过该频道。受跳变的时间间隔和重传数据包的影响，调频技术的典型带宽限制为 2-3Mbps。

无线个人网采用的蓝牙技术就是采用调频技术，该技术提供非对称数据传输，一个方向速率为 720Kbps，另一个方向速率仅为 57Kbps。蓝牙技术也可以传送 3 路双向 64Kbps 的语音。

直序扩频技术是无线局域网 802.11b 采用的技术，将 835MHz 的频带划分成 14 个子频道，每个频道带宽为 22MHz。直序扩频技术用一个冗余的位格式来表示一个数据位，这个冗余的位格式称为 chip，因此它可以抗拒窄带和宽带噪音的干扰，提供更高的传输速率。

直序扩频技术采用采用 DBPSK 和 DQPSK 调制技术，提供的最高带宽为 11Mbps，并且可以根据环境因素的限制自动降速至 5.5Mbps，2Mbps，1Mbps。

14 个子频道分配如下图：



在多个频道同时工作的情况下，为保证频道之间不相互干扰，标准要求两个频道的中频间隔不能低于 30MHz。因此从上图可以看出，在一个蜂窝区内，直序扩频技术最多可以提供 3 个不重叠的频道同时工作，提供高达 33Mbps 的吞吐量。

6. 无线局域网拓扑结构

无线局域网组网分两种拓扑结构：对等网络和结构化网络。

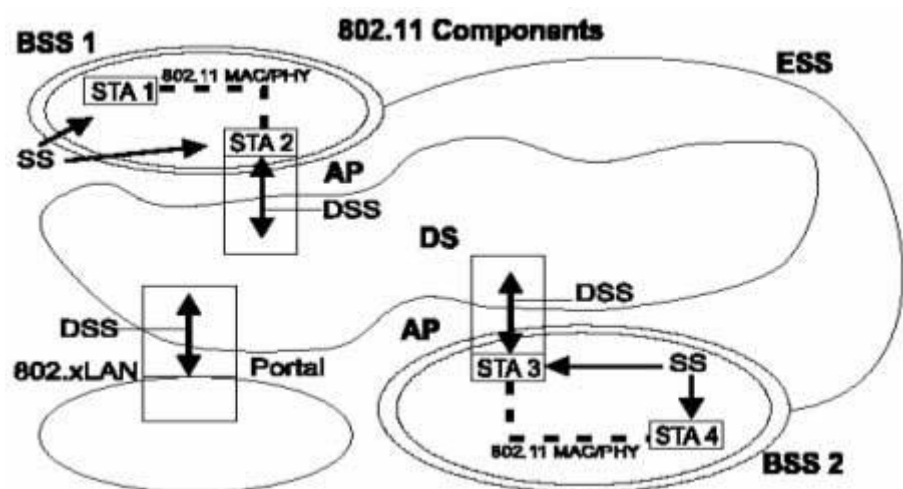
对等网络也成 Ad-hoc 网络，它覆盖的服务区称独立基本服务区。对等网络用于一台无线工作站和另一台或多台其他无线工作站的直接通讯，该网络无法接入有线网络中，只能独立使用。



对等网络中的一个节点必需能同时“看”到网络中的其他节点，否则就认为网络中断，因此对等网络只能用于少数用户的组网环境，比如 4 至 8 个用户，并且他们离得足够近。

结构化网络由无线访问点（AP）、无线工作站（STA）以及分布式系统（DSS）构成，覆盖的区域分基本服务区（BSS）和扩展服务区（ESS）。无线访问点也称无线 hub，用于在无线 STA 和有线网络之间接收、缓存和转发数据。无线访问点通常能够覆盖几十至几百用户，覆盖半径达上百米。

基本服务区由一个无线访问点以及与其关联（associate）的无线工作站构成，在任何时候，任何无线工作站都与该无线访问点关联。换句话说，一个无线访问点所覆盖的微蜂窝区域就是基本服务区。无线工作站与无线访问点关联采用 AP 的基本服务区标示符（BSSID），在 802.11 中，BSSID 是 AP 的 MAC 地址。



扩展服务区是指由多个 AP 以及连接它们的分布式系统组成的结构化网络，所有 AP 必需共享同一个扩展服务区标示符（ESSID），也可以说扩展服务区 ESS 中包含多个 BSS。分布式系统在 802.11 标准中并没有定义，但是目前大都是指以太网。扩展服务区是一个 Layer 2 网络结构，对于高层协议比如 IP 来说，它是一个子网。

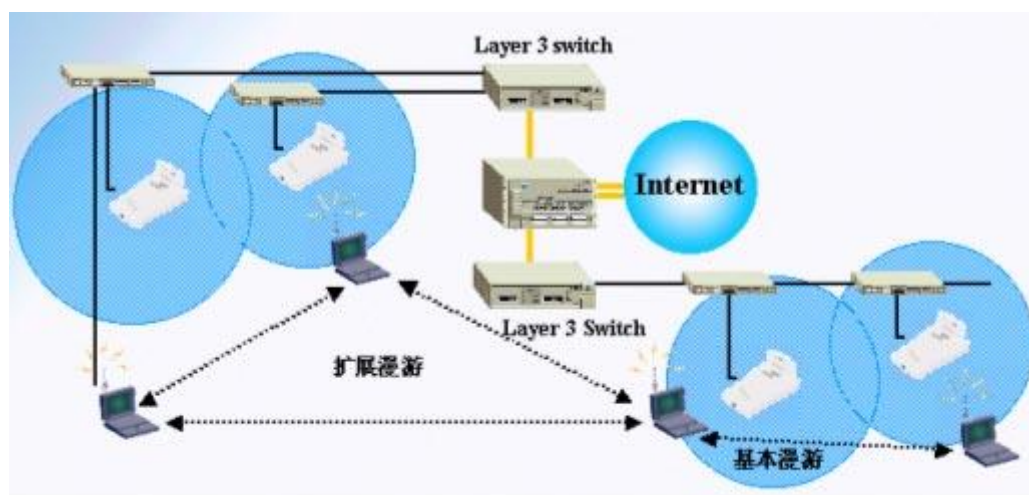
7. 无线局域网的几个主要工作过程

扫频：STA 在加入服务区之前要查找哪个频道有数据信号，分主动和被动两种方式。主动扫频是指 STA 启动或关联成功后扫描所有频道；一次扫描中，STA 采用一组频道做为扫描范围，如果发现某个频道空闲，就广播带有 ESSID 的探测信号；AP 根据该信号做响应。被动扫频是指 AP 每 100 毫秒向外传送灯塔信号，包括用于 STA 同步的时间戳，支持速率以及其它信息，STA 接收到灯塔信号后启动关联过程。

关联（Associate）：用于建立无线访问点和无线工作站之间的映射关系，实际上是把无线变成有线网的连线。分布式系统将该映射关系分发给扩展服务区中的所有 AP。一个无线工作站同时只能与一个 AP 关联。在关联过程中，无线工作站与 AP 之间要根据信号的强弱协商速率，速率变化包括：11Mbps，5.5Mbps，2Mbps 和 1Mbps。

重关联（Reassociate）：当无线工作站从一个扩展服务区中的一个基本服务区移动到另外一个基本服务区时，与新的 AP 关联的整个过程。重关联总是由移动无线工作站发起。

漫游：指无线工作站在一组无线访问点之间移动，并提供对于用户透明的无缝连接，包括基本漫游和扩展漫游。基本漫游是指无线 STA 的移动仅局限在一个扩展服务区内部。扩展漫游指无线 STA 从一个扩展服务区中的一个 BSS 移动到另一个扩展服务区的一个 BSS，802.11 并不保证这种漫游的上层连接。常见做法是采用 Mobile IP 或动态 DHCP。



8. 影响无线局域网性能的因素

传输功率：无线 AP 发送功率为 100mw

天线类型和方向

噪声和干扰：授权用户，微波炉，有意干扰等

建筑物结构：引发多路经，穿透效应等；

无线访问点摆放的位置

9. 无线局域网的安全性

1. 无线局域网（WLAN）面临哪些威胁？

由于大多数访问点采用不安全的默认配置，它们可为攻击者进入有线网络提供直接通道，这些设备被认为是网络中存在的脆弱点。大多数访问点的默认配置基本上是不安全的：访问点广播他们自己的服务设置标识号（Service Set Identifier，SSID），而且禁用 WEP 验证。另外，一些访问点设备允许与客户端设备直接通信，攻击者可以此特点重新配置访问点的安全设置。

2. 常见的无线网络安全分类

由于无线局域网采用公共的电磁波作为载体，因此与有线线缆不同，任何人都有条件窃听或干扰信息，因此在无线局域网中，网络安全很重要。常见的无线网络安全分几种：

服务区标示符 (SSID)：无线工作站必需出示正确的 SSID 才能访问 AP，因此可以认为 SSID 是一个简单的口令，从而提供一定的安全。如果配置 AP 向外广播其 SSID，那末安全程度将下降；由于一般情况下，用户自己配置客户端系统，所以很多人都知道该 SSID，很容易共享给非法用户。目前有的厂家支持“任何”SSID 方式，只要无线工作站在任何 AP 范围内，客户端都会自动连接到 AP，这将跳过 SSID 安全功能。

物理地址 (MAC) 过滤：每个无线工作站网卡都由唯一的物理地址标示，因此可以在 AP 中手工维护一组允许访问的 MAC 地址列表，实现物理地址过滤。物理地址过滤属于硬件认证，而不是用户认证。这种方式要求 AP 中的 MAC 地址列表必需随时更新，目前都是手工操作；如果用户增加，则扩展能力很差，因此只适合于小型网络规模。

连线对等保密 (WEP)：在链路层采用 RC4 对称加密技术，钥匙长 40 位，从而防止非授权用户的监听以及非法用户的访问。用户的加密钥匙必需与 AP 的钥匙相同，并且一个服务区内的所有用户都共享同一把钥匙。WEP 虽然通过加密提供网络的安全性，但也存在许多缺陷：一个用户丢失钥匙将使整个网络不安全；40 位的钥匙在今天很容易被破解；钥匙是静态的，并且要手工维护，扩展能力差。为了提供更高的安全性，802.11i 提供了 WEP2，该技

术与 WEP 类似。WEP2 采用 128 位加密钥匙，从而提供更高的安全。WEP2 目前不保证互操作性。

虚拟专用网络 (VPN)：虚拟专用网是指在一个公共 IP 网络平台上通过隧道以及加密技术保证专用数据的网络安全性，目前许多企业以及运营商已经采用 VPN 技术。VPN 可以替代连线对等保密解决方案以及物理地址过滤解决方案。采用 VPN 技术的另外一个好处是可以提供基于 Radius 的用户认证以及计费。VPN 技术不属于 802.11 标准定义，因此它是一种增强性网络解决方案。

端口访问控制技术 (802.1x)：该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站 STA 与无线访问点 AP 关联后，是否可以使用 AP 的服务要取决于 802.1x 的认证结果。如果认证通过，则 AP 为 STA 打开这个逻辑端口，否则不允许用户上网。802.1x 要求无线工作站安装 802.1x 客户端软件，无线访问点要内嵌 802.1x 认证代理，同时它还作为 Radius 客户端，将用户的认证信息转发给 Radius 服务器。802.1x 除提供端口访问控制能力之外，还提供基于用户的认证系统及计费，特别适合于公共无线接入解决方案。

3. 如何保障无线局域网安全

随着无线局域网(WLAN)、第三代互联网技术(3G)等无线互联网技术的产生和应用，无线网络使人们的网上生活变得更加轻松自如，那种拿着笔记本电脑，在智能大厦里的任意地方行走，随时随地下载资料、打印文件等早已不是电影中的情节了。无线局域网与传统有线局域网相比优势不言而喻，它可实现移动办公、架设与维护更容易等。Frost&Sullivan 公司预测无线局域网络市场在 2005 年底将达到 50 亿美元。在如此巨大的应用与市场面前，无线局域网络安全问题就显得尤为重要。人们不禁要问：通过电波进行数据传输的无线局域网的安全性有保障吗？

实际上，无线局域网比大多数有线局域网的安全性更高。无线局域网技术早在第二次世界大战期间便出现了，它源自于军方应用。一直以来，安全性问题在无线局域网设备开发及解决方案设计时，都得到了充分的重视。目前，无线局域网络产品主要采用的是 IEEE(美国电气和电子工程师协会)802.11b 国际标准，大多应用 DSSS(Direct Sequence Spread Spectrum，直接序列扩频)通信技术进行数据传输，该技术能有效防止数据在无线传输过程中丢失、干扰、信息阻塞及破坏等问题。802.11 标准主要应用三项安全技术来保障无线局域网数据传输的安全。第一项为 SSID(Service Set Identifier)技术。该技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络；第二项为 MAC(Media Access Control)技术。应用这项技术，可在无线局域网的每一个接入点(Access Point)下设置一个许可接入的用户的 MAC 地址清单，MAC 地址不在清单中的用户，接入点(Access Point)将拒绝其接入请求；第三项为 WEP(Wired Equivalent Privacy)加密技术。因为无线局域网是通过电波进行数据传输的，存在电波泄露导致数据被截听的风险。WEP 安全技术源自于名为 RC4 的 RSA 数据加密技术，以满足用户更高层次的网络安全需求。

目前，这些技术已发展成熟并得到了充分应用。无线以太网兼容性联盟 WECA(Wireless Ethernet Compatibility Alliance)认证厂商已有 30 多家，其产品大多按 IEEE802.11b 标准进行生产，具备上述的安全性能。例如 IT 业巨头英特尔公司在 2001 年推出的 11Mbps 无线 LAN 产品系列，全面支持 WEP(Wired Equivalent Privacy)的密码编码功能，用最长 128bit 的密码键对数据进行编码后，在 AP 适配器上进行通信，密码键长度可选择 40 bit 或 128bit。利用 MAC 地址和预设网络 ID 来限制哪些网卡和接入点可以连入网络，完全可确保网络安全。对于那些非法的接收者来说，截听无线局域网的信号是非常困难的，从而可以有效防止黑客和入侵者的攻击。无线局域网产品这些内在的安全特性，使许多注重商业机密的行业应用无线局域网成为可能。

此外，目前已广泛应用于局域网络及远程接入等领域的 VPN(Virtual Private Networking)安全技术也可用于无线局域网络，与 IEEE802.11b 标准所采用的安全技术不同，VPN 主要采用 DES, 3DES 等技术来保障数据传输的安全。对于安全性要求更高的用户，英特尔建议用户建网时，将现有的 VPN 安全技术与 IEEE802.11b 安全技术结合起来，这是目前较为理想的无线局域网络的安全解决方案。

4. 保护企业无线网络

当企业使用无线局域网技术，却没有采取适当的安全措施时，即使一些初级黑客都有可能利用容易得到的廉价设备对企业网络进行攻击。

为什么企业在物理建筑和有线网络上的安全防范意识不能延伸到无线系统中呢？回答也许是企业对无线网络的安全性缺乏了解——人们可能会天真地认为信号不会跑到公司的围墙外面去，或者直觉认为如果你无法看见信息，就无法窃取信息。

不能只依靠 WEP

无线网络最基本的安全措施是 WEP (Wired Equivalent Privacy)。WEP 是所有经过 Wi-Fi 认证的无线局域网所支持的一项标准功能，它主要利用一套基于 40 位共享加密密钥的 RC4 加密算法对网络中所有通过无线传送的数据进行加密，从而有效地保护网络。除了设计一套强大的安全解决方案，避免简单错误的发生也是非常明智的。避免一些错误，如没有开启 WEP、将访问点设置在防火墙之内、使用缺省的 WEP 密钥以及没有定期变更加密密钥等，能够提高无线网络的安全性。

加密密钥算法本身并不存在缺陷，只是密钥的管理不善导致了黑客的入侵。企业网络系统管理员经常会为整个公司分配一个密钥，一旦黑客获得密钥，就能访问公司所有的专有信息和网络资源。

管理员也许会赋予每一个用户不同的密钥，但这些用户却可能从来不对其进行变更。一旦黑客获得了访问权限，他们便可以一直进行非法访问，并共享企业的重要资源。管理严格的小型网络可以使用方便的手动密钥管理。但是，随着无线网络用户的增加，这种手动管理方式会变得非常烦杂，容易造成网络系统管理人员的工作疏忽。

动态密钥管理支持用户认证

为进一步提高安全性，动态安全链路技术能够支持用户认证，即要求所有的用户在开始每一个会话之前提供用户名和密码，相对基于设备 MAC 地址的认证策略，基于用户的认证功能可以为企业网络实现较高级别的安全和管理能力，基于设备 MAC 地址的认证策略会因为设备的丢失或失窃而失效，而且每当类似事件发生时，都需要对保存在每一台网络接入点设备内的 MAC 地址数据库进行变更。

动态安全链路的另一个优势在于其自动和动态的密钥管理能力完全是由访问点设备自身来实施，因此这套解决方案不需要增加任何服务器设备和其他基础设备。这种安全性实施策略非常适用不需要大量资金就可实现无线局域网安全性的小型网络，同时对希望以非集中化方式来实现企业网络安全性的企业来说也是理想的选择。

大型网络安全性更高

大型无线局域网的安全性管理不仅需要可以自动变更加密密钥的 DSL 功能，还需要更多安全性功能，从而来满足更多用户和更复杂安全性的要求。设备的增多会需要更加强大的加密密钥管理技术、更加灵活的认证机制、以及整个基础网络的集中用户管理，所有这些无法全部存储在一部无线局域网接入点设备的有限内存中。

尽管 WEP 和 DSL 解决方案中的安全性功能已经本地化——即在无线局域网接入点设备内部进行管理——但是一个能够支持上千名用户，具有最先进加密和认证技术的大型系统通常需要一套能够进行集中化管理的安全性解决方案。这些系统通过 RADIUS (拨号用户远程认证服务) 进行管理。RADIUS 能够对授权访问网络资源的网络用户进行集中化管理。

不论是对有线的以太网网络还是无线的 802.11 网络，RADIUS 都是标准化的网络登录技术。支持 802.1x 协议的 RADIUS 技术，提高了企业级无线局域网用户的认证能力。安全性功能不仅仅是网络应用的附件，更应该被融入到企业的各种商业结构中去。

安全问题比较棘手

由于 WEP 很容易被相关软件攻击,这迫使销售商和 IT 管理者去寻找新的加密解决方案。同样的,无线并没有真正的标准,虽然现在 802.1x 可能成为最终的标准,但是,现阶段它还是需要认证机构的授权。

即使零售商们致力于私密性、鉴定和授权服务,让用户头痛的安全问题仍旧不会停止。有一些更严重的问题正在显露出来,它们当中最有害的是 DoS 攻击。虽然 DoS 在所有的网络上都存在,但在无线网络上,情况会更糟,因为用户不仅需要抵御对第 2 层及以上的恶意攻击,而且网络的物理介质层也非常容易受到攻击。另外,更多不知名的恶意攻击,是专门针对 WLAN 的更为可怕的威胁,这其中包括在物理层的 RF 人为干扰、对特定基站的攻击。这种攻击使基站不能持续与 AP 相连接、让用户通过敌对基站的路由来通信,让无线网络完全暴露在外面。而且,还有一些利用无线管理帧来发动的新攻击。随着 WLAN 逐渐成为主流,我们期望 IDS 能解决这些问题。对于 IT 管理者来说,有更多的问题需要他们持续的关注。

第 5 章、无线局域网络产品的兼容性

WECA 是无线以太网兼容性联盟,有 70 多个成员,包括 3Com, Symbol, Dell, Cisco 等,目的是保证各厂家的所有 802.11b 产品的互操作性,所有通过认证的产品将颁发 Wi-Fi 证书,贴 Wi-Fi 标志。Wi-Fi 代表 Ethernet for WLAN。目前有 40 多个厂家的 100 多个产品通过了 Wi-Fi 认证,因此它们之间的互操作将得到保证。

第 6 章、Cisco 无线局域网络解决方案

1. 思科无线局域网技术指南

下一代无线局域网

Cisco Aironet 1200 系列可以为未来的无线技术提供方便的移植

无线局域网技术正在获得越来越普遍的关注,并在全球的很多希望通过更具有移动能力和生产率更高的员工而获得竞争优势的企业中得到广泛的应用。

在采用无线技术之前,企业必然会遇到很多问题。例如,目前有哪些无线局域网技术可供选择?这些技术的标准化工作进展如何?最新的无线设备是否会向后兼容,从而确保对未来的无线投资的保护?

本技术指南将解答这些问题,本文对一些热点问题的回答将可以帮助您在您的企业如何使用无线技术方面制定更加准确的决策。本指南将介绍 Cisco Aironet 1200 系列接入点产品,它为安全的、可管理的、可靠的无线局域网设立了企业级标准,并可以为未来的高速无线局域网技术提供一个平稳的移植路径。这种创新的、出色的无线基础设施平台具有双频功能,可以同时支持现有的和新兴的无线标准。Cisco Aironet 1200 系列接入点的一个最具创新性的特点是它的软件和硬件都可以升级。企业不仅可以通过升级它们的软件来利用思科在将来推出的新功能,还可以现场升级无线收发装置,利用新的高速无线标准。在 Cisco Aironet 1200 系列接入点的帮助下,您的企业可以充满信心地部署无线技术--不需要担心与将来的无线技术、协议和标准的兼容性问题。

无线技术的到来

对于计算机用户来说,无线技术并不是一个新名词。人们在 20 年之前就建立起了第一个无线连接。但是,无线技术的应用发展得非常缓慢,这主要是因为一些特殊的垂直市场的限制,例如仓储、教育和零售业。

由于下面三点原因，无线技术的部署进展非常缓慢。首先，无线数据的原始传输速率太低，无法满足一个共享式局域网上的主流用户的需要。尽管吞吐量的确在逐步增加，但是网络速度仍然大幅度地落后于有线局域网的速度。其次，专用的、非标准的解决方案统治了市场，设备之间的互操作性很低，给那些拥有多个厂商提供的产品的用户带来了许多困扰。第三，与有线解决方案相比，这些低速的专用解决方案的价格非常昂贵。

近些年来，情况发生了很大的变化。电气和电子工程师协会（IEEE）在 1999 年批准了 802.11b 标准，它可以提供最高每秒 11B 位(Mbps)的数据传输速率—近似于很多以太网工作小组所使用的 10-Mbps 连接。无线局域网首次开始适用于大部分工作环境和办公室应用。很多厂商随后立即开始支持 802.11b 标准—这迅速地降低了成本，带来了更多的需求和更加广泛的厂商支持。另外，802.11b 标准确保了用户可以获得设备互操作能力。无线以太网兼容性联盟（WECA）是一个非盈利性的国际组织，它的宗旨是检验基于 802.11b 标准的无线局域网产品的互操作能力，并在所有市场中推广该标准。随着 802.11b 标准的迅速普及，用户开始可以选择多种可互操作的、低成本的、高性能的无线设备。

可能最重要的是，各种类型的企业现在都可以通过将无线技术加入自己的企业局域网而获得巨大的利益。多年以来，膝上型电脑和笔记本电脑一直承诺可以随时随地进行计算。但是，随着对局域网和互联网的访问日益成为开展业务的不可或缺的组成部分，人们需要通过无线连接来真正实现随时随地进行计算的承诺。无线设备让用户几乎从任何地方都可以接入网络：办公桌、会议室、咖啡厅，或者企业园区和校园中的另外一个建筑物。这种能力为用户提供了最大限度的灵活性、生产率和效率，同时可以极大地促进同事、商业伙伴和客户之间的合作。此外，无线技术还可以为难以铺设电缆或者布线成本过高的场所提供局域网访问。

无线移植方案的选择

像其他任何技术一样，无线技术一直在不断地发展—提供更高的速度、带宽、安全性等。无线技术最近在技术上发展到了—一个重要的转折点。

工作在不需许可的 2.4GHz 频段的 802.11b 标准是全球应用最广泛的无线标准，它可以提供最高 11Mbps 的数据传输速率。对于一部分企业来说，这样的速度已经足以满足他们目前的需求。但是其他企业仍然希望通过新一代的设备获得更高的吞吐量、访问速度和功能，以满足他们迅速增长的无线用户的需要。

无线厂商对这种需求做出了积极的响应。目前，IEEE 任务小组正在集中精力制定两项更高性能的标准—802.11a 和 802.11g。在移植到更高性能的无线技术的过程中，用户必须了解每种无线标准的优点和缺点，并在此基础上判断哪种技术或者哪些技术最符合他们自身的无线网络需求。

802.11a 标准

IEEE 于 1999 年批准了 802.11a 标准，但是直到 2001 年 12 月市场上才出现第一款兼容 802.11a 的产品。802.11a 标准最高可以提供 54Mbps 的数据传输速率和 8 个不重叠的频率通道—从而可以增加网络容量，提高可扩展性，并能够在不干扰相邻单元的情况下创建微型单元式结构。802.11a 工作在不需申请的 5GHz 频段，因为不会受到来自于工作在 2.4GHz 频段的设备的干扰，例如微波炉、无绳电话和蓝牙（一种短距离、低速、点对点、个人局域网无线标准）设备。但是，802.11a 标准并不能与现有的支持 802.11b 的设备兼容。已经采用了 802.11b 设备，并希望获得 802.11a 技术所提供的更高通道数和网络速度的企业必须安装一整套全新的 802.11a 基础设施，以及 802.11a 接入点和客户端适配器。需要指出的是，2.4GHz 和 5GHz 设备可以在互不干扰的情况下在同一个物理环境下工作。

要在全球范围内普及 802.11a，一个重要的障碍是该标准尚未被全球各国的相关法规制定部门批准使用。到目前为止，802.11a 还未在欧洲获得批准；但是，IEEE 和欧洲通信标准委员会（ETSI）目前正在设法通过 IEEE 802.11h 任务小组达成一项协议，解决 802.11a 的电源问题和通道设置问题。

推广 802.11a 的另外一个障碍是缺乏对互操作性的认证。目前，各个厂商的产品之间的互操作性还没有保障。WECA 将为 802.11a 产品提供互操作性测试，并致力于进一步推广该技术。但是，只有在两家芯片厂商开始制造相应的芯片，并至少有三家厂商在这些芯片的基础上制造产品以后，WECA 才会开始进行这样的测试。WECA 期望认证工作将从 2002 年下半年开始。

802.11g 标准

802.11g 标准从 2001 年 11 月就开始草拟,但是预计到 2003 年之前不大可能最终完成。802.11g 可以提供与 802.11a 相同的 54Mbps 数据传输速率,但是它还可以提供一种重要的优势——对 802.11b 设备向后兼容。这意味着 802.11b 客户端卡可以与 802.11g 接入点配合使用,而 802.11g 客户端卡也可以与 802.11b 接入点配合使用。因为 802.11g 和 802.11b 都工作在不需许可的 2.4GHz 频段,所以对于那些已经采用了 802.11b 无线基础设施的企业来说,移植到 802.11g 将是一种合理的选择。需要指出的是,802.11b 产品无法“软件升级”到 802.11g,这是因为 802.11g 无线收发装置采用了一种与 802.11b 不同的芯片组,以提供更高的数据传输速率。但是,就像以太网和快速以太网的关系一样,802.11g 产品可以在同一个网络中与 802.11b 产品结合使用。由于 802.11g 与 802.11b 工作在同一个无需申请的频段,所以它需要共享三个相同的频段,这将会限制无线容量和可扩展性。

兼容性

802.11a 和 802.11g 都可以大幅度地改进现有的 802.11b 标准,因为它们所带来的更高的数据传输速率可以为无线局域网上的设备提供更高的性能和可用性。但是一个不足之处是由于 802.11a 和 802.11g 标准使用的频段不同,所以不能相互兼容。而且,802.11a 不能与现有的 802.11b 设备兼容。

那么,企业应该怎么做呢?当他们展望其无线基础设施的未来时,这个决定非常关键。它将在未来几年中决定他们所选择的产品和他们的基础设施的功能。

双频 Cisco Aironet 1200: 全球最佳

在理想情况下,企业不需要在只能支持两种不同无线标准之一的产品之间进行选择。相反,企业可以获得能够确保向后和向前兼容,并保障用户所需性能等级的设备。这种解决方案可以满足新兴的和已有的无线环境的需求。幸运的是,这种解决方案已经面世。Cisco Aironet 1200 系列接入点可以兼容所有已有的和新兴的无线局域网标准。它是如何做到这一点的?这种无线接入点支持双频——即同时支持 2.4GHz 和 5GHz 标准。因此,企业不需要再选择某一种单一的技术。

Cisco Aironet 1200 系列可以为无线基础设施提供最大限度的灵活性和可扩展性。它的双频设计可以支持基于 2.4GHz 和 5GHz 标准的设备。它让企业可以在工作场所中采用不同的客户端设备,但通过一个由双频接入点构成的单一网络来为这些不同类型的客户端提供支持。事实上,Cisco Aironet 1200 系列可以方便地进行现场升级,这使得管理员可以轻松地添加另外一个无线收发装置,或者卸载某个无线收发装置,再用另外一个装置来代替它。作为一个无线接入点,该设备可以为用户提供前所未有的十一个无线通道——八个用于 5GHz 频段,另外三个用于 2.4GHz 频段。因此,Cisco Aironet 1200 系列可以方便地扩展规模,以添加无线设备和无线用户。

Cisco Aironet 1200 系列的另外一个重要的特点是它可以使用思科提供的各种 2.4GHz 天线,从而能够为客户提供多种天线增益和覆盖模式。

Cisco Aironet 1200 系列双频设计在业界具有很高的创新性和独创性。但是,这种概念已经有一些先例。例如,在电视发展的早期,由于 VHF 频段最多只能接收 12 个频道,电视制造商们在电视机中加入了 UHF 频段。这样,观众可以收看到比以往多得多的节目——而且只通过一个设备实现。广播的发展也与之十分类似——人们在已有的 AM 频段广播的基础上加入了 FM 频段。无线局域网技术目前也在采用相似的方法。越来越多的业界厂商开始转移到双频模式。Cisco Aironet 1200 系列可以支持现有的和新兴的无线局域网标准,表明了思科对于必将到来的双频时代所做的准备。

Cisco Aironet 1200 系列可以为无线局域网提供最平稳的移植路径。它让企业可以立即升级到强大的无线技术,同时确保他们的投资可以在很长时间以后都保持作用和价值。该解决方案还有助于降低企业的无线基础设施的长期运营成本。

今天的无线应用

在 Cisco Aironet 1200 系列的帮助下,无线应用的范围将只受限于人们的想象力。特别需要指出的是,目前人们对下列无线应用具有大量的需求:

- **局域网速度的无线访问**——无论是在办公室、分支机构、家中还是机场,今天的员工都需要能够安

全地访问企业网络。利用无线连接，他们可以从一个接入点的覆盖范围内的各个地点，轻松地访问他们的应用和数据。因此，员工可以在任何地方接入网络，并全身心投入工作。

- **互联网/内联网访问**--今天，员工需要连续地访问互联网和企业的内联网。无线技术让员工可以持续地利用这些功能，进行研究，并通过电子邮件和即时消息与同事和业务伙伴交流信息，而不会受到有线连接的限制。
- **高度移动的计算**--目前，大多数无线计算都是通过膝上型电脑完成的。但是，这种局面正在迅速地发生变化。越来越多的无线厂商都开始提供一些可以大幅度减少体积、功耗和无线解决方案的成本的芯片级解决方案。

因此，无线功能将会越来越多地出现在一些较小的设备中，例如体积非常小的膝上型电脑、个人数字助理（PDA）和电话。这些设备在以无线方式连接到企业网络以后，将成为那些不会整天待在办公桌前的员工的重要工具。

计算的新纪元

无线革命才刚刚开始。新的技术、标准，以及对于员工移动性的关注将会推动无线局域网在全球以前所未有的速度迅速发展。因此，企业现在就必须制定他们的无线战略。在制定战略的过程中，他们不需要做出任何妥协。Cisco Aironet 1200 系列接入点可以提供企业目前所需要的强大的无线连接，确保向后兼容性和未来的投资保护。而且，这种无线接入点还可以提供业界领先的性能、现场升级能力和灵活性，从而可以支持多种无线标准，满足企业在相当长一段时期内的无线访问需求。

2. 思科无线安全解决方案指南

在不放弃安全性的前提下为您的网络用户提供自由和移动性

Cisco Aironet 系列--无线自由和企业级安全性

唯一一件可能比在您的网络上交换数据更加重要的事情是保障这些数据的安全。对安全性的担忧导致很多网络管理员不愿意安装无线网络，无论它能给他们带来多大的好处。不得不在网络安全和用户对于更高的移动性和灵活性之间进行权衡的企业纷纷选择了安全第一的策略。

现在，无线安全的情况发生了一定的变化，使 IT 经理们开始可以放心地部署无线局域网（WLAN）。这是因为现在有了思科无线安全套件--一个基于标准的企业级 WLAN 解决方案。作为网络行业的领导者和无线网络技术的推动者，思科现在使网络管理员可以在不牺牲用户所需要的网络安全的前提下为用户提供他们所渴求的自由。



思科--值得您信赖的品牌

思科无线安全套件建立在 IEEE 802.1x 无线标准的基础之上。它的核心是曾经获得大奖的、兼容 IEEE 802.11b 的 Cisco Aironet 系列客户端适配器和访问点。Cisco Aironet 系列以其卓越的性能、安全性和可靠性在业界占据了领先地位。

但是，不要光听我们的介绍，让我们来看看别人对它的评价。《网络世界》以 Cisco Aironet 系列卓越的质量、方便的安装和--最重要的--出色的安全性而授予该产品 "蓝带"。该杂志发现，与其他三个同类的高端 WLAN 系统相比，Cisco Aironet 系列可以提供最佳的安全性、方便的管理和最高的灵活性。《网络世界》用下面这段话总结了它对于 Cisco Aironet 系列和 802.1x Cisco LEAP（可扩展身份认证协议[EAP]Cisco Wireless）身份认证的评价："在结合了用户的登陆信息和定期的重新认证以后，Cisco LEAP 可以提供您所需要的强大的安全性，从而可以有效地保护您的企业数据，防止黑客进入您的无线局域网...."

降低 WLAN 安全风险

像有线网络一样，没有可以保证提供可以在任何时候阻止任何入侵的、绝对安全的网络环境。安全保护是一个动态的、连续的过程--而不是静态的。网络管理员和 WLAN 设备制造商需要在技术上始终比黑客领先一步。

保障 WLAN 的安全只是整个企业安全框架的一个组成部分。正如任何一位无线专家都会告诉你的一样，网络管理员会由于部署 WLAN 而在一定程度上增加网络的安全风险。安全专家建议企业在网络中部署多层防御措施，以减轻黑客攻击的威胁。其他的安全组件包括防火墙、入侵检测系统、虚拟专用网络（VPN）、内容过滤、防病毒软件、补丁管理等。

5. 网络管理员可以降低他们的网络所面临的风险，同时加强 WLAN 的安全性。利用思科无线安全套件的各种最新的、曾经获得大奖的安全特性，网络管理员可以降低他们的网络所面临的风险，同时加强 WLAN 的安全性。

无线技术可以提供移动性和自由，并可以提高员工的工作效率。WLAN 的使用率正在以指数速度迅猛增长。今天，很多企业纷纷利用无线网络来提高员工的工作效率。通过部署一个安全的无线网络，员工可以收发电子邮件，制定会议日程，以及通过他们的膝上型电脑或者手持式 PC 访问企业网络--无论他们是在会议室、同事的办公室还是在公司设在全球各地的分支机构。

企业还发现，添加一个 WLAN 也有助于改善公司的运营情况。最近进行的一项独立调查显示，WLAN 使终端用户每天可以多联网 1.75 个小时，平均每个用户可以节约 70 分钟，生产率最高可以提高 22%（资料来源：NOP World, 2001 年 11 月）。这样的生产率可以为企业的发展提供足够的保障。



图注：在对产品质量、易用性和安全性进行了全面测试以后，《网络世界》向 Cisco Aironet 系列授予了"蓝带奖"。



图注：在一个建筑物或者园区中，可以部署多个耐热阻燃型思科访问点，它们可以充当某个完全无线的网络的中心点，也可以充当某个有线网络和无线网络之间的连接点。

思科访问点可以帮助安装了思科客户端适配器的用户在园区范围内自由移动。思科新推出的无线安全套件可以确保对所有网络资源的高度安全的、不间断地访问。可以将黑客拒之门外的安全性

无线网络不同于有线网络，因此企业在向它们的网络添加无线技术时，需要注意网络的安全性和随之而来的管理问题。建筑物之外的区域，甚至某个使用 WLAN 的员工的住家，都有可能成为网络的一部分。

WLAN 的覆盖范围是三维的。这意味着可能会有一些事先没有预料到的区域进入访问点的覆盖范围。由于射频范围内的任何人都可以查看网络中传输的分组，传统的物理安全控制已经不足以确保网络的安全。

在采用了 WLAN 以后，网络的边界发生了变化。访问网络的客户端需要检查他们当前加入的是哪个网络。网络管理人员需要尽快地发现并阻止网络攻击。如果没有采取正确的安全措施，一个采用无线网络的公司最终就会像是在公司停车场中安放了一个没有任何保护的 RJ-45 端口。

今天，采用 WLAN 的企业正在部署四种不同级别的 WLAN 安全措施：没有安全、基本安全、增强安全和专业安全。像所有其他有关安全的部署一样，思科建议企业在选择和部署任何一种 WLAN 安全解决方案之前先进行网络风险评估。

没有安全保护

在讨论 WLAN 安全时，首先从没有安全保护的 WLAN 网络开始谈起似乎有些不同寻常，实际上并非如此。有相当多的企业目前仍然没有启用 WLAN 的安全特性。事实上，根据《华尔街日报》最近的一篇报道，两名黑客携带着一个膝上型电脑和一个外接天线，驱车在硅谷附近窃听空间中的 WLAN 信号，想看看他们能够获得什么样的数据。结果他们在一些“财富 500 强”公司附近发现了很好的 WLAN 访问信号。显然这些公司没有采取任何 WLAN 安全措施，这使得他们的网络面临着严重的威胁。

思科强烈建议所有企业都启用他们的无线安全特性。在建立任何一个无线网络时都必须启用安全特性。在关闭安全特性的情况下建立一个 WLAN 就好像一天二十四小时都敞开您的企业的大门。 **基本安全保护**

尽管不启用 WLAN 安全特性肯定会给网络带来危险，但是另外一种等级的安全最近也频频见诸报端，因为它们非常容易被攻破--它就是基本安全保护。当您听到 WLAN 安全受到威胁时，通常指的都是采用静态的有线等同保密（WEP）密钥的基本安全。静态 WEP 密钥是一种在会话过程中不发生变化也不针对各个用户而变化的密钥。网络管理员可以设置一个 40 位或者 128 位的静态 WEP 密钥，用其进行身份认证和加密，它使得 WLAN 很容易受到“密码再度使用”式攻击。

静态 WEP 密钥对于 WLAN 上的所有用户都是通用的。这意味着如果某个无线设备丢失或者被盗，所有其他设备上的静态 WEP 密钥都必须进行修改，以保持相同等级的安全性。退一步说，这将给企业网络的管理员带来非常费时费力的、不切实际的管理任务。

我们建议不要在大型企业中使用静态 WEB 密钥。像 AirSnort 这样的破解工具使攻击者可以主动地监控、接收和分析数据分组，破解静态 WEP 密钥。这方面已经发表了很多文章，其中包括加州大学伯克利分校出版的一个白皮书《监听移动通信：802.11 的安全性》（2001 年 1 月）。

尽管基本安全保护好过没有安全保护，但是仍然不足以满足企业的需要。唯一适于采用基本安全和静态 WEP 密钥的机构是小型企业和一些数量可能非常有限的攻击或者培训机构，他们需要建立 WLAN 供学员使用。所有大中型企业和培训管理部门都必须利用一种更加安全的方法来保护他们的 WLAN 网络--增强的安全解决方案。在选择部署一个基本安全解决方案之前，企业或者机构必须进行网络风险分析，判断静态 WEP 密钥是否足以满足它对于 WLAN 安全的需要。

增强的安全保护

增强安全解决方案利用针对每个用户、每个会话的动态 WEP 密钥来阻止未经授权的网络访问。该解决方案建立在 802.1x 身份认证框架和 EAP 的基础之上，可以提供基于用户的身份认证。它弥补了第一代静态 WEP 密钥和基本安全保护的所有不足。

为了部署大规模的企业 WLAN，网络管理员需要可扩展的、轻松的管理方案，以避免加重人员的工作负担。增强的安全保护可以提供一个这样的解决方案，同时还可以阻止各种精心策划的被动或者主动的 WLAN 攻击，消除对于管理静态 WEP 密钥的需要。这种强大的企业级 WLAN 安全解决方案可以将服务质量和移动性集成到它的框架之中，从而可以支持一组更加丰富的企业级应用。

思科新推出的无线安全套件采用了一种增强的安全解决方案。思科扩展了 EAP，创建了 Cisco LEAP，它也被称为 EAP Cisco Wireless。思科无线安全套件的企业级安全架构包括双向身份认证、消息完整性检查（MIC）、逐个分组密钥散列、基于策略的密钥旋转、初始化向量（VI）变化，以及远程拨号用户认证服务（RADIUS）记账记录的可用性。

因为它是一种增强的安全解决方案，所以网络管理员可以确信，思科无线安全套件将为他们提供企业级的安全和保护。

专业安全保护

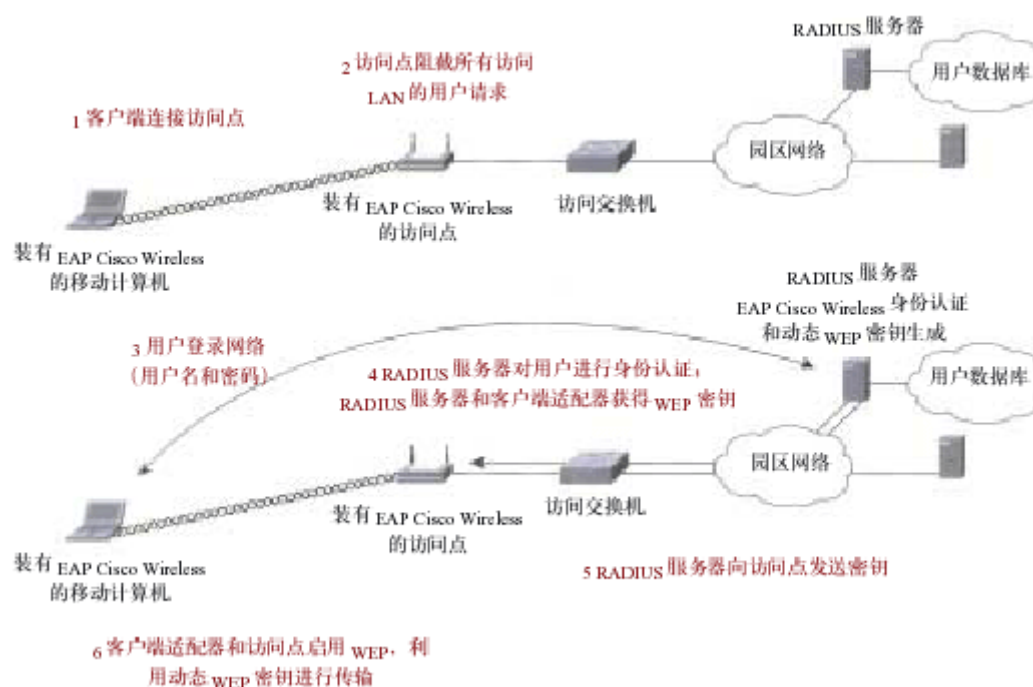
在某些情况下，企业可能需要端到端的安全性来保护他们的业务应用。管理员可以利用专业安全保护建立一个虚拟专用网（VPN），让身处公共场所（例如机场和宾馆）的移动用户可以通过隧道访问企业网络。为了建立一个安全的 VPN，

管理员必须特别注意隧道、加密、分组完整性、防火墙、用户和设备认证，以及网络管理等。这个解决方案需要一个 VPN 终端。

大多数企业都不需要在他们的内联网中部署一个专业安全 WLAN。有些特殊行业，例如需要采取广泛的安全措施的金融机构，可能需要部署专业安全解决方案和增强的安全方案。但是对于绝大多数企业网络来说，思科无线安全套件所提供的安全更加适用，因为它可以避免建立 VPN 所需要的开支和费用。

思科的 SAFE 蓝图可以为那些想要利用 EAP Cisco Wireless 部署一个增强式安全解决方案或者利用 VPN 部署一个专业安全解决方案的网络设计人员提供指导。SAFE 蓝图是一种模块化的方法，可以有效地保障那些指定了安全设计、部署和管理流程的 WLAN 网络的安全。

图注： EAP Cisco Wireless 双向认证和集中式 WEP 密钥管理



利用思科无线安全套件免除烦恼

对于正在寻找一个安全的无线网络的企业来说，采用思科无线安全套件的增强式安全解决方案正在成为业界最主要的选择。在正确配置和启用了新的思科无线安全套件的各种特性以后，网络管理员可以确信，他们的数据将会非常安全。

利用双向认证和动态 WEP 密钥，新的思科无线安全套件为企业局域网管理员们提供了将无线技术引入网络所需要的信心。它的高度的灵活性使网络管理人员可以自行选择自己需要的保护等级，并且非常牢固，足以提供一个安全框架，并围绕这个框架建立整个安全解决方案。它的安全管理非常方便，因而不会加重 IT 人员的管理负担。

一个员工要想安全地连接到思科无线安全套件只需要一个 Cisco Aironet 系列 WLAN 客户端适配器（访问卡）、启用了安全特性的新型 Cisco Aironet 客户端工具（ACU），以及针对特定的覆盖区域的服务集标识符（SSID）。WLAN 基础设施包括一个运行着思科无线安全套件的 Cisco Aironet 系列访问点和一个认证、授权和记账（AAA）RADIUS 服务器。只需点击一个按钮，文件就可以从员工的计算机，通过 Cisco Aironet WLAN 客户端适配器发送到运行着思科无线安全套件并连接到 RADIUS 服务器的 Cisco Aironet 访问点。整个过程没有任何

不便，非常安全。

利用新的思科无线安全套件，网络管理人员可以放心地部署一个能够提供强大的企业级 WLAN 安全的无线解决方案。这个解决方案包括了很多来自于 802.11 标准的建议，该标准重新定义了 WLAN 怎样阻止那些对于基于静态 WEP 的系统来说非常有效的攻击。

只有思科的客户端适配器和访问点拥有各种支持动态 WEP 密钥生成、双向认证的增强特性，以及思科无线安全套件的其他一些优点。在采用了思科基础设施、客户端卡、固件/驱动器/工具和 RADIUS 服务器，并且启用了思科无线安全套件以后，就可以全面实施下列安全措施。

EAP Cisco Wireless

Cisco Aironet 产品支持 IEEE 802.1x 标准框架和 EAP，以及 EAP 认证类型，例如 EAP-TLS 和 EAP Cisco Wireless。与基本的 EAP 相比，EAP Cisco Wireless 具有两个重要的优点。

第一个优点是客户端和 RADIUS 服务器之间的双向认证机制，这可以有效地阻止由伪装的访问点发动的"中间人"式攻击。这也有助于确保只有合法的客户端才能连接合法的、经过授权的无线访问点。

EAP Cisco Wireless 的第二个优点是对 WLAN 的集中式密钥管理。在成功地认证了客户端的身份以后，RADIUS 服务器和客户端将获得一个针对用户的 WEP 密钥，客户端将在本次登录会话中使用这个密钥。

对网络攻击的高级防范

思科解决方案可以阻止各种攻击。该解决方案可以防范 AirSnort 攻击和强力攻击，以及通过丢失或者被盗的设备发动的入侵和中间人攻击。

AirSnort 攻击

思科无线安全套件可以通过提供针对分组的密钥散列以及针对主动的重置密钥的集中式策略配置阻止"weak IV"式攻击。这些特性可以防止黑客利用 weak IV 获得足够多的分组以破解密钥。

强力攻击

尽管在理论上存在可能性，但是实际上强力攻击非常难以发起，实际上也不会产生任何效果，这要归功于 Cisco Aironet 针对用户、针对会话的动态 WEP 密钥和频繁的重置密钥功能。而其他使用基于动态 WEP 的系统的厂商则很容易受到这种攻击的威胁。

通过丢失或者被盗的设备发动的攻击

思科无线安全套件可以最大限度地降低由于损失设备和网络接口卡（NIC）而带来的风险。在我们基于 802.1x 的架构中，思科的认证对象是用户，而不是 NIC 卡。

中间人攻击

这种攻击可能是主动式或者被动式的。Cisco Aironet 的双向认证机制（EAP Cisco Wireless）可以阻止这种攻击。企业可以放心地部署思科解决方案，而无须担心来自伪装的访问点的威胁。用户密码和会话密钥在无线链路上决不会用明文传送。在这种情况下，无须管理员干预，终端用户就可以自动获得一个独特的会话密钥，从而以一种加密的方式获得对网络的访问。管理员可以通过安排他们的 WLAN，根据他们的需要，每隔一段时间重新进行一次身份认证。

IEEE 802.11 安全任务组（TGi）已经将 802.1x 和 EAP 集成到了它的基本安全框架中。在启用了这些 802.1x 安全特性以后，一个连接到某个访问点的无线客

户端只有在用户通过企业 RADIUS 服务器的身份认证以后才能获得对网络的访问权限。

很多第三方 AAA RADIUS 服务器现在也可以支持 Cisco Aironet 安全框架, 包括对 EAP Cisco Wireless 双向认证的支持。这些服务器, 加上思科安全访问控制服务器 (ACS) 和思科访问注册器 (AR), 可以帮助网络管理员灵活地选择后端服务, 而不需要降低 WLAN 的安全性。

利用针对分组的密钥散列阻止 "Weak IV" 式攻击

思科无线安全套件可以组织很多类型的攻击, 其中包括通过分析一串使用相同密钥的加密流量中的多个不安全的初始化向量而发动的 Weak IV 式攻击。利用客户端和访问点都支持的高级散列技术, WEP 密钥会在每个分组的基础上动态变化, 从而有效地阻止这种攻击。IV 和 WEP 密钥都会被散列, 以生成一个独特的分组密钥, 这可以防止黑客利用不安全的 IV 获得 WEP 密钥。

为了防止利用 IV 冲突而发动的攻击, 必须在 IV 发生重复之前更改 IV 密钥。由于在一个繁忙的网络上 IV 可能会几个小时重复出现一次, 所以管理员可以利用像 EAP Cisco Wireless 这样的机制进行重置密钥操作。

消息完整性检查

对 WEP 的另外一个担忧是它对重复攻击的抵抗能力。思科无线安全套件可以执行消息完整性检查 (MIC) 来防止 WEP 帧受到修改。Cisco Aironet WLAN 可以利用 MIC 检测并丢弃那些在传输过程中被 (恶意) 修改的分组。由于采用了 MIC 的 Cisco Aironet 产品可以发现并丢弃被修改的分组, 所以攻击者无法利用位切换或者主动的重复攻击来欺骗网络以通过身份认证。

面向组播密钥的基于策略的密钥旋转

利用 Cisco Aironet 的密钥旋转系统, WLAN 可以支持针对用户、针对会话的密钥和广播密钥。单播密钥的重置超时策略在思科安全 ACS (基于 Windows) 或者 Cisco AR (基于 UNIX) 集中配置。这个密钥旋转过程对于用户来说是透明的。网络管理人员可以在访问点配置组播密钥旋转策略。

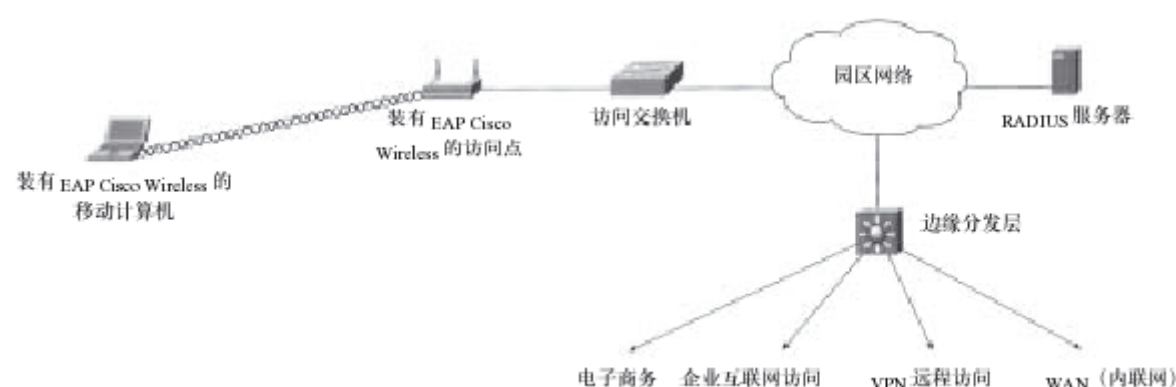
RADIUS 记账记录

思科无线安全套件的另外一个附加特性是能够为每个客户端进程生成详细的 RADIUS 记账记录。这些记录可以被发送到 AAA 服务器, 用于记录、审计和针对 WLAN 的使用收取费用。企业还可以利用这些数据审查账目。

尽管没有哪种 WLAN 安全方法是 100% 无懈可击的, 但是思科无线安全套件可以为企业环境提供强大的安全性。在采用了思科无线安全套件以后, 企业员工可以安全地使用无线网络, 随时随地投入工作。

对园区和边缘服务的安全 WLAN 访问

图注: 园区网络



值得您信赖的灵活性

Cisco Aironet 系列可以作为一个无线层无缝地集成到现有的网络中，或者重新创建一个能够迅速地、经济有效地实现移动性的纯无线网络。利用 Cisco Aironet 产品，企业可以方便地频繁改动 LAN，克服由于较旧的建筑物、租用场所或者临时性办公地点所带来的限制。

Cisco Aironet 系列产品通过了无线以太网兼容性联盟（WECA）的 Wi-Fi 互操作性认证，可以与其他 IEEE 802.11b 产品进行无缝的集成。这简化了网络管理人员和技术支持人员的部署流程。但是同时需要指出的是，思科无线安全套件只能支持基于思科技术的产品。

无线网络可以带来很好的经济效益

可想而知，您必须根据特定的预算条件来制定每项决策。这就是为什么 Cisco Aironet 产品会如此适用于企业网络管理员。随着技术的不断发展，无线网络的成本将逐渐低于传统有线局域网的成本。这是由于无线网络避免了重新布置房间、改造建筑物和解决其他一些 IT 部门每天都必须面对的困难所需要的成本。当网络需要改动时，网络管理人员只需要在房间中放入另外一台工作站，并装上一个 Cisco Aironet 客户端卡，就足以增大网络的规模--不需要铺设昂贵的线路。

利用 Cisco Aironet 无线网桥，还可以降低连接远程建筑物的成本。它们可以在以太网之间提供高速的、长距离的建筑物间无线连接，从而节约大量的时间和安装专线的成本。

第 8 章、Cisco Aironet 扩频无线网络产品

计算机无线网络产品目前已有多家生产，例如美国的 Cisco Aironet，AT&T，DEC，Motorola, Solectek, Xirocom 公司，且都符合 IEEE802.3 协议 (Ethernet，以太网) 或 802.5 协议 (TokenRing，令牌网)，可以方便地用于遵从上述协议的多种网络环境，具有良好的组网能力。

本文以品种较齐全的 Cisco 公司的 Aironet 无线网络系列产品为例，介绍无线网络产品的种类、性能及适用场合。为适合多种场合的适用需要，该系列产品有多种无线网卡，无线访问点和无线网桥，其产品的主要设计指标是：

一、扩频收发工作站



(1) 无线网桥：

型号 BR340

- 特性 ◆在 30 公里可视范围内无线桥接多段以太网。
- ◆第二代多通道直序扩频技术，每个通道速率高达 2-11M。
- ◆点对点 and 点对多点特性。

支持 SPANNING TREE 协议。

使用 IE 浏览器远程配置、诊断、优化和管理无

线系统。

- ◆无线网、以太网流量、出错情况统计，日志记录。
- ◆中继点和节点速率和频率的自动切换。
- ◆节点自动/定向登录，点对点 / 广播链路测试。
- ◆32 位系统标识码及 10 位数据加密传递。
- ◆遵循 SNMP MIB I 和 MIB II 标准。
- ◆有效、紧凑、结实的单件设计同样适合在办公室和工厂使用。

规格及性能

- ◆无线扩频方式：直接序列扩频 (DSSS)。
- ◆调制方式：BPSK、QPSK、CCK、MBOK。
- ◆频率范围：2.4-2.4835G
- ◆数据速率 BR2200 BR100 2M, BR500 11M
- ◆通道数：5-11 个 (3 个非交叠)
- ◆中央处理器：25MHz 摩托罗拉 68360
- ◆RF 输出功率：100MW (FCC)
- ◆接收灵敏度：-86dB (11M)、-93dB (1M)。
- ◆系统内存：标准为 1M
- ◆只读闪存：256K

网络支持

- ◆有线网络协议：IEEE802.3/802.5
- ◆有线网络连接：10Base2 (BNC), 10BaseT (RJ45), 10Base5 (AUI)
- ◆有线网络容量：10Mbps
- ◆有线网络过滤：按节点地址、网络协议、多目地址等进行智能包过滤。

- ◆无线网络协议：IEEE802.11 或基于 CSMA/CA 的专利微蜂窝结构(TMA)。
- ◆无线网络漫游：有专利 TMA 支持。
- ◆无线接入数目：128-2048 个点（部分网桥可限制）。

配置及管理

- ◆本地配置：通过串行口(DB-9 母头)。
- ◆远程配置：通过 Telnet, FTP, SNMP, HTML 命令。
- ◆自动配置：通过 BOOTP 或 DHCP
- ◆SNMP 遵循：MIB I 和 MIB II。
- ◆指示灯：无线、有线网络及链路工作情况。开机显示无线连通品质情况。

物理特性

- ◆尺寸：20X15X5cm
- ◆重量：0.7kg
- ◆电源：输入 90-260V, 50/60Hz, 输出 12-18V/1A, 功率<20W
- ◆温度：-20℃至+50℃ 湿度：95%
- ◆符合规定：FCC Part 15, Class B, FCC Part 15.247



(2) 无线访问点

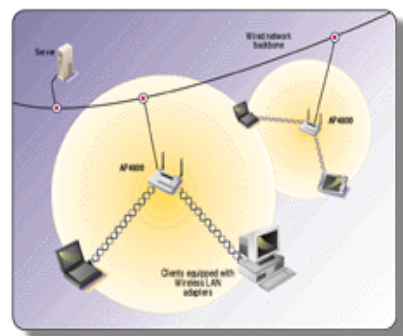
型号 AP340

- 特性
- ◆在 30 公里视通范围内无线连接多个用户单元。
 - ◆第二代多通道直序扩频技术，每个通道速率高达 2-11M。
 - ◆点对点和点对多点特性。

- ◆符合 IEEE 802.11d 工业标准 SPANNING TREE 协议。
- ◆通过 Telnet, FTP, SNMP 或使用 IE 浏览器远程配置、诊断、优化和管理无线系统。
- ◆无线网、以太网流量、出错情况统计，日志记录。
- ◆中继点和节点速率和频率的自动切换。
- ◆节点自动/定向登录，点对点 / 广播链路测试。
- ◆32 位系统标识码及 10 位数据加密传递。有三套 SID 标识系统供用户使用。
- ◆遵循 SNMP MIB I 和 MIB II 标准。
- ◆有效、紧凑、结实的单件设计同样适合在办公室和工厂使用。

规格及性能

- ◆无线扩频方式：直接序列扩频 (DSSS)。
- ◆调制方式：BPSK、QPSK、CCK。
- ◆频率范围：2.4-2.4835GHz
- ◆数据速率：AP330 2M
AP340 11M
- ◆通道数：5-11 个（3 个非交叠）
- ◆RF 输出功率：100mW (FCC)
- ◆接收灵敏度：-86dB (11M)、-93dB (1M)。
- ◆系统内存：标准为 1M
- ◆只读闪存：256K
- ◆通道数：5-11 个（3 个非交叠）



- ◆RF 输出功率：100MW（FCC）
- ◆接收灵敏度：-86dB（11M）、-93dB（1M）。
- ◆系统内存：标准为 1M
- ◆只读闪存：256K

网络支持

- ◆有线网络协议：IEEE802.3
- ◆有线网络连接：10Base2(BNC), 10BaseT(RJ45), 10Base5(AUI)
- ◆有线网络容量：10Mbps（在 Root 状态 AP 系列方能接入有线）。
- ◆有线网络过滤：按节点地址、网络协议、多目地址等进行智能包过滤。
- ◆无线网络协议：IEEE802.11 或基于 CSMA/CA 的专利微蜂窝结构(TMA)。
- ◆无线网络漫游：有专利 TMA 支持。
- ◆无线接入数目：128-2048 个点

配置及管理

- ◆本地配置：通过串行口(DB-9 母头)。
- ◆远程配置：通过 Telnet, FTP, SNMP, HTML 命令。
- ◆自动配置：通过 BOOTP 或 DHCP
- ◆SNMP 遵循：MIB I 和 MIB II。
- ◆指示灯：无线、有线网络及链路工作情况。开机显示无线连通品质情况。

物理特性

- ◆尺寸：20X15X5cm
- ◆重量：0.7kg
- ◆电源：输入 90-260V, 50/60Hz, 输出 12-18V/1A, 功率<20W
- ◆温度：-20℃至+50℃ 湿度：95%
- ◆符合规定：FCC Part 15, Class B, FCC Part 15.247



(3) 无线网卡

型号 PCI2200 PCI4500 PCI4800

- 特性
- ◆在可视范围内无线连接无线访问点。
 - ◆第二代多通道直序扩频技术，每个通道速率高达 2-11M。
 - ◆点对点特性。

- ◆符合 IEEE 802.1d 工业标准 SPANNING TREE 协议。
使用 Adhoc 协议，无线网卡之间可以相互通信。
- ◆通过主机平台专用软件方能配置、诊断、优化和管理无线网卡。
- ◆节点速率和频率的自动切换。
- ◆节点自动/定向登录，可作点对点测试。
 - ◆32 位系统标识码及 10 位数据加密传递。有三套 SID 标识系统供用户使用。
 - ◆遵循 SNMP MIB I 和 MIB II 标准。
 - ◆主要适合在办公室等室内使用。

规格及性能

- ◆无线扩频方式：直接序列扩频（DSSS）。

- ◆调制方式: BPSK、QPSK、CCK。
- ◆频率范围: 2 • 4-2 • 4835G
- ◆数据速率: PCI2200 PCI4500 2M
PCI4800 11M
- ◆通道数: 5-11 个 (3 个非交叠)
- ◆RF 输出功率: 100mW (FCC)
- ◆接收灵敏度: -86dB(11M)、-93dB (1M)。

网络支持

- ◆有线网络协议: IEEE802 • 3
- ◆有线网络过滤: 按节点地址、网络协议、多目地址等进行智能包过滤。
- ◆无线网络协议: IEEE802. 11 或基于 CSMA/CA 的专利微蜂窝结构 (TMA)。
- ◆无线网络漫游: 有专利 TMA 支持。
- ◆无线接入: 只能连接无线访问点, 不能再接入其他用户。
Adhoc 状态可以单用户单元之间作广播式互连。

配置及管理

- ◆本地配置: 通过主机平台专用软件方能配置、诊断、优化和管理无线网卡。
- ◆自动配置: 通过 BOOTP 或 DHCP
- ◆SNMP 遵循: MIB I 和 MIB II。
- ◆指示灯: 有网络及链路工作情况。

物理特性

- ◆尺寸: 14. 7X8. 7X13cm
- ◆重量: 0. 13kg
- ◆结构: PCI 总线
- ◆电源: 5V/800mA
- ◆符合规定: FCC Part 15. 107/15. 109, Class B,



(四) 网络适配器 (单用户单元)

型号 UC2200 UC4500 UC4800

特性 ◆在 30 公里视通范围内无线连接无线访问点。

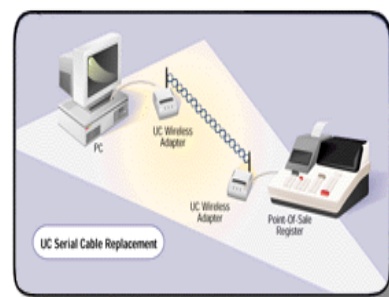
◆第二代多通道直序扩频技术, 每个通道速率高达 2-11M。

◆点对点 and 点对多点特性。

- ◆符合 IEEE 802. 1d 工业标准 SPANNING TREE 协议。
使用 Adhoc 协议, 单用户单元之间可以相互通信。
- ◆通过 Telnet, FTP, SNMP 或使用 IE 浏览器远程配置、诊断、优化和管理无线系统。
- ◆无线网、以太网流量、出错情况统计, 日志记录。
- ◆节点速率和频率的自动切换。
- ◆节点自动/定向登录, 点对点 / 广播链路测试。
- ◆32 位系统标识码及 10 位数据加密传递。有三套 SID 标识系统供用户使用。
- ◆遵循 SNMP MIB I 和 MIB II 标准。
- ◆有效、紧凑、结实的单件设计同样适合在办公室和工厂使用。

规格及性能

- ◆无线扩频方式：直接序列扩频（DSSS）。
- ◆调制方式：BPSK、QPSK、CCK。
- ◆频率范围：2.4-2.4835GHz
- ◆数据速率：UC2200 UC4500 2M
UC4800 11M
- ◆通道数：5-11 个（3 个非交叠）
- ◆RF 输出功率：100mW（FCC）
- ◆接收灵敏度：-86dB（11M）、-93dB（1M）。



网络支持

- ◆有线网络协议：IEEE802.3
- ◆有线网络连接：10BaseT(RJ45)
- ◆有线网络容量：10Mbps
- ◆有线网络过滤：按节点地址、网络协议、多目地址等进行智能包过滤。
- ◆无线网络协议：IEEE802.11 或基于 CSMA/CA 的专利微蜂窝结构(TMA)。
- ◆无线网络漫游：有专利 TMA 支持。
- ◆无线接入：只能连接无线访问点，不能再接入其他用户。
Adhoc 状态可以单用户单元之间作广播式互连。

配置及管理

- ◆本地配置：通过串行口(DB-9 母头)。
- ◆远程配置：通过 Telnet, FTP, SNMP, HTML 命令。
- ◆自动配置：通过 BOOTP 或 DHCP
- ◆SNMP 遵循：MIB I 和 M18 II。
- ◆指示灯：无线、有线网络及链路工作情况。开机显示无线连通品质情况。

物理特性

- ◆尺寸：13.8X10.5X5.4cm
- ◆重量：0.358kg
- ◆电源：输入 90-260V, 50/60Hz, 输出 12V/0.8A, 功率<15W
- ◆符合规定：FCC Part 15, Class B, FCC Part 15.247



(5) 笔记本无线网卡

型号 PC2200 PC4500 PC4800

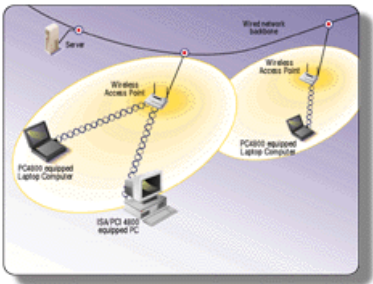
- 特性
- ◆在可视范围内无线连接无线访问点。
 - ◆第二代多通道直序扩频技术，每个通道速率高达 2-11M。
 - ◆点对点特性。

- ◆符合 IEEE 802.11 工业标准 SPANNING TREE 协议
使用 Adhoc 协议，无线网卡之间可以相互通信。
- ◆通过主机平台专用软件方能配置、诊断、优化和管理无线网卡。
- ◆节点速率和频率的自动切换。
- ◆节点自动/定向登录，可作点对点测试。
- ◆32 位系统标识码及 10 位数据加密传递。有三套 SID 标识系统供用户使用。
- ◆遵循 SNMP MIB I 和 M18 II 标准。

◆主要适合在办公室等室内使用。

规格及性能

- ◆无线扩频方式：直接序列扩频（DSSS）。
- ◆调制方式：BPSK、QPSK、CCK。
- ◆频率范围：2.4-2.4835G
- ◆数据速率：PC2200 PC4500 2M
PC4800 11M
- ◆通道数：5-11 个（3 个非交叠）
- ◆RF 输出功率：100MW（FCC）
- ◆接收灵敏度：-86dB（11M）、-93dB（1M）。



网络支持

- ◆有线网络协议：IEEE802.3
- ◆有线网络过滤：按节点地址、网络协议、多目地址等进行智能包过滤。
- ◆无线网络协议：IEEE802.11 或基于 CSMA/CA 的专利微蜂窝结构（TMA）。
- ◆无线网络漫游：有专利 TMA 支持。
- ◆无线接入：只能连接无线访问点，不能再接入其他用户。
Adhoc 状态可以单用户单元之间作广播式互连。

配置及管理

- ◆本地配置：通过主机平台专用软件方能配置、诊断、优化和管理无线网卡。
- ◆自动配置：通过 BOOTP 或 DHCP
- ◆SNMP 遵循：MIB I 和 MIB II。
- ◆指示灯：有网络及链路工作情况。

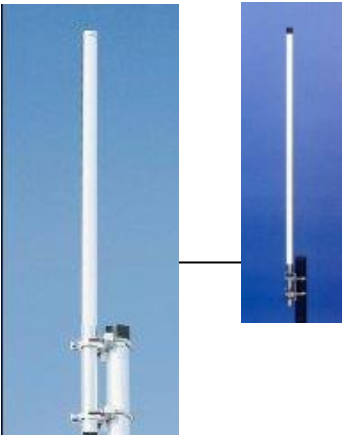
配置及管理

- ◆本地配置：通过主机平台专用软件方能配置、诊断、优化和管理无线网卡。
- ◆自动配置：通过 BOOTP 或 DHCP
- ◆SNMP 遵循：MIB I 和 MIB II。
- ◆指示灯：有网络及链路工作情况。

物理特性

- ◆尺寸：5.4X11.1X5cm
- ◆重量：0.045kg
- ◆结构：PCMCIA Type II
- ◆电源：490MA
- ◆温度：-40℃至+85℃ 湿度：95%
- ◆符合规定：FCC Part 15

二、扩频天线馈线系统



(1) 室外天线：

①全向天线

- ◆型号：AIR-ANT4121 ◆增益：12dBi
AIR-ANT2506 5.2dBi
- ◆频率：2.4-2.5G
- ◆激化方式：垂直激化

- ◆驻波比：1.5:1
- ◆输入抗组：50 欧姆
- ◆接口类型：N 型
- ◆波束宽度：360°
- ◆功率输入：50W
- ◆雷电保护：直接接地
- ◆抗风强度：45M/S
- ◆温度：-20℃至+80 湿度：100%



②定向天线

- ◆型号：AIR-ANT1949 (Yagi) ◆增益：13.5dBi
- ◆频率：2.4-2.5G
- ◆激化方式：垂直
- ◆驻波比：1.5:1
- ◆输入抗组：50 欧姆
- ◆接口类型：N 型
- ◆波束宽度：AIR-ANT1949 30°
- ◆功率输入：50W
- ◆雷电保护：直接接地
- ◆抗风强度：45M/S
- ◆温度：-40℃至+80 湿度：100%

第 9 章、无线网络典型联接方式与实例

第一章讲述了无线网络产品系列及其关网络功能、使用方法和适用场合。无线网络产品的多种使用方式可以组合出适合各种情况的无线联网设计，可以方便的解决许多以线缆方式难以联网的用户需求。例如，数十公里远的两个 LAN 相联：其间或有河流、湖泊相隔，拉线困难且线缆安全难保障，或在城市中敷设专线要涉及审批复杂、周期很长的市政施工问题，无线网能以比线缆低几倍的费用在几天内实现，无线网也可方便的实现不经大的施工改建而使旧式建筑具有智能大厦的功能。

无线网络应用的典型方式是：

1、点对点方式。有 2 种形式，把 1 个远程站点联入 1 个 LAN；把 2 个 LAN 相联。如果是两个 LAN 相联，则在两个 LAN 中分别接入无线路由器或无线网桥；如一边是单机，则在其机内插入无线网卡即可。视通信距离联接相应天线，以无线网络软件设置相应的 ID 号、中端号和地址，即可调试天线的方向、角度。当无线网络软件指示接收质量为良好或合用时，即认为无线链路接通，双方可做网络设置和操作了。

如你的网中已有路由器，而且天线距网络有相当距离，如数十米至数百米，则应使无线网桥尽量靠近天线以缩短射频电缆长度、降低射频信号衰减，把无线网桥和路由器以数字线缆相联。这种方式的一种扩展是在两点间如距离过远或有遮挡时，在中间增加了一个无线路

由器来做中继。网络的设置也作相应变动。

2、无线 HUB 方式。在一个建筑物或一个不大的区域内有多个定点或移动点要联入一个 LAN 时,可用此方式。要注意的是:各站点要与无线转接器(Access, HUB)用相同的网络 ID 以支持解扩,又要有各自的地址号以相区别。

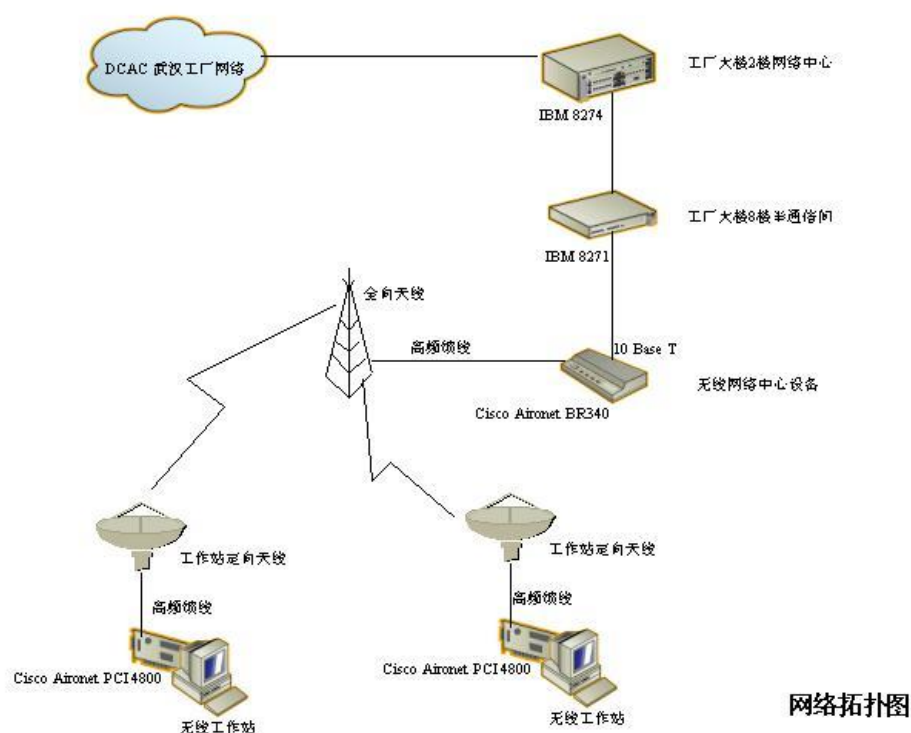
3、一点多址方式当要把地理上有相当距离的多个 LAN 相联时,则可在每个 LAN 中接入无线网桥。这时主站或转接站使用全向天线,各从站视距离使用定向或全向天线与之相联。各无线网桥均使用同样的网络 ID 以支持扩频通信,使用各自的地址(网段)以相区别。正确的网络设置,可以使各工作站,服务器之间互访。当需把 10km 之内的多个定点站点或 2km 之内的多个活动站点(各站点均是单机)联入网内时,可以用无线网桥的 HUB 工作方式来实现。

4、不同协议网络间互联。在联网的两边各用与当地网络环境和对方网络环境相套配的设备 and 相应的网络设置即可实现。其通信部分和前述的相同。上述只是几种典型联网方式,在实际工作中可以组合使用,变化出很多具体的形式。以上用法中涉及到的网络操作部分与有线网是相同的,本文认为读者有有线联网的知识。

这里介绍几种不同无线网产品一些较典型的用法以供参考。

一、CISCO AIRONET

例一、武汉某公司无线网



根据厂区的具体情况,考虑到铺设光纤的工程量较大,而且投资较多,可采用无线网技术,利用该技术建网方便灵活,可保护投资,更方便以后类似物理环境网络的扩展。

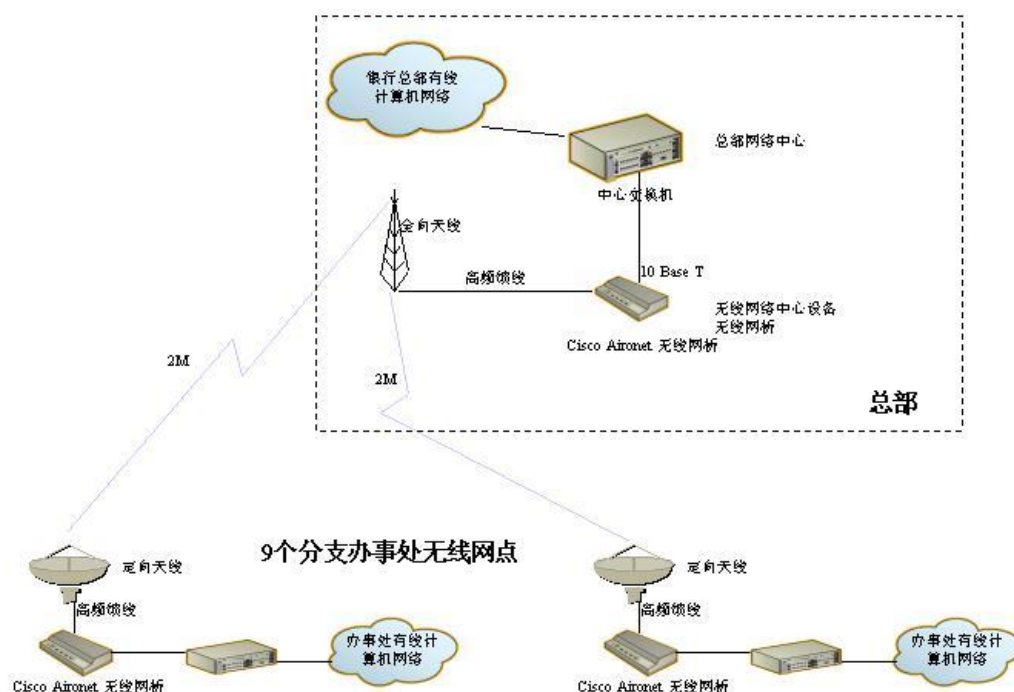
利用管理大楼在厂区内的优势,采用上面介绍的无线扩频网的第一种应用方式,由电脑网络中心通过无线通信覆盖车库和货场两个点位,通过网络中心的无线网桥,将无线网连接到网络中心的局域网中,这样,车库和货场两个点位的计算机便可以与网络中心的服务器进行通信了。

采用了 Cisco Aironet 无线网络产品,包括无线访问点、网卡、全向和定向天线等,具体的配置如下:

- 在管理大楼 8 楼半通讯间(与楼顶距离 30M)左右放置一台 CISCO AIR-BR342 无线访问网桥,可以提供 11M 的无线数据传输速率,该设备背板有一个 10BASE-T 的以太网口,通过双绞线跳线连接 IBM 8237 交换机,可将无线网连入中心局域网, CISCO AIR-BR342 可以连接多大 2048 个无线用户端设备,完全可以满足该无线网的扩展需求。
- 在管理大楼顶楼斜顶平台安装一个增益为 5.2Dbi 的全向天线,提供覆盖厂区的无线电波,通过长约 30 米的低损同轴电缆,并加一放大器以提供放大的信号,连接中心的 AIR-BR342 无线访问网桥,利用防雷接地设备,确保了设备的安全。

在车库及货场的计算机各安装一块 AIR-PCI4800 无线网卡,通过一 13.5DBi (Yagi) 定向天线接收网络中心 AIR-BR342 无线访问网桥发射的无线信号,可与中心网络保持通信,由于天线安装在露天地点,因此建议选用防雷保护器。

例二、某工行 O A 系统无线网络系统



某工行无线网络拓扑图

该网络连接网点 9 个,无线网络覆盖半径 10 公里,主要连接 O A 及信贷台帐网络,电子邮箱,部分柜台业务。通信带宽 2 M,最远通信覆盖半径 10 公里左右。网络前后运行一年半,仅有一次线路故障。目前代替 D D N 线路 11 条(64K 9 条,9.6K 3 条),每月节省通信费用近 3 万元,一年共 30 多万元的支出,还没有计算开通所有 D D N 的初装费及设备投入费用。按此推算投入应在 1 年半左右收回。该网络由专人管理,其安全保障与有线网络通信一样,任何人包括设计安装人员在未经网络系统管理员的授权均难侵入该网络。具体方案设计:

根据的具体情况,考虑到铺设光纤的工程量较大,而且投资较多,可采用无线网技术,利用该技术建网方便灵活,可保护投资,更方便以后类似物理环境网络的扩展。

本设计方案采用上面介绍的无线扩频网的点对多点应用方式,在银行总部大楼楼顶安装一根 5.2 dBi 全向天线,提供覆盖四周的无线电波信号,通过高频馈线连接 Cisco Aironet 无线网桥,利用该无线网桥背板的 10Base-T 的以太网口,可以将无线网连接到网络中心的局域网中。

在各区点位采用 Cisco Aironet 无线网桥,利用定向天线发射、接收无线信号,与网络中心进行通讯。

另外,考虑到办公大楼与各办事处点位的可视性良好,不需要加中继站将信号放大传播,

本方案采用了 Cisco Aironet 无线网络产品,包括无线网桥、全向天线和定向天线等,具体的配置如下:

- 在银行总部大楼放置一台 AIR-BR 无线访问网桥,可以提供 2M 的无线数据传输速率,该设备背板有一个 10BASE - T 的以太网口,可将无线网连入中心局域网。
- 在银行总部大楼楼顶平台安装一个增益为 5.2Dbi 的全向天线,提供覆盖四周的无线电波,通过的低损同轴电缆,连接中心的 AIR-BR 无线网桥,利用防雷接地设备,确保了设备的安全。

在各办事处点位各配置一台 AIR-BR 无线网桥和一套增益为 13.5Dbi 的定向天线,利用背板 10BASE-T 以太网端口连接该办事处的有线局域网,将数据信息通过无线网连接与总部的计算机网络进行通讯。

二、其它无线网案例

例 1:

要把 A 地的一个工作站联入 10km 以外 B 地的一个有线网,传输速度要求不低于 1Mbps。其地理环境是 A 地为 2 层楼,但临近有 9 层楼, B 地为 10 层楼,其间有遮挡,但满足通信要求。其网络环境为 Novell 网络操作系统(Ethernet)。

联网方法是:在有线网中接入无线路由器,在 A 地的计算机内插入无线网卡(Internet);两边各用一个增益为 20dBi 的直径 60cm 的抛物面天线, A 地天线架在临近高楼的顶层, B 地天线架在本楼顶层。以射频电缆联接天线与各自无线网卡的接口上。两边已分别设置好网络 ID、中断向量、地址(在同址完成网络联通)。借助无线网的测试软件调整天线的方向与角度,当测试软件指出通讯状态为良好时,安装工作即告完成,网络操作系统的运行和有线网相同,网络操作完成是透明的。在实际工作中,当无线网联通后, A 地的单机换成了路由器,以使 A 地的单机可以随着工作的发展方便的扩展成一个局域网。

例 2:

把高能物理所的 Internet(国际互联网)网站联到 18 公里外的国际会议中心,并要求高可靠性和良好畅通。国际物理年会的轻光子会议在国际会议中心举行,有数百外国专家出席并要求通过计算机网与其工作室相联系,存取、查询和互相交流存储于各自计算机中的资料。因此以电话线联网在传输速率、可靠、方便(离开会只有十余天)方面均不能满足要求,故我们采用无线联网方案。

其地理环境是:高能物理所计算站是 2 层楼,国际会议中心是 40m 高的 8 层楼,其间高楼林立,两点间微波路径被挡。故我们以距高能所 3km 远的电子部 30 层楼做中继,以保证天线之间可视或基本可视。

联网方法是:在高能物理所的网络(通过卫星与国际 Internet 相联)上接入无线网桥,天线安装于 2 层楼顶,电子部的网络中接入无线网桥(通过路由器)使高能物理所与电子部网络相联,并具有路由选择功能,再在电子部的网络中接入用于与国际会议中心相联的无线网桥,为方便,其天线设在了机房内窗前,采用的是 20dBi 增益的 60cm 抛物面天线。在国际会议中心安装 4 台 HP 工作站、26 台终端和 Cisco 路由器,环境为 Unix 操作系统,通过无

线网桥(放在楼顶, 室外)以 27dBi 增益天线和电子部相联, 无线网桥和机房相距 120m。运行效果很好, 链路通畅、可靠, 始终未见丢包现象, 在国际会议中心的终端或工作站上, 通过无线网络与 Internet 联接, 在国际间方便、快捷的检索和传送, 其内容即有文字也有图象。该工作中涉及的计算机均运行 Unix 系统, 使用 TCP/IP 协议, 在各无线网桥中做了相应设置。

例 3:

在一定的区域内把多个活动站点联入网内。

其地理环境是: 某港口集装箱码头的 3000mX300m 区域内有 15-30 个活动站点, 其间无大的遮挡。视采用的设备与造价, 可以有多种实现方案。我们采用的联网方法是: 在 3000m 的区间中设 2 个相距 1400m 左右的无线网桥(Bridge Plus), 采用 6dBi 增益的全向天线覆盖整个区域。活动站点机内使用无线网卡(In-ternal)及 6dBi 增益全向天线。网桥和各活动站点均使用相同的网络 ID 和各自的网络地址。当活动站点从 1 个网桥的覆盖区移向另一个时, 无线网络单元会自动检测信号强度而视需要转换通信点, 这样每个活动站均可无间隙地访问网络。并在全区域内互不干扰的同时与网络保持联通。该方法的好处是易于扩大活动站的移动区域且天线费用低廉。当然, 也可用一个无线网桥而同时使用高增益天线, 其工程施工与调试均简便。

例 4:

商业大楼的收费系统。其要求是: 不能在建筑物内作大的施工以保持大楼建筑的原样; 要在不影响营业的情况下, 把各营业组(每层楼约 25 个)的计算机联网; 还要考虑到可能的变动。

采用的方法是在每层楼的大厅中设 2 个无线转接器(Access, HUB), 每个营业组的计算机(使用笔记本或台式机均可)用一个无线网卡和室内天线, 各机 ID 号均相同但有各自的地址。每层只 2 根线缆由窗子穿出联到 4 层的计算站。此工作也可用无线网桥取代无线转接器与计算站网络相联的线缆, 造价虽高, 但可不用线缆与计算站联网。

以无线网络代替有线网还有下列优点: 极易于扩充, 加入新点; 营业布局的变动与网络无关; 大厅内即省去不雅观、难装饰的大量布线, 又免去了线路损坏的可能。

第 10 章、无线联网的现状与发展前景

一、无线网络的需求及实现

依赖电脑, 正是现在许多人的工作方式和几乎一切数据管理、检索、设计的手段。十年前, 便携机的出现, 使人们可以随身带着自己的计算机在任何地方使用它, 使计算机深入到更广的工作场合, 改变了许多人的工作方式。在移动中, 在非办公室环境中“带着自己的工作环境, 在任何需要的地方随时使用”, 是高效率及新工作模式的需要也是计算机日益深入人们的工作与生活方式的必然结果。但随着计算机网络的发展及其间大量可用信息的充实, 计算机单机工作已远远不能满足人们的工作需要对于一台计算机, “没有网络不是真正的计算机”, “网络就是电脑”, 是人们由于工作需要而引伸的“计算机”的概念, 也是社会信息化发展的需要和结果。

在上述需求下, 做为计算机有线网的补充的计算机无线网络发展起来了。其作用是方便地在某个区域中使移动的计算机随时得到网络的支持; 使地域上分离较远的计算机或局域网快速方便的联成一个网络, 特别是当要联网的数据处理设备间有江河、山谷相隔而不易拉线

时；同时也省去了困难且费时的布线、改线，线路易毁坏的难题。

从技术角度看，正是 90 年代初微波扩频技术从军用解密转向民用和作为扩频通讯技术支持手段的超大规模集成电路技术的迅速发展，为低功率微波扩频通信在计算机联网中应用创造了条件，使计算机高质量无线联网和社会广泛应用成为现实。

美国一些技术计算机网络、电讯产品厂家在无线局域网产品的研制方面取得了重大进展：1992 年 AT&R 和 NCR 公司与 Motorola 公司最先推出了各自基于微波扩频技术的无线网络产品；继而 Proxim 公司、Telexsystem(即现在的 Arionet)公司，Solectek 公司等也在 93 年前后推出了自己的产品。而且，越是近来推出产品的公司，其产品的品种和性能也更见完善。到现在，美国生产无线网络产品及组件的公司已达到 20 余家。

日本、欧洲几家公司也分别推出了基于 2.45GHz 微波扩频技术的无线网络产品。我国这方面的研究工作也在进行中。

二、计算机无线网络的应用现状

在美国，计算机无线网络广泛的应用在计算机需要移动办公的地方，以便在任何需要的地方在网络的支持下工作。即“漫游联网”。如在国会的办公室、会议厅、走廊，在无线 HUB(Access)的链接下，只要在使用者的笔记本电脑上装上很小的无线网络的收发装置，如 Par-allel 或 PCMCIA 网卡，就可以在任何时候任何地方，检索网络数据库中各种资源。在医院，医生和护士可以拿着笔记本电脑在病床前实时记录和查询病人的病历，检索药品。工厂车间的工程师可以直接存取公司集中保存的零部件清单、工程图和工作工艺。也可在上述的任一场合，和联网的任何地点发送和接收电子邮件、传真等任何网络能提供的服务。无线网快捷、方便的联网能力在校园网(一个建筑间)的扩建与完善中也得到充分的体现。而在大型会议和展览等临时场合，不必布线，在一天内即可享受联网服务更是方便。在中国，8 月份在国际会议中心召开了 2 个国际物理年会和 Intrnet 协会的会议，参加会议的各国专家，也通过无线网络和 Internet 节点联机，使我们的会议第一次得到国际互联网的支持和服务。

在中国，由于信息化的发展和工作管理模式的差别，使无线网的应用场合与国外有所不同。目前在我国把无线网用于计算机的移动漫游联网的应用不多，而主要用于没有适当线路和不易布线的远距离联网的场合，把相距相当远的两个网络联网。如把分布在不同地域的工厂总部和各分厂联网，或把一个城市的银行与其分布在城市各处的下属机构相联。类似的形式用的很多的还有研究单位和中国专利局这样的信息服务单位，用来和 Internet 网络节点以无线网相联，以实现国际互联网的快速，高层次的检索与通信。

正是由于目前国内无线网的主要用于联接远距离的有限局域网的需求，我们在远距离联网和设备使用方面甚至突破了其原产地的使用界限。

三、计算机无线网络目前存在的问题和解决

计算机无线网络产品目前价格偏高，这是由于其销量远没有有线网络产品大，也是由于从前没有一个可以遵循的工业标准，各厂家基本处在自成系统的开发阶段，整体兼容性差。现在 IEEE802.11 协议的制定，将在很大程度上解决网络物理层和链路层的规范性问题。

相对于相当普遍的无线网服务，无线网适用的软件却很少，这主要是目前缺少相关的标准。在应用层和传输层之间、在链路层和物理层协议到应用层之间缺乏规范的交互手段和存取依据。无线网络因访问协议、解、扩频的延时，通信侦听方式的区别和无线网速率远低于有线网而产生的影响等诸多因素，使无线网络技术难以照搬有线网的规范和软件，因而使无线网适用的软件和功能显得不充分。

从应用上看，无线网络完成实时语言和图象传输还有相当困难，一是目前传输速率不够，二是缺少专用的软硬件设备。当然这也正是无线网络产品正在着重发展的 2 个方向：传输速

率将在近期有较大的提高,而多媒体多路复用器有多个厂家正在开发,有幸的是也有国内的单位在进行项工作。

四、计算机无线网络的标准化

美国 IEEE802 委员会一直在研究制定关于计算机无线网的技术规范,这一工作终于在 1995 年 9 月有了结果:它制定了关于无线网物理层和链路层的 802.11 协议,这就建立了一个开放的标准。802.11 中规定了一个统一的媒介访问控制(MAC)协议,RF 收发器和红外收发器的物理层接口,无线网络厂家在此协议的规范下,将可以推出大量的可互操作的低价格无线网络产品。在有线网中可以方便的检测到两个相冲突的信号在线上产生的异常电信号,而采用 CSMA/CD 协议解决冲突。在无线网中不一定能检测了信号的冲突,802.11 协议针对无线通信作用区域有限这一特定技术因素而采用了 CSMA/CA 协议。它有一整套“请求发送(RTS)”“清除发关(CTS)”和“接收确认(ACK)”的握手规则,以冲突避免的原则使互相碰撞减少到最小,也解决了无线网中特有的网上结点不能完全互相通信时产生的“隐藏节点”的冲突难点。802.11 协议规定了无线网络的帧格式并在其中为接收器提供了指定的物理层传输类型的信息。关于物理层,802.11 支持一种红外传输标准和两种 RF 传输标准。这两 RF 标准均采用 2.4GHZ 的工业、科研和医学频带(ISM 频带,2.4-2.485GHZ),带宽为 83MHZ。对于扩频技术,802.11 规定了跳频(FH)和直扩式(DS)两种工作方式及相应的技术参数。

由于无线网中的计算机的计算要求可以移动和在一定区域内漫游,故 802.11 远比与它相似的 802.3(有线 ETHERNET 协议)复杂。而移动中的计算机怎样选择定的访问节点,802.11 并未规定。开发人员可以建立各自的决策原则并依据该原则并依据该原则决定移动计算机漫游无线网覆盖区域时如何选用访问节点。

五、计算机无线网络的发展与应用的前景

由于 IEEE802.11 协议的制定,使无线网络产品的开发有了工业标准,从而将增加工业界的开发速度与规模,在近期将有更多的生产厂家开发的具有良好兼容性的无线网络产品投放市场,并降低价格。而依据规范开发网络基层到应用层接口的中间件厂家也将有其产品的明确的下层界面,使基层协议与无线网适用软件界面的问题易于解决,提高网络传输层的功能并向无线网应用软件提供更好的支持。著名的无线网络厂商 SOLECTEK 公司的 JONATAN CHEAH 博士认为 802.11 协议的进一步的工作是提出无线网桥,路由器和中继器等更先进设备的标准;

发展更快的数据传输速率,以扩大无线网络的能力和适用范围。在此技术背景和急剧扩大的社会需求的条件下,无线网络将会迅速的为需要在移动中联网及在网间漫游的任何场合;为在不易布线的地方和远距离的数据处理节点提供强大的网络支持。运行于网上的信息将是数据、实时的语音和图象。

到目前为止,计算机无线网产品已有了新的进展:Solectek 公司已推出了基于 IEEE802.11 协议的快速无线网桥,其数率达到 10Mbps,并通过了美国 UL 测试。其 1 点多址能力和地址过滤能力很是先进,实时图象、语音传输也可以很好的解决。45Mbps 的无线网桥正在紧张的开发过程中,预计明年完成,计算机无线网数率低的问题在迅速解决。

第 11 章、计算机无线网技术应用介绍

一、计算机无线网技术适用范围:

1、在不能使用传统走线方式的地方、传统布线方式困难、布线破坏性很大或因历时艺术等原因不能布线的地方;

- 2、有水域或不易跨过的区域阻隔的地方；
- 3、重复地临时建立设置和安排通讯的地方；
- 4、无权铺设线路或线路铺设环境可能导致线路损坏；
- 5、时间紧急，需要迅速建立通讯，而使用有线不方便、成本高或耗时长；
- 6、局域网的用户需要更大范围进行移动计算的地方；

二、应用介绍

1、石油工业。

油矿的地形起伏不平，敷设电缆后不易传导，而且电缆穿过炼油厂可能是潜在的危险。无线网连接可提供从钻井台到压缩机房的数据链路以便显示和输入由钻井获取的重要数据。海上钻井平台由于宽大的水域阻隔，数据和资料的传输比较困难。敷设光缆费又用很高，施工难度很大。使用无线网技术，费用不及敷设光缆的十分之一，效率高，质量好。

2、货场管理。

铁路运输货场和码头货场，由于大型吊车、运输道路和货物通道不能敷设电缆，使用步话机报告货位和货号极易产生差错，无线计算机网络可以使货物情况和资料直接传输到计算机中进行处理大大提高工作效率和服务质量，避免了不必要的差错。

3、医护管理

现在很多医院都有了计算机管理系统、大量的计算机病人监护设备、计算机控制的医疗装置和药品等库存计算机管理系统。计算机无线网络可以使医疗专家和管理者在医院内的任何地方使用移动和手持计算机设备能极力方便的存取这些信息。利用计算机无线网医生和护士在设置计算机专线的病房、诊室或急救中进行汇诊、查房、手术时可以不必要带着沉重的病例，而使用笔记本电脑实时记录医嘱，并传递处置意见，查询病人病例和检索药品。还可以访问中央专家系统以帮助诊断或预测药物的相互作用和反应。

4、工厂的技术处理。

工厂往往不能敷设连到计算机的电缆，在加固混凝土的地板下面也无法敷设计算机电缆，空中起重机使人很难在空中布线，零备件及货物运通道使得也不便在地面布线。这种情况使用数字化制造设备、数字采集装置、机器人设备时应用无线计算机是很合适的工程师和技术人员进行检修、更改产品设计、讨论工程方案以及其他技术处理时，可以利用计算机无线网在工厂车间或厂区的任何地方查阅技术档案、工作工艺和工程图，发出技术指令、请求技术支持，甚至和厂外专家讨论问题。

5、库存控制

仓库零、备件和货物的发送和贮存注册可以使用无线链路直接为条形码阅读器、笔记本电脑和中央处理计算机连接，进行清查货物、更新存储记录和出据清单。

6、展览和会议

在大型会议和展览等临时场合可在极短的时间方便的得到计算机网络的服务。可以通过计算机无线网和世界互联网 Internet 连接并获得所需要的资料。也可以使用移动计算机在网络范围内互通信息、传递稿件和制作报告。

7、金融服务

银行和证券、期货交易业务都需要计算机无线网络的支持，把一个城市的银行与其分布在城市各处的下属机构相连。即使已经有了有线计算机网，为了避免由于线路等出现的故障，仍需要使用无线计算机网做备份。在证券和期货交易业务中价格以及“买”和“卖”的信息变化极为迅速、频繁，利用手持通信器输入信息，通过计算机无线网络迅速传递到计算机、报价服务系统和交易大厅的显示版，管理员、经纪人和交易者可以迅速利用信息进行管理和用手持通信器直接进行交易。避免了用手势、送话器和人工录入及报价而产生的不准确和时间延误所造成的损失。

8、饮食、交通旅游服务

很多餐厅的服务员已经使用步话机或寻呼技术把餐厅中顾客需要的菜通知厨房，厨房也用同样的办法通知餐厅，顾客所需要的菜已经准备好了。这实际只是整个过程的一部分。计算机无线网络可以进一步做到，由餐厅中走来走去的点菜服务员通过手持终端机把顾客的需求送入计算机，把菜单立即打印给厨房并且把做好的菜立即通知给服务员，当然也可以在手持终端机屏幕显示的菜单上直接点菜，结帐时可通过同一个系统及时打印结帐单。当某个品种的菜售完时，厨房也可以立即回应某道菜没有了，而不必等待几分钟才能知道。这样极大的提高了效率，快速的服务和及时的上菜可大大提高座位的周转率及每个座位的销售额。旅馆采用计算机无线网，可以做到随时随地为顾客进行及时周到的服务。登记和记帐系统一经建立，顾客无论在区域范围内的任何地点进行任何活动，比如在酒吧、健身房、娱乐厅或餐厅等都可以通过服务员的手持通讯终端来更新记帐系统。而不必等待复杂的核算系统的结果。

9、竞赛记分系统

计算机无线网可以用来完成场、馆进行的各种竞赛记分的处理、统计、发送和记录存储工作。也适合于一些文艺及其它竞赛的比赛计分系统，特别是在那些多用途并进行多种比赛的场合。由于比赛场地与总记分台或大记分牌之间相隔有相当的不便敷设电缆的场地(如体育场的跑道)，往往只能采取由服务员将记分单人工传递，然后进行处理、统计、录入并发送数据和显示出来，时间较长，易出差错。用计算机无线网系统来完成处理、统计、发送和显示工作，可以不必花昂贵的钱安装管道、敷设专用线路(而且今后还不能移动)，效率高、质量好。

10、移动办公系统

在办公环境中使用计算机无线网络系统，可以使办公用计算机具有移动能力，在网络范围内可实现计算机漫游。各种业务人员、部门负责人、工程技术专家和管理人员，只要有可移动计算机或笔记本电脑，无论是在办公室、资料室、洽谈室，甚至在宿舍都可通过计算机无线网络随时查阅资料、获取信息，通过网上强大的通讯功能和其他人商讨技术关键、修改原有的技术方案，甚至可以发出越洋邀请和国际上的专家会商和研究问题，领导和管理人员可以在网络范围的任何地点发布指示，通知事项，联系业务，更新记录。也就是说可以随时随地用移动方式办公。

第 12 章、总结

做为一个著名的网络厂家，3Com 公司具有全线的无线局域网络产品线，包括宽带家庭网关，无线工作组网桥，中小企业无线访问系统 AP6000，大中型企业无线访问系统 AirConnect 以及 AP8000，大楼到大楼的无线网桥以及丰富的无线网卡，其中 XJACK 可伸缩天线网卡更是 3Com 的专利产品。

采用 3Com 的丰富无线网产品线可以很灵活的满足用户的组网需求，在提供高性能的同时，还保证很好的安全性，即支持基于 802.11b 标准的安全机制，又支持动态安全链路，VPN，以及基于 802.1x 的增强性安全或认证功能。

3Com 的全线产品具有简单安装，简单使用，简单管理/维护的特点，适合于各种层次的网络环境使用。

3Com 公司的无线产品都通过 Wi-Fi 认证，因此不管是无线访问点，还是无线网卡都能与其它厂家通过 Wi-Fi 认证的产品互操作。

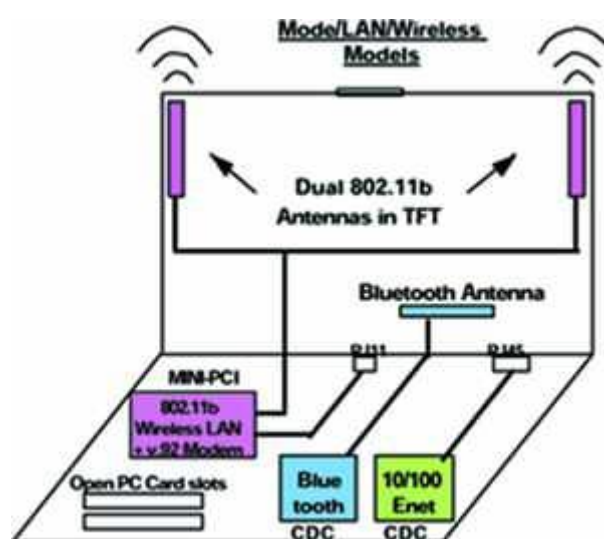
3Com 公司除提供无线局域网产品之外，还提供全线的企业网络交换产品，Web 支持工具。有线网络做企业的骨干，无线网络做骨干网的延伸，扩展和增强，相互补充，从而可以提供完整的企业网络解决方案。

第八章、无线网络产品选购指南

如今，无线设备的数量正在激增，无论是在办公室、会议室、机场、酒店，还是在舒适的家中，人们都能随时随地接入无线网络。为了更好地满足这种需求，很多 IT 厂商都推出了支持无线技术的产品，现在的市场中已经有了丰富的无线网络产品可供选择。然而，更多的用户并不清楚如何选购产品，下面让我们领略一下市场上无线主流的产品。

* 集成 802.11b 无线网卡和“蓝牙天线”

无线局域网是目前最为成熟的无线网络应用类型，其现行的行业标准“802.11b”，该名称定义来自于 IEEE（电气和电子工程师协会）。目前的笔记本电脑都具有支持这种标准的功能。而蓝牙无线技术可以简便地实现电脑、手持电脑、手机、网络访问设备和其他无线设备之间的连接与通讯。IBM、Toshiba 等国际厂商的产品在这一领域比较完善。



目前很多最新的高端笔记本电脑已将 802.11b 无线网卡集成在系统内部，提供高达 11Mbps 的传输速率。另外，IBM 的 ThinkPad 笔记本还将“蓝牙天线”和蓝牙卡集成在了笔

记本内部。(配图 1—集成蓝牙卡和蓝牙天线) 东芝的 Tecra 9000 笔记本电脑内置了 802.11b 和蓝牙无线通讯天线, 具备全面的无线连接性能。

* 高速无线 PC 网卡

如果用户目前的笔记本电脑并没有集成上述的无线网卡, 也不要紧, 因为通过 PC 卡选件同样可以实现无线网络的搭建。用户可以先购买高速无线 PC 网卡, 然后只要将其插入笔记本电脑的 PC 卡插槽, 就可以登录无线网络。另外, 为了使台式机也可以实现无线连接功能, 一些厂商还提供 USB 无线网卡。上述 PC 网卡采用行业标准设计, 符合 IEEE 802.11b 标准, 数据传输速率高达 11Mbps, 支持网络漫游。

IBM、HP 等厂商已经把这样的产品推上了市场: HP 无线网卡: 工作波段 2.4GHz, 支持 11、5.5、2 或 1Mbps 动态速率转换及负载平衡; 即插即用, 支持操作系统 Win95/98/2000/NT4.0/CE; 40 位和 64 位加密算法(128 位即将就绪)。IBM 高速无线局域网 PC 卡: 工作频段 2.4GHz, 传输速度 1, 2, 5.5 和 11Mbps (速度可自动调节); 介质访问协议支持载波侦听多路存取/冲突规避 (CSMA/CA); 为了保证安全的无线数据传输, 这种网卡采用基于 WEP (Wireless Equivalent Privacy) 的加密技术, 该网卡支持 128 位的 WEP 加密, 代表了目前的最高水平。

* 蓝牙 PC 卡

如果用户的笔记本电脑也没有集成“蓝牙天线”和蓝牙卡, 那么, 通过蓝牙 PC 卡选件, 照样可以搭建起一个无线网络。通过它, 用户可以简单地组成一个临时工作组, 诸如文件、名片、图片、声音文件、日历和邮件都可以实现无线传输。笔记本电脑可以与其它支持蓝牙标准的设备建立起这样短距离、可移动的无线连接。这些设备包括支持蓝牙的 PC、移动电话和 PDA。例如: 在一个会议室中, 会议成员可以通过这种蓝牙 PC 卡连接起来, 相互共享和交换文件。(配图 2—蓝牙 PC 卡)



IBM 蓝牙 PC 卡: 工作频段 2.4GHz; 传输速率可达 721Kbps; 使用距离为 10 米; 支持通用访问——串行口; 拨号网络 (作为数据终端); FAX (作为数据终端)。3Com 蓝牙网卡: 工作频段 2.4GHz; 最大有效距离为 10 米; 另有 USB 接口的蓝牙网卡。

* 高速无线局域网接入点

基于 802.11b 的无线局域网解决方案的基本设施由高速无线局域网 PC 卡和接入点组成。802.11b 接入点 (Access Point) 是建立无线与有线以太网之间连接的网络设备, 相当于一个“无线集线器”。单个的接入点用来管理小型工作组网络, 而多个接入点可以支持多个用户或多个地点。这种接入点兼容性很强, 它有着与上述网卡相匹配的 11Mbps 传输速率, 并

可在 5.5, 2, 1Mbps 等速度下使用, 同时支持 WEP 加密。目前, IBM、HP、CASIO 等厂商都已经推出基于行业标准的接入点。

* 蓝牙 PDA

蓝牙 PDA 可以直接无线接入互联网, 它的一个重要功能就是快速启动某些最常用的网络应用, 如电子邮件。它也可以和具有蓝牙功能的笔记本电脑直接同步, 一些拥有全面无线解决方案的笔记本电脑厂商也推出了支持这种应用的选件。和最新的 IBM ThinkPad 笔记本电脑一并推出的选件 Ultrabay Plus, 可以把一台 PDA 安装在笔记本电脑上面, 两者无需任何线缆连接, 便可以实现数据的互通和交换。(配图 3—PDA 与笔记本互联) 伴随着无线需求的扩大, 很多厂商都有些针对 PDA 的无线接入选件。如 TDK 公司推出的 blue M 背夹, 它可以卡在 IBM WorkPad C500 背面使用, 使这款 PDA 成为蓝牙 PDA。康柏的 iPAQ 等产品本身也具有简单的无线网络功能。



* 蓝牙手机

如果全球旅行者需要实现在世界各地的无线上网, 那么, 通过购买蓝牙手机可以实现广域网的应用。笔记本电脑用户通过蓝牙手机登录广域网, 用户既可以连接到公司的网络中, 又可以实现对互联网的漫游。目前市场中, 很多手机支持蓝牙功能, 如 NOKIA 6310 和的 ERICSSON T39、T68, 它们都是直接内建蓝牙模组的手机。

可以看出, 在目前的无线网络中, PC 仍然是核心的网络终端。就笔记本电脑目前的“无线化”来看, 能够把所有无线连接组件全部集成在笔记本内部的厂商只有 IBM 一家。在这样的情况下, 我们的无线网络还不能像有线网络那样普及、平易, 但是在我们的身边, 已经有越来越多的人正享受着这些无线产品带来的便捷与欢乐。

附录一、无线局域网常用品牌及产品简介

3Com Access Point 8000

产品特点: 3Com Access Point 8000 是专为满足局域网客户端需要集成化的 SNMP 网络管理与 RADIUS 认证的大型企业用户的需求而设计的。支持 IEEE 802.1x 安全性标准, 能够支持无线客户端和 RADIUS 服务器通过一台接入点设备完成相互之间的身份认证; 集中化的网络管理; 并有多重天线选择, 覆盖范围高达 305 米。

应用领域：大型企业无线网络构建。

公司网址： www.3Com.com.cn

安奈特 AT-WL2411

产品特点：该产品可以用来构建一个兼具先进安全特性和高级管理特性的无线局域网解决方案，拥有各种先进的产品特性例如 IP 隧道、DHCP。AT-WL2411 的增强安全功能消除了同时访问公众和内部无线网络的安全屏障，该产品支持 SNMP 网管。

应用领域：园区网络，公共场所。

公司网址： www.alliedtelesis.com.cn

Avaya WOMO

产品特点：无线办公及移动办公（Wireless Office & Mobile Office）解决方案是一个低成本、高性能的集成解决方案，专为中国设计。它的组成包括 VPN 硬件网关、支持 IEEE 802.11b 和 IEEE 802.11a 的无线网桥、支持 802.11b 的无线网卡、VPN Manager 管理软件、客户端的 VPN 软件以及可在国内主要城市的移动场所使用的无线上网服务卡。

应用领域：在企业内部实现无线移动办公，外出办公时，使用运营商提供的无线环境接入企业网络。

公司网址： www.avaya.com.cn

Cisco Aironet 1200

产品特点：Cisco Aironet 1200 系列接入点的模块化设计可以实现单频和双频配置，一个单独的接入点可以提供 802.11b 和 802.11a 接入。Cisco Aironet 1200 系列利用 IEEE 802.1x 标准和它的可扩展认证协议（EAP）、远程访问拨入用户服务（RADIUS）等多种手段提供安全保护。Cisco Aironet 1200 系列可以简化无线局域网的管理。

应用领域：企业网、电信网。

公司网址： www.cisco.com

D-Link DWL-1000AP+

产品特点：可与其他 Airplus 系列产品配套使用，支持高达 11M/22Mbps（双速）的传输速率；可支持 4 种不同的工作模式：作为无线网络访问节点；作为点对点的桥接设备与其他访问节点进行通信；作为点对多点无线桥接设备；或者作为无线客户端。具有内置 DHCP 功能，可自动为连接的无线客户端分配 IP 地址而无需在网络上使用单独的 DHCP 服务器。

应用领域：企业和电信级用户。

公司网址： www.dlink.com.cn

Edimax EW-7205AP

产品特点：EW-7205AP 作为一款无线局域网集中器产品，完全符合 IEEE802.11b 无线局域网标准，无线部分采用直序扩频技术，支持多种工作模式，适应各种场合，可以作为无线访问节点将 IEEE802.11b 无线网络和有线网络无缝地连接起来。

应用领域：企业网。

公司网址： www.edimax.com.tw

Enterasys RoamAbout

产品特点：RoamAbout 802.11 系列产品由两部分组成：全功能交换接入点和直接序列扩

频(DSSS)无线以太网 PC 卡,前者可以通过网线迅速而轻松地连接有线局域网。它具备包括策略管理在内的全面系统可管理性,远程供电降低成本,会话加密为每个用户提供一个动态加密密钥。

应用领域: 室外或室内的无线局域网络连接。

公司网址: www.enterasys.com.cn

GCI GC-511A 无线局域网 AP

产品特点: 带有四个 10/100Mbps 以太网交换端口,其高性能天线提供了良好的传输效果,并可实现无线网络之间的无缝漫游。安装过程简单,提供 Web 方式的配置管理和诊断维护,并提供 DHCP 功能和动态速率调整,提供 64 位或 128 位 WEP 加密、负载平衡和网络过滤。

应用领域: 写字楼、酒店、机场等公共场所。

公司网址: www.gci.com.cn

港湾网络 Aeohammer AP 2000

产品特点: Aeohammer AP2000 采用专用 CPU,集成了港湾专有的 HammerOS 操作系统。Aeohammer AP2000 同时支持 802.11b、802.11g、802.11a 三种标准,采用模块式结构,实现从 11M 到 54M 带宽的平滑过渡。Aeohammer AP2000 将无线接入用户的运营管理、安全机制、计费控制等策略融合到整个无线局域网接入系统中。

应用领域: 城市公共热点区域的无线接入。

公司网址: www.harbournetworks.com

华为 Quidway WA1006

产品特点: QuidwayWA1006 无线接入点遵循 IEEE 802.11 及 IEEE 802.11b+协议,支持 64 位/128 位/256 位 WEP 加密,支持 ESSID、WEP 及过滤 MAC 地址等安全机制,支持用户隔离,支持以太网随线供电标准 802.3af,支持丰富的网管,支持软件方式的动态功率调节,可通过增加 802.11a 射频卡实现双模 AP 的升级。

应用领域: 企业网、电信网。

公司网址: datacomm.huawei.com

明基 AWL500Plus 无线访问接入点

产品特点: AWL 500Plus 的安全体系是建立在 IEEE802.1x 标准上的,从而为用户建立了一个安全的网络环境,它完全支持 EAP 协议和多种加密手段,还支持动态 WEP Key 技术、PPPoE 数据包的转发、基于 MAC 地址的访问列表、同一 AP 内的 BBS 隔离,使 ISP 可以根据需要灵活的配置自己网络系统。

应用领域: 电信运营商的无线互联网接入、企业无线局域网、小区宽带接入

公司网址: www.benq.com.cn

NETGEARWAB102 双频 AP

产品特点: NETGEAR 802.11a/b 自适应双频无线接入点 WAB102,支持完善的 WEP 加密以及 MAC 地址过滤等安全措施。WAB102 可保证 802.11a/b 无线网络灵活切换。

应用领域: 无线网向新一代无线网络的升级。

公司网址: www.netgear.com

清华同方 TFW2000C

产品特点:无线访问接入点 TFW2000c 完全兼容 802.11b 的无线标准。另外增加了 PBCC-22 (也称 CCK-PBCC) 调制方式。采用 PBCC-22 方式保持了对 IEEE 802.11b 的完全兼容,并使最高传输速率达到了 22Mbps。支持 WEP 加密、DHCP、支持 VPN 透明传输。

应用领域:家庭、无线办公室。

公司网址: www.thtfnet.com

上广电应确信 SVA InfiniteAir2020

产品特点:上海广电应确信有限公司 SVA InfiniteAir2020 是一款无线局域网接入点,支持 TCP/IP、NDIS3、NDIS4、IPX、NETBEUI 通信协议和 SNMP 管理,支持动态主机配置协议 DHCP,可自动获得网络地址,提供 64 位 WEP 加密技术、ACL 存取控制、ESSID 访问功能。

应用领域:企业、家庭。

公司网址: www.svanetworks.com

神州数码 DCWL-3000 无线 AP

产品特点:DCWL-3000AP 采用 DSSS 扩频调制模式,支持 MAC 地址过滤,并可以启动 AP 隐藏功能;这款 AP 加强增益的无线信号发射接收性能,配合高接收灵活度的 DCWL-340PC 无线网卡可以延长一般无线使用距离。全中文的操作界面,AP Manager 集群网管。

应用领域:中小企业、SOHO、家庭用户。

公司网址: www.networks.digitalchina.com

SMC 无线局域网安全服务器

产品特点:支持安全认证,VPN 安全支持,基于权限的网络访问,在不同子网中任意漫游及稳定的连接漫游,基于 Web 的配置和管理,支持多达 4 个无线接口,支持 RADIUS、L2CAP、Kerberos、802.1x Windows NT/2000 域或一个内置数据库以控制用户访问网络资源。

应用领域:构建安全无线网络。

公司网址: www.smc-prc.com

TP-Link TL-WA200 无线接入点

产品特点:TP-Link TL-WA200 无线接入点符合 IEEE802.11b 无线网络的国际标准,外接高效率天线,室内最远覆盖范围可达 35~100 米,室外最远覆盖范围可达 100~300 米。采用 64/128 位 WEP 加密以及 ACL 访问列表控制、ESSID 访问控制,支持 DHCP、提供无缝隙漫游 (Roaming) 技术。

应用领域:家庭 SOHO、企业、政府、教育。

公司网址: www.tp-link.com.cn

网新易尚无线宽带路由器

产品特点:YWG-3305 是 11Mbps 无线 Cable/DSL 宽带路由器,集成了四个 10/100Mbps 交换端口。YWG-3305 支持网络地址转换 (NAT),并内置 DHCP 服务器。同时,YWG-3305 还提供了一套全功能的访问控制体系。内建一个全状态监测技术 (SPI) 防火墙,可防御 DoS 攻击。

应用领域:小型办公室、酒店、宾馆、机场。

公司网址: www.yishang.com.cn

附录一、AIRONET 无线网产品安全性说明

该部分的目的在于说明 Aironet 无线局域网系统的保密性，并且介绍 Aironet 系列产品的解决方案和在安全保密方面的增强型功能，因为无线局域网采用的传输介质是开放的空间，显然一个基本问题就提出来“如何防止他人从空间截获我的有用数据？”。该文件将尽量回答这个问题并回答一些当一个保密性很强的单位考虑用无线网时提出的其他一些问题。

操作原理

无线局域网系统通常有一个 Cell 或一组 Cells 组成，每个 Cell 都包含几个无线站点，每一个 Cell 均由一个接入点（Access Point）控制，接入点通常连接到一个以有的主干链路（有线以太网），它管理一个 Cell 内的所有流量，所有的无线工作站都和接入点连接，并和接入点同步到一个频率和时钟，因此他们可以从接入点接入并将数据传给接入点，截取数据的原理亦然。那就是如果有人想要截取数据，它首先必需在接入点的覆盖范围内，并且和接入点同步上才能建立链路。那么我们怎样才能防止此事发生？如果有人买了另一个 Aironet 无线适配器并且试图接入我的无线网络怎么办？Aironet 系列提供一些防止他人窃入，和在同样的系统中防止他人阻截的方法。

我们怎样解决安全问题

1. 网络 ID 号

网络 ID 号是无线接入点设置的一个密码，只有当无线适配器设置了同样的网络 ID 号，它才能和接入点同步并接入到网络中，如果有人想要用 Aironet 接入到你的网络，它必需知道你的网络 ID 号才可能接入。让我们假设有人偷了你的适配器并且连接到你的网络，你所要做的只是修改你的网络 ID 号，那么你的网络又将恢复安全。修改网络 ID 号可以在本地修改也可以非常方便地通过 SMP 网管功能在本地监视器上对每个无线设备进行远程设置，因此不要担心远程无线适配器的设置。

3. 基于 RC4 加密算法和 128 位的密匙

Aironet 本身的发射功率很小，小于 100mW，而且还被扩展到 11MHz 带宽，一方面，平均能量很底，另一方面，不存在频率单一的载波，因此不能被扫描跟踪，这也是此项技术一直用于军事上的原因。在软件上，它还采用了域名控制、访问权限控制和协议过滤等多重安全机制；在安全保密（WEP）方面，特殊用户可选以下附件：基于 RC4 加密（1988RSA 运算法则）和密码（40 或 128 位加密密匙）。

总结

使用无线以太网时的所遇到的一般的安全问题我们已经有了一个回答。使用以上所说的特点可以达到一个非常高的安全水平。

在任何网络中都没有绝对的安全，一个有足够权限和信息的人能进入到任何网络，不管该网络是无线还是有线。这个问题将提出有线网和无线网相比较，哪一个更安全？

考虑到 Aironet 所有的安全特性，我们可以很轻松地，说无线网和有线网一样安全甚至比有线网更安全。

附录二、国家无线电委员会对 2.4GHz 频段的管理办法

为了适应无线电技术的不断发展，满足无线电通信业务的需求，根据国际电联频率划分的有关规则，参照目前国际上通用技术标准，结合我国频谱使用的实际状况，国家：

无委日前对 2000MHz 频段地面无线电业务使用的频率进行了重新规划。

具体安排如下：

一、蜂窝移动通信（1）

工作频段： 1710 — 1755MHz 和 1805 — 1850MHz

二、蜂窝移动通信（2）

工作频段： 1865 — 1880MHz 和 1945 — 1960MHz

上述两种业务频段作为公众蜂窝移动通信频段，由国家无委根据公众蜂窝移动通信运营单位的申请和实际需求进行分配或指配。

三、无线接入（FDD 方式）

（一）工作频段：1800 — 1990MHz 和 1960 — 1980MHz

（二）上述频率用于公众通信网，由国家无委根据公众通信运营单位的申请和实际需求进行分配或指配。

四、无线接入（TDD 方式）

（一）工作频段：1900 — 1920MHz

（二）频率指配及台站（网）审批管理权限按现行的微波通信台站管理办法执行。

五、扩频数据通信

（一）工作频段：2400 — 2483.5MHz

（二）台站（网）审批管理权限按现行的微波通信台站管理办法执行。

上述第一至第五项业务的有关技术指标由国家无委办公室另行制定。

六、多路微波有线电视电视传输系统（MMDS）

工作频段：2533 — 2599MHz

七、无线电定位

工作频段：2300 — 2690MHz

八、微波接力通信

工作频段：2300 — 2690MHz

九、工业、科学、医疗设备无线电磁波辐射频段：2400 — 2500MHz

上述第六至第九项业务的审批管理办法及技术指标按现行规定执行。

十、由于移动业务难以与微波和无线电定位业务在同频段兼容，因此，在两者有影响的地区，由移动通信业务设台组网单位与现有微波或无线电定位设备使用单位（持有无线电台执照者）协商，本着既要保障移动通信业务发展需求，又要妥善处理现用设备

的原则，采取设备改频、替代及经济补偿等方法予以解决。各地无委要积极做好协调工作。（无委）

附录三、AIRONET 无线网产品参考报价（部分）

类别	产品名称	型号说明	单价
1200 Series Access Points			
	AIR-AP1200	AP Platform, Cardbus and MPCIE Slots (no radio), Enet Uplink	1,125
	AIR-AP1220B-A-K9	802.11b AP w/Avail CBus Slot, FCC Cnfg	1,349
	AIR-AP1220B-E-K9	802.11b AP w/Avail CBus Slot, ETSI Cnfg	1,349
1200 Series Access Point Radio Modules			
	AIR-MP20B-A-K9=	2.4GHz 11Mbps Access Point Mini-PCI Module FCC Cnfg	238
	AIR-RM20A-A-K9	802.11a CardBus Radio Mod w/ Dual Int Ant,FCC Cnfg	750
	AIR-RM20A-J-K9=	802.11a CardBus Radio Mod w/ Dual Int Ant,Japan Cnfg	800
1100 Series Access Points			
	AIR-AP1120B-A-K9	802.11b AP, Single MPCIE Radio, Int Ant, FCC Cnfg	899
	AIR-AP1120B-E-K9	802.11b AP, Single MPCIE Radio, Int Ant, ETSI Cnfg	899
350 Series 802.11b (2.4 GHz) Adapters			
	AIR-PCM352	802.11b PC Card w/Integrated Antenna	254
	AIR-PCI352	802.11b PCI Adapter w/RP-TNC Connector, Dipole Antenna	449
	AIR-LMC352	802.11b PC Card w/Dual MMCX Connectors	318
802.11a (5 GHz) Adapters			
	AIR-CB20A-A-K9-40	802.11a CardBus Adapt w/Int Ant, FCC Cnfg, 40PK	14,656
	AIR-CB20A-J-K9	802.11a CardBus Adapt w/Int Ant, TELEC Cnfg	366
Power Options			
	AIR-PSINJSYS1200=	1200 Platform 110-220V Power Supply and Injector System	94
	AIR-PWR-A=	Pwr Sply In:100-240VAC Out:48VDC 380mA -for 1100, 1200 Series	62
	AIR-PWRINJ2=	Power Injector for 1100, 1200 Series	94
	AIR-PWR1783=	350 WorkGroup Bridge 110V Only Power Supply- Spare	78
	AIR-PWR1793=	350 WorkGroup Bridge110-220 V Power Supply- Spare	178
	AIR-PWR2124-002=	340 BR 110/220V Power Supply Spare for Bridge, no line cord	134
	AIR-PWR4852=	340 AP 110V Power Supply- Spare	59
	AIR-PWR4855	340 AP 110-220V Power Supply	0
	AIR-PWR4855=	340 AP 110-220V Power Supply- Spare	134
Power Supply			
	AIR-PWR-SPLY-AP	AIR Line Cord APAC/Universal Power Supply	0
	AIR-PWR-SPLY-AR	AIR Line Cord Argentina/Uruguay/Universal Power Supply	0

	AIR-PWR-SPLY-AU	AIR Line Cord Australia/Universal Power Supply	0
	AIR-PWR-SPLY-CE	AIR Line Cord Central Europe/Universal Power Supply	0
	AIR-PWR-SPLY-CH	AIR Line Cord China Main/Universal Power Supply	0
	AIR-PWR-SPLY-DM	AIR Line Cord Denmark/Universal Power Supply	0
	AIR-PWR-SPLY-IS	AIR Line Cord Israel/Universal Power Supply	0
	AIR-PWR-SPLY-IT	AIR Line Cord Italy/Universal Power Supply	0
	AIR-PWR-SPLY-JP	AIR Line Cord Japan/Universal Power Supply	0
	AIR-PWR-SPLY-NA	AIR Line Cord North America/Domestic Power Supply	0
	AIR-PWR-SPLY-SA	AIR Line Cord South Africa/India/Universal Power Supply	0
	AIR-PWR-SPLY-SW	AIR Line Cord Switzerland/Universal Power Supply	0
	AIR-PWR-SPLY-UK	AIR Line Cord United Kingdom/Universal Power Supply	0
Power Cords			
	AIR-PWR-CORD-SW	AIR Line Cord Switzerland	0
	AIR-PWR-CORD-SW=	AIR Line Cord Switzerland Spare	30
	AIR-PWR-CORD-SA	AIR Line Cord South Africa	0
	AIR-PWR-CORD-SA=	AIR Line Cord South Africa/India Spare	40
	AIR-PWR-CORD-IS	AIR Line Cord Israel	0
	AIR-PWR-CORD-IS=	AIR Line Cord Israel Spare	40
	AIR-PWR-CORD-DM	AIR Line Cord Denmark	0
	AIR-PWR-CORD-DM=	AIR Line Cord Denmark Spare	20
	AIR-PWR-CORD-CH	AIR Line Cord China Main	0
	AIR-PWR-CORD-CH=	AIR Line Cord China Main Spare	30
	AIR-PWR-CORD-AP	AIR Line Cord Asia Pacific (APAC)	0
	AIR-PWR-CORD-AP=	AIR Line Cord APAC Spare	20
	AIR-PWR-CORD-AR	AIR Line Cord Argentina/Uruguay	0
	AIR-PWR-CORD-AR=	AIR Line Cord Argentina/Uruguay Spare	20
	AIR-PWR-CORD-AU	AIR Line Cord Australia	0
	AIR-PWR-CORD-AU=	AIR Line Cord Australia Spare	20
	AIR-PWR-CORD-CE	AIR Line Cord Central Europe	0
	AIR-PWR-CORD-CE=	AIR Line Cord Central Europe Spare	20
	AIR-PWR-CORD-IT	AIR Line Cord Italy	0
	AIR-PWR-CORD-IT=	AIR Line Cord Italy Spare	20
	AIR-PWR-CORD-JP	AIR Line Cord Japan	0
	AIR-PWR-CORD-JP=	AIR Line Cord Japan Spare	20
	AIR-PWR-CORD-NA	AIR Line Cord North America	0
	AIR-PWR-CORD-NA=	AIR Line Cord North American Spare	20
	AIR-PWR-CORD-UK	AIR Line Cord United Kingdom	0
	AIR-PWR-CORD-UK=	AIR Line Cord United Kingdom Spare	20
Access Point and Bridge Accessories			
	AIR-CONCAB1200=	1200 Platform Console Cable	16

	AIR-ACC1833	340 Series Bridge Mounting Kit	74
	AIR-ACC3986-001	340 Series Bridge Slide mount kit	119
	AIR-ACC5559-072	Serial Cable for 340/350 Series AP Console Port Cnfg	15
Antennas - 2.4 GHz			
	AIR-ANT1728	2.4 GHz, 5.2 dBi Ceiling Omni Ant. w/RP-TNC Connector	239
	AIR-ANT1729	2.4 GHz, 6 dBi Patch Ant w/RP-TNC Connector	329
	AIR-ANT1949	2.4 GHz, 13.5 dBi Yagi Mast Mount Ant. w/ RP-TNC Connector	554
	AIR-ANT2506	2.4 GHz, 5.2 dBi Mast Mount Omni Ant w/RP-TNC Connector	239
	AIR-ANT3195	2.4 GHz, 3 dBi Patch Antenna w/ RP-TNC Connector	299
	AIR-ANT3213	2.4 GHz, 5.2 dBi Divers. Pillar Omni Ant. w/RP-TNC Con.	314
	AIR-ANT3338	2.4 GHz, 21 dBi Solid Dish Antenna w/RP-TNC Connector	1,499
	AIR-ANT3351	2.4 GHz, 2.2 dBi Divers. Dipole Ant. base w/MMCX Connectors	284
	AIR-ANT3549	2.4 GHz, 9 dBi Patch Antenna w/ RP-TNC Connector	359
	AIR-ANT4121	2.4 GHz, 12 dBi Omni Mast Antenna w/RP-TNC Connector	1,043
	AIR-ANT4941	2.4 GHz, 2.2 dBi Dipole Antenna w/ RP-TNC Connector	29
Antenna Cable			
	AIR-CAB020LL-R	20 ft LOW LOSS CABLE ASSEMBLY W/RP-TNC CONNECTORS	258
	AIR-CAB050LL-R	50 ft. LOW LOSS CABLE ASSEMBLY W/RP-TNC CONNECTORS	398
	AIR-CAB100ULL-R	100 ft. ULTRA LOW LOSS CABLE ASSEMBLY W/RP-TNC CONNECTORS	598
	AIR-CAB150ULL-R	150 ft. ULTRA LOW LOSS CABLE ASSEMBLY W/RP-TNC CONNECTORS	798
Antenna and Cable Accessories			
	AIR-ACC1622	RP-TNC Male Connector for 9913 Cable	29
	AIR-ACC1623	RP-TNC Female Connector for 9913 Cable	29
	AIR-ACC1655	RP-TNC Male Connector for RG-58 Cable	29
	AIR-ACC1725	Magnetic Antenna Mount Base w/RP-TNC Connector	149
	AIR-ACC1828	RP-TNC Female Connector for RG-58 Cable	44
	AIR-ACC2537-060	60 in (1.5m) RP-TNC Ant. Cable w/Mounting Bracket	104
	AIR-ACC2538	RP-TNC Connector with Mounting Bracket	44
	AIR-ACC2662	Antenna Mount for use with ANT1949	104
	AIR-ACC3354	Lightning Arrestor with grounding ring, RP-TNC Connector	314
Regulatory Domain Options			
	AIR-AMERICAS	Regulatory Domain Configuration for Americas (FCC)	0
	AIR-CHINA	Regulatory Domain Configuration for China (MII)	0
	AIR-EMEA	Regulatory Domain Configuration for EMEA (ETSI)	0
	AIR-ISRAEL	Regulatory Domain Configuration for Israel (MC)	0
	AIR-JAPAN	Regulatory Domain Configuration for Japan (TELEC)	0

Cisco Aironet Documentation-			
	DOC-7814371=	Cisco Aironet 1200 Ser Access Pt 2.4 GHZ Radio Install Instr	53
	DOC-7812108=	Installation Instructions for Cisco Aironet Power Injectors	53
	DOC-7814622=	Aironet 1200 Ser Access Point Radio Upgrade Instructions	53
	DOC-7811532=	Quick Start Guide: Cisco Aironet Wireless LAN Adapters	60
	DOC-7814830=	Quick Start Guide Cisco Aironet 1100 Series Access Point	45
1100 Series Software Options			
	S11W7K9-12204JA	Cisco 1100 Series IOS WIRELESS LAN	0
	S11W7K9-12204JA=	Cisco 1100 Series IOS WIRELESS LAN	0

（此价格为 CISCO 公司 FOB USA 价格，仅供参考，如有变更，恕不另行通知）