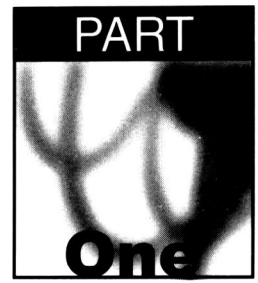

第1部分
无线基础知识

CHAPTER 1

第 1 章　无线硬件设备

工欲善其事，必先利其器。要想成为无线安全专家，首先必须获得必要的设备。本章将详细分析一些非常好的硬件设备，而且我们只选择那些性价比最高的硬件。所有这些产品都是我们推荐你选用的。

后面将探讨一些可用于组建典型无线 LAN 的出色硬件，其中包括访问点、无线网卡、天线和 PDA。随着时间的推移，我们的推荐也可能发生变化，所以，如果你有任何问题或疑问，请直接与作者联系，邮件地址是 cyrus@airscanner.com。

1.1　访问点

很多厂商都在生产访问点（Access Point，简称 AP），而且所有访问点的功能是基本相同的。但是，不同厂商的访问点在安全性和功能特色上有明显的区别。如本章所述，有的访问点能根据无线网卡上的 MAC 地址限制用户连接，有的访问点则能关闭信标广播，使黑客所用的破解程序看不到这个访问点。幸运的是，诸如此类的高级安全特性在 SOHO（小型办公室／家庭办公室）访问点中正在变得越来越常见。

我们对 5 个城市的 1300 多个访问点进行实地调查之后，得出以下结论：思科（Cisco）的市场占有率最高，为 39.7%；朗讯科技（Lucent）排名第二，为 19.2%；然后是 Linksys，为 17.1%；其他所有厂商的占有率为 24%。有趣的是，本来为 SOHO 设计的 Linksys 访问点正在快速地获得企业用户的认同。这可能归功于 Linksys 的设备价格低、应用广泛、增加了 MAC 限制功能，以及能够关闭信标广播。然而，价格不菲的 Cisco 访问点仍然占据主流地位，由此不难推断出，有大量的资金正花在拓展和开发企业内部无线网络产品上。

1.2 Linksys WAP11

主页：http://www.linksys.com

Linksys WAP11 是一款简单高效、物美价廉的访问点产品。以前，由于缺乏安全功能，WAP11 并没有得到广泛使用。幸运的是，这个问题已得到了解决。自固件版本 1.4i.1 起，这款访问点具备了几个新功能，比如禁止信标广播，并能根据客户端的 MAC 地址限制连接等。

WAP11 需要用基于客户端的软件来管理，这要么通过 USB 接口来进行，要么通过以太网连接(而不是无线连接)上的 SNMP 来进行。1.4i.1 固件版本新增的特性要求使用 SNMP 接口。但是，只有在使用 USB 接口时，才能查看这些设置。我们为此联系了 Linksys，但他们的支持人员也不清楚为什么不能用这两个接口来配置这些特性。他们表示，这个问题可能暂时无法解决。但无论如何，它的管理界面很有条理，也很容易配置。图 1.1 和图 1.2 给出了管理界面的两个例子。

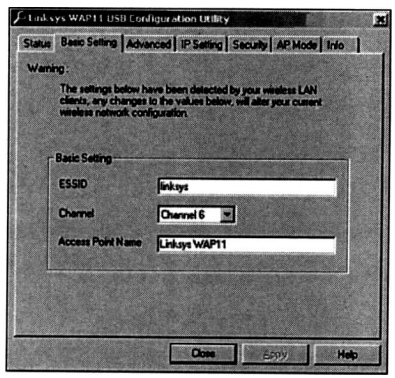

图 1.1 Linksys WAP11 管理界面上的 Basic Setting 选项卡

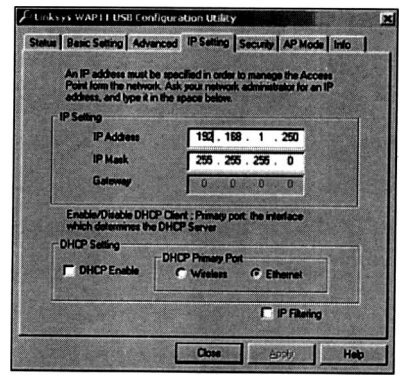

图 1.2 Linksys WAP11 管理界面上的 IP Setting 选项卡

WAP11 的一个特色是它有两个天线，可以让一个天线专门负责发送，另一个天线专门负责接收。默认设置是两个天线都能发送和接收。由于能配置天线的使用方式，所以 WAP11 几乎能在任何环境下工作。WAP11 使用的是一个标准的（RP-TNC）连接器，所以你可以购买高增益天线配件来代替原配的天线。这有助于将覆盖范围限制在特定的区域，或者将覆盖范围定向到一个特定的区域。1.4 节“天线”就这个主题提供了更多的信息。

技术规格

默认 SSID：Linksys

默认 IP：192.168.1.250

默认频道：6
加密：40／128 位 WEP
客户端：32
尺寸：长：8.9 英寸
　　宽：5 英寸
　　高：1.6 英寸
重量：12 盎司

1.3 NetGear ME102

主页：http://www.netgear.com

NetGear ME102 是一款小巧的、功能齐全的访问点产品。它只有 6.4 英寸长，5.6 英寸宽，1.1 英寸高，是市面上最小巧的访问点，所以，它是出差旅行或者空间有限时的理想选择。但是，“个头”小并不表示功能弱。进行了 1.4h3 固件升级之后，ME102 能支持 128 位加密、点到点及点到多点配置，并通过 MAC 地址限制增强了访问点客户端的功能。

ME102 的管理需要使用基于客户端的软件，这要么使用一个 USB 接口，要么使用以太网连接(而不是无线连接)上的 SNMP。要想查看和配置 MAC 地址限制(如图 1.3 所示)，必须使用 SNMP 接口。此外，还可通过 SNMP 看到统计信息页，其中列出了访问点上的无线及以太网接口的统计信息（如图 1.4 所示）。ME102 的另一个有用特性是它能为管理接口设置多个密码。这样一来，网管就能在不泄露自己的密码的前提下，允许用户查看访问点的配置。作为普通用户登录时，你可以浏览所有配置，只是不能更改它们。

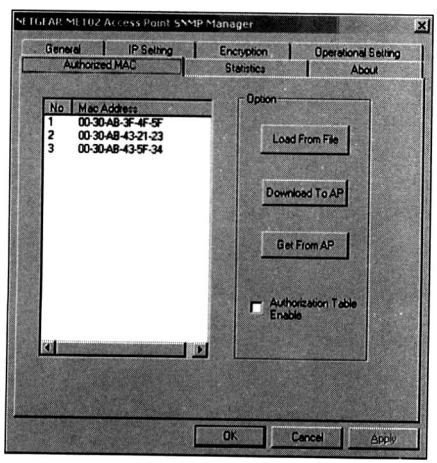

图 1.3　设置 MAC 地址限制

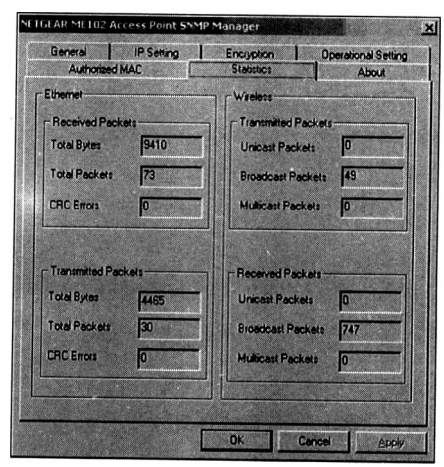

图 1.4　管理界面中的统计信息页

通过几次测试，我们发现 ME102 的总体功能和可用性完全超出了我们的预期。这款访问点具有非常强大的功能，是许多情况下的理想选择。尽管无法与企业级的访问点相比，但它绝对物有所值。

技术规格

默认 SSID：Wireless
默认 IP：192.168.0.5
默认频道：6
加密：40／128 位 WEP
客户端：32
尺寸：长：6.4 英寸
　　宽：5.6 英寸
　　高：1.1 英寸
重量：0.076 磅

1.4 天线

几乎每个人每天至少都要使用一个天线。事实上，大多数人在每天的日常生活中经常利用天线为自己带来方便，只是许多人没有意识到而已。如车门遥控开关系统、高速公路收费口、卫星电视、传呼机、手机及无线网络等，它们全都离不开天线。在使用这些天线的用户中，很少有人能说得清楚天线的原理和用途。因此，在这里简单介绍一下天线技术，并解释天线与我们的无线网络的关系。

天线只是无线电收发装置的一种扩展。信号一经生成，就会通过空气，从无线电装置发射出去，并被另一个天线接收，然后传给另一个无线电装置。生成并随即发射出去的信号以赫兹（Hertz，Hz）为单位来计量；“赫兹”不是汽车租赁公司，而是对每秒的周期数进行计量的一个单位。假定在光滑平面上有一个 Slinky（一种螺旋状的金属弹簧），它的一端是固定的。晃动它，就会产生波动。这种“波”代表通过空气传送出去的射频（Radio Frequency，RF）能量。如果只是轻轻地晃动，产生的波会长一些，频率会低一些。快速晃动它，产生的波会短一些，但波动更频繁，频率会高一些。较低的频率通常能传送更远的距离，但由于延迟较大，所以会限制数据流（数据量）。较高的频率具有较低（更好）的延迟，但传送距离有限，而且中途不容易穿透建筑物和其他障碍物。

以本地的一家 FM 广播电台为例。假定他们以 103.5MHz（兆赫）播出信号，这个频率就相当于每秒完成 103 500 000 个周期。整个城市的听众都能接收到他们的信号，即使在建

筑物和房间内，也几乎不受任何干扰。但是，一旦超出这个城市的范围，信号就会大幅减弱，直至最终完全收听不到这家 FM 电台的节目。与此同时，距离你有两个州那么远的一家 AM 无线广播电台则在 1320kHz 上播出信号，这个频率相当于每秒 1320000 个周期。如果在室外安置性能优良的天线，就能在很远的距离之外收到他们的信号，惟一困难的地方就是你需要调整天线。

总之，天线是传输 RF 信号的基本组件。很多情况下，假如使用优质天线来发射低功率信号，相较于使用劣质天线来发射高功率信号，前者在抵达目的地后反而具有更好的精确度。天线的质量根据它们能提供的增益量来评定。“增益”（Gain）是指使用一个定向天线能够获得的功率上的提升。

提示：整体增益是相对于理论上的“等向天线”而言的。等向天线在现实世界中是不可能存在的，但常常将等向天线作为一个参考基准。

假如一个天线的标定增益单位是 dB，就需要向厂商核实，它到底是 dBi，还是 dBd。如果他们说不清楚，或者根本不知道，就最好不要买他们的产品，选择其他的厂商。

假定等向天线的增益是 0-dBi，则偶极天线的增益为 2.14dB。因此，如果天线标定的增益单位是 dBd，而不是 dBi，就在它的基础上加 2.15，从而获得 dBi 值。

如前所述，在市面上出售的大多数天线中，标定的增益单位都是 dBi，但这并不是评价其总体性能的惟一因素。例如，天线的功率输入也是一个不可忽视的因素。大多数 802.11b 无线网卡的发射功率都是 32mW。根据表 1.1 提供的转换表，可以推算出 32mW（Pwr 列表示的是“功率”）相当于 15dBm。dBm 的计算公式是：

dBm = 10 log (32mW/1)

表 1.1 dBm 功率换算表

dBm	Pwr	dBm	Pwr
53	200W	25	320mW
50	100W	24	250mW
49	80W	23	200mW
48	64W	22	160mW
47	50W	21	125mW
46	40W	20	100mW
45	32W	19	80mW
44	25W	18	64mW
43	20W	17	50mW
42	16w	16	40mW

续表

dBm	Pwr	dBm	Pwr
41	12.5W	15	32mW
40	10W	14	25mW
39	8W	13	20mW
38	6.4W	12	16mW
37	5W	11	12.5mW
36	4.0W	10	10mW
35	3.2W	9	8mW
34	2.5W	8	6.4mW
33	2W	7	5mW
32	1.6W	6	4mW
31	1.25W	5	3.2mW
30	1.0W	4	2.5mW
29	800mW	3	2.0mW
28	640mW	2	1.6mW
27	500mW	1	1.25mW
26	400mW	0	1.0mW

例如，假定已知一张典型网卡的发射功率是 15dBm，而你准备使用一个 3-dBi 的天线，就可以使用以下等式来计算“等效全向功率”（Effective Isotropic Radiated Power，EIRP）：

15dBm + 3dBi = 18dBm (64mW) EIRP

目前，美国联邦通信委员会（Federal Communication Commission，FCC）将 802.11 移动电台限制为 1W（或者 30dBm）EIRP。对固定电台限制要宽松一些，允许它们超出 1W。针对固定电台，他们要求这样计算：天线增益如果超出 6dBi，就要每 3dB 减去 1dB。下面的例子说明了如何对 LinksysWAP11 和 24-dBi 天线进行这样的计算：

20dBm + 24dBi = 44dBm or 25W

(44dBm –((24dBi – 6dB)/3)) = EIRP

(44dBm – (18dBi / 3)) = EIRP

(44dBm – 6dBi) = EIRP

EIRP – 38dBm or 6.4W

除了天线增益和发射功率，还应该考虑天线的尺寸。这取决于天线的频率和类型，有很多不同尺寸的天线可供选择。天线的尺寸直接关系到它所用的频率。以车内使用的 CB 无线电装置为例，它的工作频率为 26.965MHz（频道 1）和 27.405MHz（频道 40）。如果需

要为频道 1 选择一个全波段的天线，就要求天线的长度为 36.491英尺。可通过下面的公式来换算：

L(英尺) = 984/f(MHz)

L = 984/26.965MHz

L = 36.491英尺

现在，将 CB 天线与工作在 460.175MHz 的全波段天线（警方用这种天线来与总台保持联系）进行比较：

L(英尺) = 984/f(MHz)

L = 984 ／ 460.175 MHz

L = 2.142 英尺

可以看出，两个天线之间的长度相差 34.349 英尺。所幸的是，对我们而言，无线 802.11b 网络的工作频率为 2.4GHz 或者说 2400MHz 之内，所以不需要太长的天线。

无线网络中所用的天线主要有两类：全向天线和定向天线。全向天线可接收和传输来自各个方向（即 360°）的信号。如果需要覆盖一个大房间，或者需要提供常规性覆盖，就适合使用这种天线。与大多数人的想法相反，真正的全向天线并不能提供任何增益。被当做全向天线出售的大多数天线都不能全方位地发送无线电信号。这种天线的设计思想是让 y 轴上的信号无效，将有效信号集中在 x 轴上。

定向天线获取 RF 能量，并将其集中在一个特定的方向上。可以分别用灯泡和手电筒来比喻全向天线和定向天线。灯泡相当于全向天线，因为它发出的是漫射式的光线。相反，手电筒（相当于定向天线）要借助于一个反射镜，将光线集中在一个方向上。从理论上讲，最适合使用定向天线的场合包括：建立点对点的无线连接时；要在某个特定位置减少 RF 信号的“流失”时。

1.5 带护罩的八木天线：HyperLink HG2415Y

主页：http://www.hyperlinktech.com

HG2415Y 是一款品质优良、性能出众的八木（定向）天线（也称 Yagi 天线。要想进一步了解这一款天线，请访问 http://www.hyperlinktech.com/web/hg2415y.php——译者注）。它重约 1.8磅，非常轻巧，特别容易安装。它自带两个 U 形螺丝支架，可将它连接到直径最大为 23/8 英寸的天线竿上。

这款天线配备 24 英寸长的猪尾连接线(pigtail),可以选用 N，TNC 或者 SMA 连接器来终止。我们测试时所用的产品是用 N Female 连接器来终止的。我们使用一条 CA-WL2CABLE1 猪尾连接线，将天线连接到一张 ORiNOCO PCMCIA 卡上。初始测试表明：

使用了这款天线之后，有效通信距离达到了使用访问点内置天线时的 3 倍。图 1.5 和图 1.6 的屏幕截图展示了信号强度。

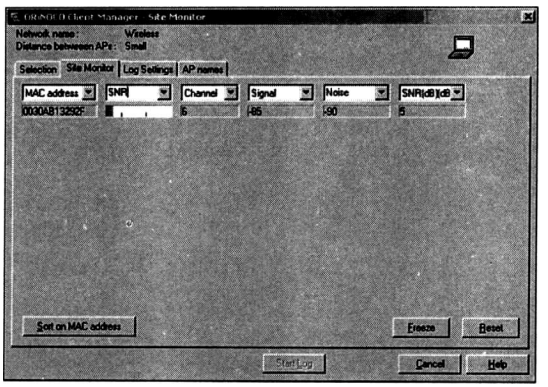

图 1.5　基准——使用内置天线

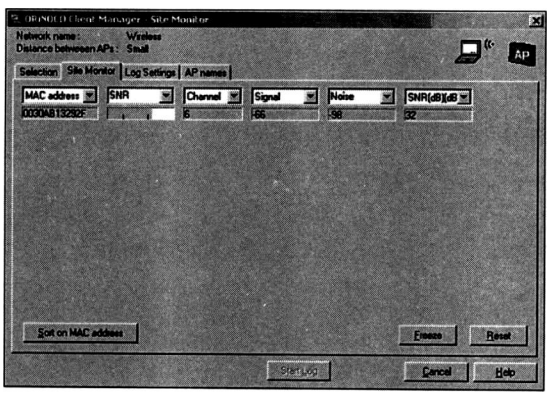

图 1.6　使用 HyperLink HG2415Y 天线时的信号采样

可以看出，使用 HyperLink HG2415Y 天线后，信号强度得以显著增强。这款天线非常适用于点到点连接，而且对于自然环境的影响有很强的抵御力。事实上，即使在风速高达每小时 150 英里的情况下，这款天线仍然能正常地工作。所以，这款天线非常适合在严酷的自然环境下使用。总的来说，这款天线是同类产品中的佼佼者，应该成为你的首选。

技术规格

频率：2400~2500MHz

增益：14.5-dBi

-3dB 波束宽度：30°

阻抗：50 欧姆
最大输入功率：50 瓦特
VSWR :平均＜1.5:1
重量：1.8 磅
尺寸：19 英寸长，直径为 3 英寸
极性：垂直和水平
抗风力 > 150 英里每小时

提示：VSWR 是指“电压驻波比”(Voltage Standing Wave Ratio)，表示正向功率与反向功率之比（也就是输入天线的功率与反射回无线电装置的功率之比）。

1.6 抛物面栅格天线：HyperLink HG2419G

主页：http://www.hyperlinktech.com

HyperLink HG2419G 同样性能出众。这款高增益、高效率的天线经过了工程师们精心的设计。它的材料选用的是高度耐用的镀锌钢，外表是浅灰色的 UV 涂层。所以，它不仅耐用，而且外观也非常吸引人。

Hyperlink 公司为这款天线提供了增益分别为 15-dBi、19-dBi （本书测试的是这一款）以及 24-dBi 的三种型号。除了提供高增益，这款天线还具有非常好的选择性。其中， 24-dBi 的型号由于提供了 8° 的波束宽度，所以将它受干扰的可能性降至最低，而且功率得到了最大限度的提升。和大多数定向天线一样，这一款天线尤其适用于在多个网络之间实现点到点的连接。通过测试 HG2419G，我们发现有效通信距离达到了使用访问点内置天线时的 3 倍，而且连接稳定。图 1.7 和图 1.8 的屏幕截图展示了信号强度。

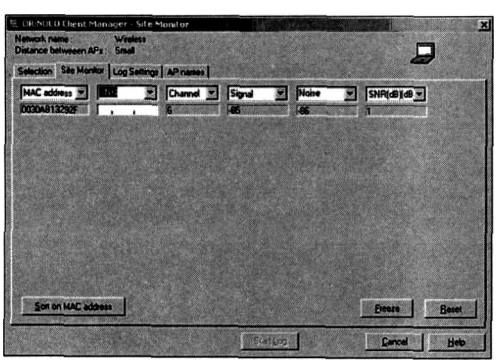

图 1.7 基准——使用内置天线

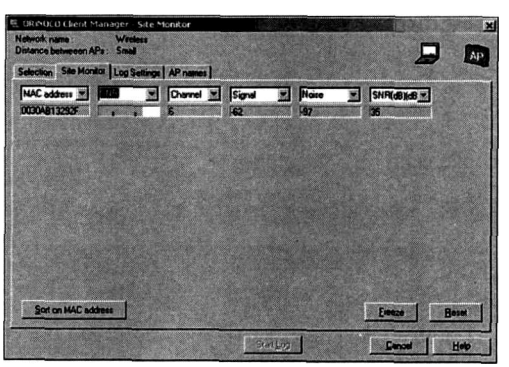

图 1.8 使用 HG2419G 天线

HG2419G 可以安装在直径最大为 2.5 英寸的标准天线竿上，而且仰角最大能调整到 15°。这样一来，你就能在很多地方使用这款天线，在屋顶上安装也显得非常灵活。这款天线集众多特性于一身（比如可以选择垂直波和水平波、高增益、紧密波束宽度以及适用于恶劣环境），所以在市场上非常受欢迎。

技术规格

频率： 2400~2500MHz
增益： 19-dBi
-3dB 波束宽度： 17°
阻抗： 50 欧姆
最大输入功率： 50 瓦特
VSWR **：平均<**1.5:1
重量： 3.9 **磅**
长度： 16.7 **英寸长，直径为** 23.6 **英寸**
极性：垂直或水平
抗风力：> 150 **英里每小时**

1.7 SigMax 全向天线：Signull SMISMCO10

主页： http://www.signull.com

SMISMCO10 作为一种全向天线，是针对中长范围的多点连接而设计的。它高不到 3 英尺，重不到 1 磅，但不大的个头却蕴藏着惊人的力量。

Signull Technologies 的这款天线提供了三种型号：10-dBi（本书测试的型号）、8-dBi 和 5-dBi。这三种型号都非常适合用来扩展公司访问点或者无线节点的信号覆盖范围。它们很容易就能安装在室内，并立即全方位地扩大信号的有效覆盖范围。也可考虑将其安装在一个仓库中，使无线库存管理设备能在更大的区域内使用。此外，还可以将这些天线安装在室外，使信号覆盖范围能扩展到室外的庭院或停车场。我们对 SMISMCO10 的实际测试证实了 Signull所承诺的高性能。图 1.9 和图 1.10 展示了信号强度。

测试这款天线时，我们直接将其连接到访问点上，并试着使用一张标准的 ORiNOCO PCMCIA 无线网卡来连接它。图 1.10 展示的信号强度在围绕访问点的各个方向上都是一致的。

由于坚固耐用、重量轻及出色的性能， Signull Technologies 的 SMISMCO10 天线非常适合添加到你的无线 LAN 中。

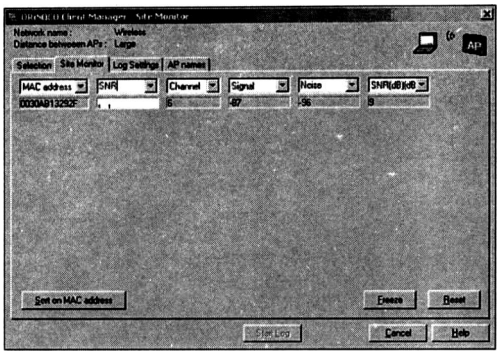

图 1.9　基准——使用内置天线

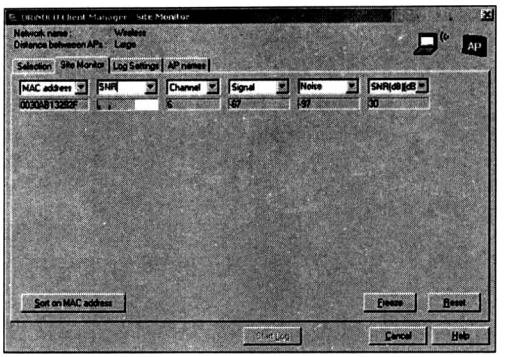

图 1.10　使用 SMISMCO10 天线

技术规格

频率：2400~2500MHz
增益：10-dBi
波束宽度：360°
阻抗：50 欧姆
最大输入功率：50 瓦特
VSWR：平均＜1.5:1
重量：0.75 磅
宽度：7 / 8 英寸
长度：38 英寸
极性：垂直
抗风力＞100 英里每小时

1.8　SigMax 环形八木天线：Signull SMISMCY12

主页：http://www.signull.com

Signull Technologies 公司的这款环形八木天线也在我们的推荐之列。除了具备出色的性能，它还采用了非常时尚的外形设计——谁说无线安全就不讲究美观了呢？此外，这款天线是透明的，你可以清清楚楚地看到其内部设计。所以，你可以把这款天线当作学习工具来使用。

测试时发现，将这款天线对准测试访问点，能显著增强信号强度。Signull Technologies 为这款天线提供了三种型号：8-dBi、12-dBi（本书测试的就是这个型号）和 15-dBi。测试用的这款 12-dBi 天线，似乎已经能提供足够的性能提升。但是，在实际应用中，15-dBi 也

可能是一种更好的选择。图 1.11 和图 1.12 的屏幕截图展示了信号强度。

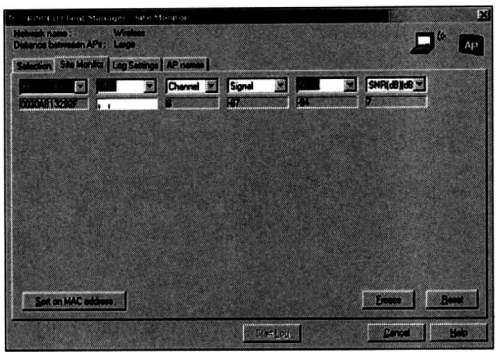

图 1.11　基准——使用内置天线

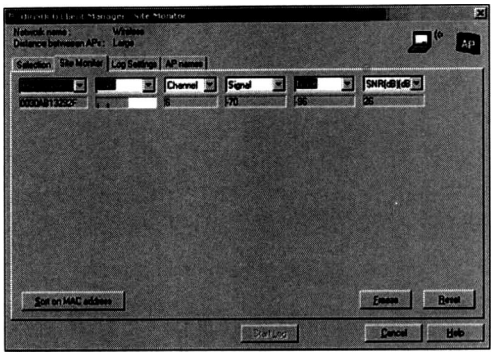

图 1.12　使用 SMISMCY12　天线

虽然这款天线因为其透明设计而独具特色，但在露天长时间使用，也可能出现问题。所以这款天线最好安装在室内，或者加上保护套之后再安装到室外。幸运的是，这款天线不仅形象好，性能也不错。如图 1.12 所示，SMISMCY12 的性能确实相当理想。这款天线适用于创建和链接无线网络，选购时应该重点考察它。

技术规格

频率：2400~2500MHz
增益：12-dBi
-3dB 波束宽度：30°
阻抗：50 欧姆
最大输入功率：50 瓦特
VSWR：平均＜1.5:1
重量：2 磅
宽度：4 英寸
长度：23 英寸
极性：垂直和水平
抗风力＞ 100 英里每小时

1.9　TechnoLab 的对数周期八木天线

主页：http://www.technolab-inc.com

TechnoLab　公司的这款八木天线也是不错的选择。由于采用了小巧玲珑的设计，使其

非常适合用做室内定向天线。另外，也可以将它安装在一幢大楼的周界上，从而轻松地建立楼宇之间的通信链接。

测试表明，这款小巧的天线具有非常出色的性能。测试时，我们将这款八木天线直接连接到测试访问点上，并试着用一张标准的 ORiNOCO PCMCIA 卡来连接它。结果表明，这款天线具有非常好的选择性，能在指定的方向上显著改善信号强度。图 1.13 和图 1.14 的屏幕截图展示了在不同情况下的信号强度。

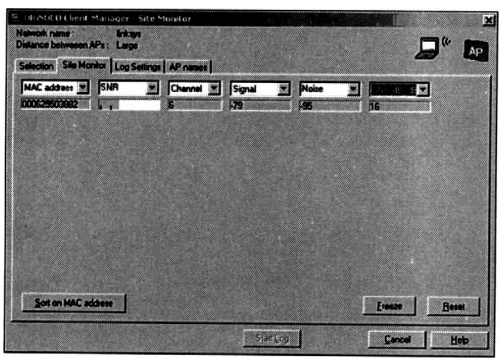

图 1.13　基准——使用内置天线

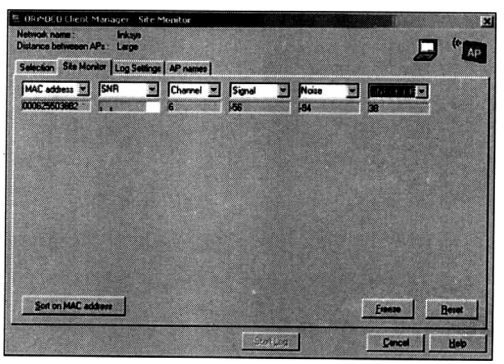

图 1.14　使用八木天线

我们还结合使用内置天线和 TechnoLab 的八木天线来测试访问点，结果没有出现信号衰减的情况。这一点很重要，因为在很多情况下，访问点不仅要提供远程用户连接，还要提供本地用户连接。这款天线不仅体积小、重量轻，它的频率范围还允许你将其用做其他用途（而非仅限于无线联网）。总之，TechnoLab 的八木天线是一款非常有用的天线，可考虑将其添加到自己的无线办公网络或者无线校园网中。

技术规格

频率：900~2600MHz
增益：12-dBi
-3dB 波束宽度：30 度
阻抗：50 欧姆
最大输入功率：10 瓦特
VSWR 平均＜ 2:1
重量：1.8 磅
长度：N/A
极性：N/A
抗风力：N/A

1.10 无线网卡

无线网卡（Wireless Network Interface Card，WNIC ）是安装无线硬件设备时不可或缺的基本组件。本节只介绍 ORiNOCO 品牌的网卡，因为它们是同类产品中的佼佼者。

1.11 ORiNOCO PC 卡

主页：http://www.orinocowireless.com

毫无疑问，Agere Systems 的 ORiNOCO 无线 PCMCIA 卡是市场上最受欢迎的网卡。作为标准的 PCMCIA 卡，它们能插入笔记本电脑的 Type II 插槽中。这种卡有两个型号：Silver 和 Gold。Silver 卡提供 64 位 WEP 保护，Gold 卡则提供 128 位 WEP 保护。两种卡都提供高达 11Mbps 的连接速度，并符合 Wi-Fi 标准，所以它们能与其他系统兼容。 Gold 和 Silver 卡最吸引人的一个特性在于，它们都能连接一个外置天线。虽然这个特性并不是独一无二的，但在其他厂商的同类产品中，却很少具备这个特性，而且这是进行无线审计和网络管理时需要的一项非常关键的特性。此外，这种卡还获得了众多操作系统的支持，其中包括 Mac，Novell，Windows 和 Linux。

可以将 ORiNOCO 卡配置成“对等”（特别）或者“基础”这两种模式。其中，对等模式允许你快速组建一个小型网络，无需使用访问点，就能实现卡与卡之间的通信。在基础模式中，ORiNOCO 卡需要和正在使用访问点的大型公司网络建立关联，并由访问点将信息中继传输到有线网络中。

组建办公室网络时，Agere Systems 的 Gold 和 Silver ORiNOCO 卡将是你最理想的选择。它们坚固耐用，能连接外置天线，并获得了众多操作系统的支持——所有这些都成为我们推荐它们的理由。

1.12 手持设备

手持计算设备也称为“个人数字助理”（Personal Data Assistant，PDA），它们正在快速地普及。PDA 的用途越来越广泛，人们对无线网络连接能力、审计和管理的需求也在相应地增强。能在家里或办公室的任何地方，用一支小巧的触控笔点几下屏幕，即可查看电子邮件——想像一下这个场景，就知道 PDA 为什么如此受欢迎了。

许多公司早就在着手为 PDA 市场开发能提高生产力的高端应用程序。例如， Pocket PC（使用微软的嵌入式操作系统 Windows CE ）随机赠送了一个 Microsoft Terminal Server

Client，允许你在网络上的几乎任何位置连接服务器。医学专业的学生甚至能够使用 PDA 连接到无线网络，通过流式视频来观看手术过程。因此， PDA 市场具有相当大的增长潜力。

过去，PDA 操作系统市场有两大主要的竞争者，一个是 Palm（使用 Palm OS），另一个是 Pocket PC（使用 Windows CE）。但是，使用 Palm OS 的人越来越少，更多的人倾向于使用 Windows CE （就目前来看，Palm OS 占有的市场份额虽然少于以前，但仍然多于 Windows CE—— 译者注）。所以，本书会尽可能地避免提及 Palm，只是在第 8 章讨论感染它的病毒时，会最后一次地提到它。

写作本书时，Palm 并没有表现出它支持 802.11b 连接的积极愿望。相反，Pocket PC 则展示了它在这个方面的强大功能。许多厂商都在为他们的硬件编写 Pocket PC 驱动程序，希望继续扩展这种功能已经非常强的产品。和台式机和笔记本一样，最终会有众多型号的硬件支持和运行 Pocket PC 操作系统。每个设备都是独一无二的，能提供与众不同的特性和优势。购买手持设备时，应该综合考虑多方面的因素，尤其是它是否有更大的内存空间、更高的屏幕分辨率以及是否支持 PCMCIA 卡和 CF 卡之类的外设。

经过我们的调查，发现有一款设备完全符合我们的要求，这就是 Compaq iPAQ。考察无线连接能力以及特性集， iPAQ 无疑是 PDA 市场上最好的一款产品。很多公司，比如 ORiNOCO、Network Associates 及 Cisco 等，都在积极地推动 iPAQ 的应用，使其在无线领域中占据越来越重要的地位。很多厂商都在设计专门用于 iPAQ 的软件，并衷心地赞叹它支持众多外置硬件设备的能力。

PDA 虽然不如台式机那么强大，但却是家庭或商业网络的一种非常有用的扩展。随着 802.11b 网络的普及，免费公共网络的增多，手持设备必然会在普通用户中得到进一步的普及。除此以外，越来越多的公司员工会借助自己的 PDA，通过“虚拟专用网络”（Virtual Private Network，VPN ）来进行远程办公。

1.13 Compaq iPAQ

主页：http://www.compaq.com

考察市面上拥有无线功能的众多手持设备，Compaq（康柏）公司的 iPAQ 无疑是其中的佼佼者。下面的描述是基于 iPAQ 3765 的，但根据惯例，它以后必将推出升级版本。iPAQ 采用微软 Pocket PC 2002 操作系统，处理器是一颗 206MHz 的 Intel StrongArm 32 位 RISC 处理器，配备的 RAM 则高达 64MB。

不仅主机具有强大的功能，你还可以为它添加背夹（也称为 Extension Pack，即“扩展包”）。图 1.15 展示了这种背夹，作为一种附加装置，它们用于增强 iPAQ 的整体功能。目前市面上有多种不同的背夹产品。在它们的帮助下，iPAQ 能够利用从 PCMCIA 卡和 CF 卡，

一直到 IBM 微型硬盘和 GPS 设备在内的几乎一切东西。换言之，使用背夹，你的标准 iPAQ 可以立即转变成一个无线工作站。由于很多设备都支持 PCMCIA 标准，所以 PCMCIA 规格背夹（部件编号为 173396-001 ）可能是功能最丰富，最值得你拥有的。

图 1.16 展示了一台 iPAQ，它连接了一个 PCMCIA 规格的背夹，而且背夹中已经插入一张无线网卡。采用这种设置，就能轻松连接各种 802.11b 网络，并执行多项任务，比如浏览网页（使用内置的 Internet Explorer ）或者管理远程网络（使用 Terminal Server 程序）。如果再装上 Ruksun 的 NetForce 或者 Epiphan Consulting 的 CENiffer（参见第 10 章的讨论），就能大幅增强 iPAQ 的总体功能以及可用性。其他软件开发商（比如 NetStumbler 和 Network Associates ）也开发了基于 iPAQ 的软件产品。随着可用的硬件和软件越来越多，以及无线网络的日益普及，Compaq iPAQ 必然成为未来市场上的一股支配性力量。

图 1.15　专门为 iPAQ 设计的背夹

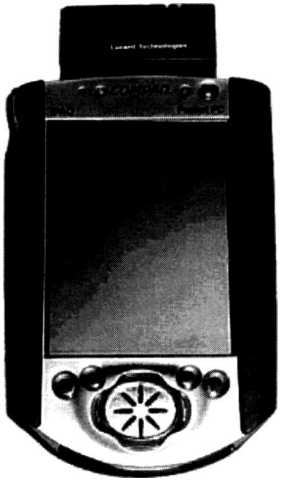

图 1.16　带有 PCMCIA 背夹和无线网卡的 iPAQ

技术规格

操作系统：Pocket PC 2002
处理器：206MHz Intel StrongArm 32 位 RISC 处理器
RAM：32MB 或 64MB
显示屏：TFT 液晶显示屏（4096 色）
显示分辨率：240×320
电池：可充电的锂电池（950mAh）
重量：6.7 盎司
高度：5.11 英寸