



802.11 无线网络权威指南 (第 2 版)



2006-8-23



翻译整理人员：

陈琳琦、郭新峰、钱良荣、刘超、席娟
许平华、尹周良、郑建波、周小琛、朱列

本中文根据《O'Reilly 802.11 Wireless Networks The Definitive Guide 2nd ed.chm》
英文版本翻译整理而成。

目录

802.11 无线网络权威指南	1
(第 2 版)	1
目录.....	3
序	14
前言.....	16
第 1 章 无线网络导论.....	24
1.1 为何需要无线？	24
1.1.1 无线频谱：关键资源	25
1.2 无线网络的特色	27
1.2.1 没有实体界限	27
1.2.2 动态实体介质	27
1.2.3 安全性	28
1.2.4 标准的好处	29
第 2 章 802.11 网络概论	31
2.1 IEEE 802 网络技术规格	31
2.2 802.11 相关术语及其设计	33
2.2.1 网络类型	34
2.2.2 再论传输系统	37
2.2.3 网络界限	38
2.3 802.11 网络的运作方式	40
2.3.1 网络服务	40
2.4 移动性的支持	44
2.4.1 移动性网络设计	45
第 3 章 802.11 MAC	47
3.1 MAC 所面临的挑战	48
3.1.1 射频链路质量	48
3.1.2 隐藏节点的问题	49
3.2 MAC 访问控制与时钟	50
3.2.1 载波监听功能与网络分配矢量	51
3.2.2 帧间隔	52
3.2.3 帧间隔与优先程度	53
3.3 利用 DCF 进行竞争式访问	54
3.3.1 DCF 与错误复原	55
3.3.2 使用重传计数器	55
3.3.3 DCF 与延迟	55

3.3.4 Spectralink 语音优先性	56
3.3.5 帧的分段与重组	57
3.3.6 帧格式	58
3.3.7 Frame Control 位	58
3.3.8 Duration/ID 位	62
3.3.9 Address 位	62
3.3.10 Basic Service Set ID (BSSID)	63
3.3.11 顺序控制位	63
3.3.12 帧主体	64
3.3.13 帧检验序列 (FCS)	64
3.4 802.11 对上层协议的封装	65
3.5 竞争式数据服务	66
3.5.1 广播与组播数据或管理帧	66
3.5.2 单点传播帧	67
3.5.3 省电程序	69
3.5.4 多种速率支持 (Multirate Support)	71
3.6 帧的处理与桥接	72
3.6.1 无线介质到有线介质 (802.11 至以太网)	73
3.6.2 有线介质至无线介质 (Wired Medium to Wireless Medium)	74
3.6.3 服务质量延伸功能	75
第 4 章 802.11 帧封装细节	76
4.1 数据帧	76
4.1.1 Frame Control (帧控制)	77
4.1.2 Duration (持续时间)	77
4.1.3 地址与 DS Bit	79
4.1.4 数据帧的次类型	81
4.1.5 数据帧的封装	82
4.2 控制帧	85
4.2.1 一般的帧控制位	85
4.2.2 RTS (请求发送)	86
4.2.3 CTS (允许发送)	87
4.2.4 ACK (应答)	88
4.2.5 PS-Poll (省电模式一轮询)	89
4.3 管理帧	90
4.3.1 管理帧的结构	90
4.3.2 长度固定的管理帧元件	91
4.3.3 管理帧的信息元素	99
4.3.4 管理帧的类型	112
4.4 帧发送以及连接与身份认证状态	116
4.4.1 帧等级	117

第 5 章 有线等级隐私 (WEP)	119
5.1 WEP 的密码学背景	119
5.1.1 串流密码锁的安全性	120
5.1.2 密码政治学	121
5.2 WEP 的加密机制	121
5.2.1 WEP 的数据处理	122
5.2.2 WEP 的帧格式	125
5.3 关于 WEP 的各种问题	126
5.3.1 RC4 在密码学上的性质	126
5.3.2 WEP 统设计上的瑕疵	126
5.3.3 针对 WEP 密钥的还原攻击	127
5.3.4 防范密钥还原攻击	128
5.4 动态 WEP	129
第 6 章 802.1X 使用者身份认证	130
6.1 可延伸身份认证协议 (EAP)	131
6.1.1 EAP 的封包格式	131
6.1.2 EAP 的要求与回复	132
6.1.3 EAP 身份认证方式	133
6.1.4 EAP 认证的成功或失败	134
6.1.5 EAP 交换程序范例	134
6.2 EAP 认证方式 (EAP Method)	135
6.2.1 加密的方式	135
6.2.2 非加密式 EAP 认证方式	137
6.2.3 其他的内层身份认证方式	138
6.3 802.1X: 网络连接埠的身份认证	139
6.3.1 802.1X 的架构及相关术语	140
6.3.2 802.1X 的帧过滤	141
6.3.3 EAPOL 的封装格式	141
6.3.4 定位	142
6.4 802.1X 与无线局域网络	142
6.4.1 802.11 网络上的 802.1X 交换程序范例	142
6.4.2 动态产生密钥	144
第 7 章 802.11I: RSN、TKIP 与 CCMP	145
7.1 临时密钥完整性协议 (TKIP)	145
7.1.1 TKIP 与 WEP 的差异	145
7.1.2 TKIP 的数据处理与过程	147
7.1.3 Michael 完整性检验	152
7.2 「计数器模式」搭配「区块密码锁链—信息真实性检查码」协议 (CCMP)	154
7.2.1 CCMP 的数据处理	155

7.3 固安网络 (RSN) 的运作方式	157
7.3.1 802.11i 密钥阶层体系	157
7.3.2 802.11i 密钥的产生与传递	159
7.3.3 混合加密类型	160
7.3.4 密钥快取	161
第 8 章 过程管理	162
8.1 管理架构	162
8.2 扫描	162
8.2.1 被动扫描	163
8.2.2 主动扫描	164
8.2.3 扫描结果	165
8.2.4 加入网络	166
8.3 身份认证	167
8.3.1 802.11 “身份认证”	167
8.4 事先身份认证	170
8.4.1 802.11 事先身份认证	170
8.4.2 802.11i 事先身份认证与密钥快取	171
8.5 连接过程	173
8.5.1 连接程序	173
8.5.2 重新连接程序	174
8.6 节省电力	176
8.6.1 Infrastructure (基础型) 网络的电源管理	176
8.6.2 IBSS 的电源管理	181
8.7 计时器的同步	183
8.7.1 Infrastructure 的计时同步	184
8.7.2 IBSS 的计时同步	184
8.8 频谱的管理	185
8.8.1 传输功率控制 (TPC)	185
8.8.2 动态选频 (DFS)	188
8.8.3 Action 帧	190
第 9 章 PCF 免竞争服务	196
9.1 以 PCF 提供免竞争访问	196
9.1.1 PCF 作业	196
9.1.2 基站的传输	197
9.1.3 免竞争期间的长短	199
9.2 PCF 帧的封装细节	199
9.2.1 免竞争期间结束 (CF-End)	201
9.2.2 CF-End+CF-ACK	202
9.3 电源管理与 PCF	204

第 10 章 物理层概观	205
10.1 物理层架构	205
10.2 无线链路	205
10.2.1 使用执照与管制	206
10.2.2 展频	208
10.3 RF 传播与 802.11	210
10.3.1 信号接收与效能	210
10.3.2 路径损耗、传输距离与传输量	212
10.3.3 多重路径干扰	213
10.3.4 讯符间干扰 (ISO)	214
10.4 802.11 的 RF 工程	215
10.4.1 RF 零件	215
第 11 章 跳频物理层	218
11.1 11.1 跳频传输	218
11.1.1 802.11 FH 的细节	219
11.1.2 802.11 跳频序列	220
11.1.3 加入 802.11 跳频网络	220
11.1.4 ISM 幅射量规定与最大传输量	221
11.1.5 干扰效应	221
11.2 高斯频移键控 (GFSK)	222
11.2.1 二阶式 GFSK	222
11.2.2 四阶式 GFSK	223
11.3 FH PLCP	224
11.3.1 分封 (Framing) 与白化 (whitening)	224
11.4 FH PMD	226
11.4.1 传输率 1Mbps 之 PH PHY 所使用的 PMD	226
11.4.2 传输率 2 -Mbps 之 FH PHY 所使用的 PMD	226
11.5 PH PHY 的特性	226
第 12 章 直接序列序列物理层： DSSS 与 HR/DSSS (802.11B)	228
12.1 直接序列传输	228
12.2 差分相移键控 (DPSK)	234
12.2.1 差分二进制相移键控 (DBPSK)	234
12.2.2 差分正交相移键控 (DQPSK)	234
12.3 “原本的” 直接序列物理层	236
12.3.1 PLCP 的分封 (framing) 与处理	237
12.3.2 DS PMD 附属层	238
12.3.3 DS PHY 的 CS/CCA	238
12.3.4 DS PHY 的特性	239
12.4 互补码调制 (CCK)	240

12.5 高速直接序列物理层 (HR/DSSS PHY)	240
12.5.1 PLCP 分封 (Framing) 与搅码 (scrambling)	241
12.5.2 HR/DSSS PMD	243
12.5.3 802.11b PHY 的非必要功能	246
12.5.4 HR/DSSS PHY 的特性	246
第 13 章 802.11A 与 802.11J.....	248
13.1 正交分频多工 (OFDM)	248
13.1.1 载波多工	249
13.1.2 正交性的意义 (不使用微积分)	249
13.1.3 防护时间	250
13.1.4 周期延伸 (周期前置)	251
13.1.5 加窗法 (Windowing)	253
13.2 802.11 所采用的 OFDM	253
13.2.1 将 OFDM13.2.1 302.11 a 所选用的 F.M 参数.....	253
13.2.2 作业频道的结构	254
13.2.3 作业频道	258
13.3 OFDM PLCP	260
13.3.1 帧的格式	260
13.4 OFDM PMD	263
13.4.1 编码与调制.....	263
13.4.2 电波效能: 灵敏度与频道拒斥.....	264
13.4.3 净空频道评估	264
13.4.4 传送与接收.....	264
13.5 OFDM PHY 的特性	266
第 14 章 802.11: 延伸速率物理层 (ERP)	267
14.1 802.11g 的组成元件	267
14.1.1 相容性议题	268
14.1.2 防护机制	268
14.2 ERP 的物理层收敛程序 (PLCP)	271
14.2.1 ERP-OFDM 的帧格式	271
14.2.2 802.11 g 的单载波帧格式	272
14.3 ERP 的实际搭酬介质 (PMD)	275
14.3.1 净空频道评估 (CCA)	275
14.3.2 接收程序	276
14.3.3 ERP 物理层的特性	276
第 15 章 802.11N 前瞻 :MIMO-OFDM	278
15.1 共同功能	278
15.1.1 多进与多出 (MIMO)	278
15.1.2 频宽	279

15.1.3 MAC 效能的提升	279
15.2 WWiSE	280
15.2.1 MAC 的改良	280
15.2.2 WWiSE MIMO 硬件层	283
15.2.3 WWiSE PLCP	286
15.2.4 WWiSE PMD	289
15.3 TGnSync	291
15.3.1 TGnSync MAC 的改良	291
15.3.2 TGnSync PHY 的改良	297
15.3.3 TGnSync 硬件层传输（PLCP 与 PMD）	300
15.4 比较与结论	304
第 16 章 802.11 的硬件	306
16.1 802.11 界面的一般结构	306
16.1.1 软件控制的无线电：离题插播	308
16.1.2 硬件实作上的议题	309
16.2 实现上的差异	310
16.2.1 重新激动界面卡	310
16.2.2 扫描与漫游	310
16.2.3 速率的选择	311
16.3 解读规格表	311
16.3.1 灵敏度比较	311
16.3.2 延迟范围	312
第 17 章 802.11 与 WINDOWS	313
17.1 Windows XP	313
17.1.1 安装网卡	313
17.1.2 选择网络	316
17.1.3 安全性参数与 802.1× 的状态设置	317
17.1.4 设置 EAP 认证方式	321
17.1.5 WPA 的状态设置与安装方式	326
17.2 Windows 2000	328
17.2.1 动态 WEP 的状态设置	328
17.3 Windows 电脑验证	329
17.3.1 运作方式	329
第 18 章 802.11 与 MACINTOSH	332
18.1 AirPort Extreme 网卡	332
18.1.1 软件安装	332
18.1.2 设置与监视 AirPort 界面	334
18.2 在 AirPort 上使用 802.1X	337
18.2.1 EAP 方法的配置设置	340

18.2.2 密钥链	341
18.2.3 故障排除	341
第 19 章 802.11 与 LINUX	345
19.1 Linux 所支持的 CIA	345
19.1.1 PCMCIA Card Services 概观.....	345
19.1.2 PCMCIA Card Services 的安装	347
19.1.3 监控网卡	348
19.1.4 排除资源的冲突	350
19.2 Linux 无线延伸功能与工具	352
19.2.1 编译与安装.....	352
19.2.2 以无线工具和 iwconfig 来设置界面	352
19.3 Agere (Lucent) Orinoco	358
19.3.1 编译与安装.....	359
19.3.2 设置 orinoco_cs 界面的配置	360
19.4 采用 Atheros 芯片组的网卡与 MADwifi	361
19.4.1 驱动程序架构与硬件访问层	361
19.4.2 先决条件	362
19.4.3 组建驱动程序	362
19.4.4 驱动程序的使用	362
19.5 在 Linux 中使用 xsuplicant	363
19.5.1 先决条件	363
19.5.2 编译与安装 xsupplicant.....	363
19.5.3 xsupplicant 的配置设置	364
19.5.4 网络连接与身份认证	365
19.5.5 Linux 上的 WPA.....	369
第 20 章 使用 802.11 基站	370
20.1 基站的基本功能	370
20.1.1 基站的种类.....	372
20.2 以 Ethernet 供电 (PoE)	374
20.2.1 PoE 的种类	375
20.3 选购基站	376
20.3.1 真的需要基站吗？	378
20.4 Cisco 1200 基站	378
20.4.1 设置 1200 基站	379
20.4.2 无线界面的配置设置	379
20.4.3 安全性的配置设置.....	381
20.4.4 监控.....	382
20.4.5 故障排除	383
20.5 Apple AirPort 基站	384

20.5.1	初次设置	384
20.5.2	管理界面	385
第 21 章	无线网络逻辑架构.....	388
21.1	评估逻辑架构	388
21.1.1	移动性	388
21.1.2	安全性	391
21.1.3	效能.....	392
21.1.4	骨干工程	396
21.1.5	网络服务	397
21.1.6	用户端整合	397
21.2	网络拓扑范例	398
21.2.1	拓扑 1: 单一子网络	398
21.2.2	拓扑形态 2: E. T. Phone Home 或 Island Paradise.....	403
21.2.3	拓扑形态 3: 动态 VLAN	407
21.2.4	拓扑形态 4: 虚拟基站	411
21.3	逻辑架构的选择	416
第 22 章	安全性架构	418
22.1	安全性的定义与分析	418
22.1.1	无线局域网络的安全问题	419
22.2	身份认证与访问控制	422
22.2.1	工作站身份认证与连接.....	423
22.2.2	链路层身份认证	424
22.2.3	网络层身份认证	426
22.2.4	以 RADIUS 整合用户身份认证.....	426
22.3	以加密确保私密性	428
22.3.1	静态 WEP	429
22.3.2	802.1X 动态 WEP 密钥	429
22.3.3	改良型 RC4 加密: TKIP	431
22.3.4	C C M P: AES 加密	431
22.3.5	较上层的安全协议 (IPsec、SSL 与 SSH)	432
22.4	安全性协议的选择	434
22.4.1	协议栈的安全防护	434
22.4.2	身份认证方式的选择	437
22.4.3	加密方式的选择	441
22.5	私设基站	442
22.5.1	检测	443
22.5.2	实际定位	443
22.5.3	关闭私设基站	446
第 23 章	网络规划与工程管理.....	448

23.1 工程规划与需求	449
23.2 网络需求	450
23.2.1 覆盖范围需求	451
23.2.2 容量需求	453
23.2.3 可移动性的需求	457
23.2.4 网络整合的需求	457
23.3 物理层的选择与设计	458
23.3.1 2.4 GHz (3.2.11 b/g) 频道规划	459
23.3.2 5 GHz (802.11a) 频道规划	461
23.3.3 混合式频道规划 (802.11 a+b/g 网络)	462
23.4 基站摆设位置规划	462
23.4.1 建筑物	463
23.4.2 初步规划	465
23.4.3 电波资源管理与频道规划	466
23.4.4 规划的修正与测试	466
23.4.5 准备最后的报告	468
23.5 使用天线调整覆盖范围	468
23.5.1 天线类型	469
第 24 章 802.11 网络分析	474
24.1 网络分析工具	474
24.1.1 8.2.11 网络分析软件	475
24.2 Ethereal	475
24.2.1 编译与安装	476
24.2.2 将无线界面设定为监听模式	476
24.2.3 执行 Ethereal	478
24.2.4 减少数据量	480
24.2.5 使用 Ethereal 进行 8.2.11 分析	480
24.3 802.11 网络分析项目清单	485
24.3.1 显示过滤初探	485
24.3.2 一般疑难排除过程	486
24.4 其它工具	489
24.4.1 搜索、量测与对映网络	490
24.4.2 WEP 密钥还原	490
24.5 身份认证	491
第 25 章 802.11 效能比较	492
25.1 802.11 效能评估	492
25.1.1 计算示范	493
25.2 改善效能	494
25.3 802.11 可调参数	495

25.3.1	无线电波管理	495
25.3.2	电源管理调校	497
25.3.3	计时过程	498
25.3.4	可调参数一览表	499
第 26 章	结论与展望	500
26.1	标准化过程	500
26.1.1	新的标准	500
26.2	无线网络的当前趋势	502
26.2.1	安全性	502
26.2.2	网络部署与管理	503
26.2.3	应用程序	506
26.2.4	协议架构	507
26.3	结语	508

序

早在碰面之前，Matthew Gast 就已经是我的心灵导师。我发现 Apple 果真推出传闻已久的 802.11b AirPort 基站，便于 2000 年 10 月开始报导无线数据网络。

我曾经热衷于所谓的红外线无线网络，也曾浪费许多时间把玩一些“有趣”却走入死胡同的网络技术。原本以为 802.11b 不过是另一种玩具。很高兴我是错的！

一路这样摸索过来，让我遇见了初版的《802.11 无线网络技术通论》。广告说成那样，这玩意真的能动吗？我对 ISO 参考模型、TCP/IP 与 Ethernet 架构还算颇有了解，不过仍然无法将 Ethernet 的「分享式竞争：（shared contention）与这种容许众声喧哗的介质兜在一块。

通过文字与图表，Matthew 教我一些原本并不了解的东西。过去五年，我在纽约时报(New York Times)、西雅图时报(The Seattle Times)、PC World 以及自己所开设的 Wi-Fi Networking News (<http://www.uifinetnews.com>) 网站上发表过许多文章。写了以浅显易懂的方式向一般大众解释何谓 Wi-Fi，当我深入探究技术细节时，这些文字图表都是我一再回顾的东西。

一开始，我从《802.11 无线网络技术通论》学习相关术语 (acronym)。通过 Matthew 这本书，后来终于超越只知「WDS 代表 Wireless Distribution System」的程度，真正了解基站之间如何通过「允许四方协商封包传输：的 802.11 内建机制，彼此交换数据。

物换星移，802.11 家族逐渐成熟而多样化，如今本书第一版已经稍嫌过时。不过令人惊讶的是，这些所谓的「创新」，仍然根植于 1990 年代初期至中期的技术发展。相较于 2005 年，本书第一版的术语 (alphabet soup) 只能用清淡来形容。

【译注：alphabet soup 原本是康宝所推出的一种浓汤，里面有英文字母形状的面团，后来引申为缩略术语(acronym)。】

为了弥补本书初版与无线网络发展现况之间的差距，Matthew 持续在 O'Reilly 的 Wireless DevCenter 发表文章，每一篇我都迫不及待地仔细拜读。在一一场 Wi-FiPlanet 所举办的会议上，有人把 Matthew 介绍给我认识。我们可说是一见如故：如果记得没错的话，当时我向他请教 802.1X 相关细节，而他只想谈谈我的书，了解我在做些什么。（之前我写过两本通俗的 Wi-Fi 书，不过无法与 Matthew 这本优秀的技术书相提并论。）

从那时起，我就坐拥少有的特权，得以分享 Matthew 的真知灼见。Matthew 从不轻易论断，而是倾向深入研究。与生俱来的好奇心驱使他不断深掘，直到获得技术上与逻辑上一致的答案。

以发展过程错综复杂且充满政治角力的 802.1X 标准为例。（若非 Matthew，我还不知道 X 应该大写，因为 802.1X 是独立而非附属于其他规格的标准。虽然大家遵循的是 IEEE 所立下的规矩，不过连 IEEE 本身都犯了这个错误。）

802.1X 本身并不复杂，它采用一种通用的信息传递方式进行身份认证，称为「可延伸身份认证协议」(Extensible Authentication Protocol，简称 EAP)。不过对于如何确保 EAP 本身的安全性，十足反映出 Microsoft 与 Cisco 之间的竞争。为了控制这项老旧协议，两家公司角力的结果，反而让 EAP 无法达到更高的安全性。

Matthew 跳脱这些沾染宗教色彩的论战，在 O'Reilly Network 发表一篇文章，列举出各种可行的方法、所遭遇的困难，以及互通性相关议题，这些精华都收录在本书当中，而且增加了不少篇幅。本书出版之前，我想读者很难在其他地方找到更完整、更具说服力的解释。你很难在他处找到比这些内容更清晰、更容易理解且不受市场政治左右的文章。

有时候, **Matthew** 会将本书迟迟未能改版, 归咎于自己加入一家生产无线网络交换器的新创公司。不过我倒认为, 读者反而因此受惠于这些得之不易的知识。

以往, **Matthew** 与 802.11 之间的关系就像是熟悉自家一草一木的工匠。马桶坏了, 他就动手换个活门。客厅需要新的电源插座, 他就研究看看如何进行, 然后接条线过来。

但是 **Matthew** 的新工作, 让他从周末的家居战士变身为万能师傅。打掉内墙、重砌、铺管与架线不仅难不倒他, **Matthew** 还会偶尔抱怨一下当地的建筑法规。很荣幸能够认识 **Matthew**, 更荣幸的是能够介绍这本书给各位, 让各位都能够一探过去几年来, 我和其他人一直共享的秘密花园。

— Glenn Fleishman

西雅图, 华盛顿

2005 年 2 月

前言

人们可以行动自如，而网络则不然。

相较于其他说法，这句话更足以解释无线局域网络（wireless LAN）在硬件方面的爆炸性成长。不过短短几年，无线局域网络已经从昂贵、新奇的玩物，成长为当前的主流技术。

无线网络让使用者摆脱网络连接的束缚，不再受制于网络实体位置，不过要摆脱具体的网络限制，需要不少的协议工程·为了提供使用者不受空间限制的服务·系网络必须掌握更多使用者所在位置的信息。

本书的写作，有更多时间是花费在飞机上、机场里以及火车上。要将演变中的网络技术浓缩为一本书，大部分的研究工作都离不开网际网络。要不是能够随时随地访问网络，本书或许得耽搁更久方能问世。

无线网络的优势使它们快速成长为数十亿美元的设备市场。如今 Wireless LAN 在整个网络环节中已占有一席之地，学习如何掌握 Wireless LAN 自然成为人们必须面对的课题。

解放的普罗米修斯：Wireless LAN 的种种可能性

相较于固定（或有线）网络，无线网络具备下列优点：

移动性

使用者有四处游走的需要，不过数据通常集中储存。能够让使用者在行动间访问数据，可大幅提高生产力。配置网络是为了提供使用者有价值的服务。过去，网络设计人员所关注的焦点在于网络连接点，因为每个连接点通常对映到一位使用者。不过无线网络并没有实体连接点，因此使用者身份便成为网络设计的重心。

部署容易，配置快速

对传统的有线局域网络（wired LAN）而言，要在某些场所布线相当困难。建筑物老旧通常是问题所在；要在一栋设计蓝图已经不知去向的旧式石材建筑中穿墙布线，的确不是件容易的事。此外，有些地区碍于法令限制，要在列为古迹的建筑物中架设局域网络更是难上加难。就算设备地点位于新建的设施，除了所费不菲，布线也十分耗时。

弹性

既然无须网线，也就没有重新布线的问题。利用无线网络，使用者可以迅速建构小型。临时性的群组网络以供会议之用，随意游走于办公室隔间也变得易如反掌。相形之下，无线网络的扩充十分容易，因为网络介质无处不在。使用者再也不必到处拉线。接线甚或是绕线。弹性是 hot spot（热点）市场一包括旅馆、机场、车站（甚至是列车本身！）、图书馆以及咖啡馆一的最大卖点。

成本

有时候，采用无线技术可以节省不少成本。举例而言，可以利用 802.11)设备在两栋建筑物之间搭设一道无线桥梁（wireless bridge）。配置无线桥梁须支付一些初期购置成本，包括户外

设备、无线基站 (access point) 以及无线网卡(wireless interface)。扣除初期的固定资本支出，以 802.11 做为底层架构、视线 (line-of-sight) 对接的网络，每月所需要支付的营运成本可说是微乎其微。长期而言，这种点对点 (point-to-point) 的无线链路远比电话公司所提供的专线便宜得多。

虽然有上述种种的好处，在 1997 年 802.11 标准确定之前，使用者只能屈就于个别厂商所提供的解决方案，承担其所附带的风险。直到 802.11 开始席卷市场，传输速度随即由 2Mbps 跳升为 11Mbps 以至于 54Mbps。无线界面卡以及天线的标准化，使得配置无线网络不再遥不可及。许多服务供应商(service provider) 趋势推出相关服务，一些主要城市的自愿团体也开始利用 802.11 建构公用无线网络(public wireless network)。

802.11 已经成为一种普遍公认的连接方式。只要有一组基站，就可以为访客提供连接服务，不必再通过 Ethernet 开放公用连接点。802.11 成为标准这几年来，「热点」(hot spot)一词的含义，已经从带点异国情调的固定场所，转变为能够在行进间提供连接的技术。以 802.11 搭配卫星上链，就算行进速度很快，一样可以访问网际网络。有些铁路通信系统已经开始提供移动式热点。即便巡航速度 (cruising speed) 高达每小时 550 英里，波音公司的 Connexion 也可以在飞机上提供类似服务。

致读者

本书主要针对需要进一步涉猎 Wireless LAN 营运(operation) 部署(deployment) 以及控管(monitoring) 种种技术层面的读者：

- 打算将 802.11 设备整合到现有网络或是配置 802.11 网络的设计人员 (network architect)。
- 负责配置与维护 802.11 未网络的管理人员 (network administrator)。
- 关切 802.11 设备在部署上可能衍生的安全问题以及致力解决这些问题的安全专业人员 (security professional)。

本书假定读者具备某种程度的电脑网络相关背景知识。读者应该对 IEEE 802 网络 (特别是 Ethernet)、OSI 参考模型、TCP/IP 以及其他相关网络通信协议有基本的了解。对大多数网管人员而言，无线局域网络并非全新领域，不过还是有若干新的概念，特别是在无线传输方面。

关于本书第二版的说明

有些技术变动十分快速，想要为之著书立说不容易。困难之处，部分是因为无法十分确定应该涵盖哪些内容。本书改版这几年间，安全性占据整个发展的主轴，因此更新这方面的信息就成为本次改版的重点。本书有两个主要目的：除了教导读者 802.11 标准本身，也提供配置 802.11 Wireless LAN 实务上的建议。这两个目的本身互不冲突，因此各位可以挑选自己感兴趣的章节。为了协助读者决定阅读顺序以及对章节配置有整体的概念，将各章内容摘要于下：

第一章〈无线网络导论〉论述了无线网络与传统有线网络之间的差异，以及采用无线介质时必须面临的种种问题，例如网络界限模糊以及介质不可靠等问题。Wireless LAN 或许具体展现了 Christian Huitema 所说的『Internet 没有中口，只有不断扩展之边际』。当 Wireless LAN 技术逐渐普及，整个边际也就更形模糊了。

第二章〈802.11 网络概观〉描述了 802.11 Wireless LAN 的整体架构。802.11 有点类似 Ethernet，不过加入了一些新的网络元件，以及一堆新的术语。读者可在本章看到使用 802.11

网络时，将会接触到的网络元件。大致而言，这些元件包括工作站（station 配备无线网卡的行动设备）、基站（access point，位于工作站与传输系统之间的桥接器）以及传输系统（distribution system，即有线骨干网络）本身。工作站在逻辑上被划归他各个基本服务集（basic service set，简称 BSS）。如果没有基站参与其中，该网络即是较为松散。由工作站彼此自治（ad-hoc confederation）的独立型基本服务网域（independent BSS，简称 IBSS）。基站允许个别的 BSS 彼此串连为逻辑上相连的群组，此种结构称为延伸式服务组合（Extended Service Set 简称 ESS）。

第三章 <802.11 MAC> 深入探讨了 802.11 标准的介质访问控制（Media Access Control，简称 MAC）层协议。和所有 IEEE 802 网络一样，802.11 将 MAC 层功能与实体介质访问功能加以区分。802.11 包含了许多不同的物理层，不过使用相同的 MAC。网络介质的访问方式主要还是通过竞争（contention），不过其所采用的是碰撞避免（collision avoidance，即 CSMS/CA）而非碰撞检测（collision detection，即 CSMA/CD）。本章同时探讨了 802.11 帧（frame）的数据封装方式（data encapsulation），让网络管理人员得以了解传输数据时所使用的帧格式。

第四章 <802.11 帧封装细节> 以第三章为基础，详细说明了不同类型的帧及其使用场合。本章比较偏向参考之用，而不是做为实际的阅读材料。本章详细描述了三种主要帧。数据帧（data frame）负责传输数据。控制帧（control frame）扮演监督（supervisory）的角色。而管理帧（management frame）负责协助 802.11 MAC 完成其他延伸作业。信标信号（Beacon）除了用来宣布 802.11 网络的存在，以及协助整个连接过程（association process），对工作站进行身份认证时也派得上用场。

第五章 <有线对等私有（WEP）> 描述了对等私有（Wired Equivalent Privacy，简称 WEP）协议。虽然有所瑕庇，WEP 仍是无线局域网络安全领域许多后续工作的基础。本章探讨了何谓 WEP、WEP 如何运作。以及为何不能仰赖 WEP 提供有用的隐私与安全。

第六章 <802.1X 使用者身份认证> 描述了 802.1X 身份认证架构。搭配「可延伸身份认证协议」（Extensible Authentication Protocol），802.1X 为无线局域网络提供了坚固的身份认证解决方案，同时改善了加密方面的功能。

第七章 <802.11i: RSN、TKIP 与 CCMP> 描述了 802.11i 无线局域网络安全标准。为了解决 WEP 的基本瑕庇，802.11i 设计了两种新式的链路层加密协议，以及产生与传递密钥的机制。

第八章 <管理作业> 主要在探讨 802.11 网络的管理作业。加入任何网络之前，工作站必须通过扫描，以寻找由基站或 IBSS 创建者主动发布的网络。传送任何数据之前，工作站与基站之间必须处于连接状态。本章同时探讨了 MAC 内建的省电功能，省电功能可以让以电池供电的工作站进入休眠模式，并且定时醒来接收为其暂存的数据。

第九章 <采用中枢协调功能的免竞争服务> 主要在探讨中枢协调功能（point coordination function，简称 PCF）。PCF 在实作上并不常见，因此本章可略过不读。PCF 是以免竞争（contention-free）方式访问无线介质的基础。在免竞争访问中，无线介质是由中央控管，访问时必须持有权杖（token），此权杖通常提供自基站。

第十章 <物理层概观> 探讨了 802.11 模型中物理层（physical layer，简称 PHY）的一般架构。PHY 本身可进一步区分为两个次协议层（sublayer）。物理层收敛程序（Physical Layer Convergence Procedure，简称 PLOP）次协议层，除了加入同步信号（preamble）以形成完整帧，同时也加入了本身的标头，而实体搭配介质（Physical Medium Dependent，简称 PMD）

次协议层，则会为帧加入调制（modulation）的搁节。较常见的 PHY 是以射频（radio frequency，简称 RF）做为无线介质，因此本章将以 RF 系统与技术的简短讨论做为结尾。

第十一章〈FH PHY〉所描述的是最早期的 802.11 物理层。市面上已经很难买到 FH PHY 相关产品，不过早期大多数设备均采用此物理层。历年来一直参与 802.11 技术发展的机构，或许也有熟悉此物理层的需要。

第十二章〈DS PHYs: DSSS 术为基础的两种物理层。802.11 原始标准所规范的物理层提供 1Mbps 与 2Mbps 两种速率。不过，直到 802.11b 加入 5.5Mbps 与 11Mbps 这两种传输率，整个技术才算真正起飞。本章将一并描述这两种密切相关的物理层。

第十三章〈802.11a 与 802.11!：5-GHz OFDM PHY〉探讨了 802.11a 5-GHz 物理层，传输速度可达 54Mbps。此物理层所使用的调制技术，称为「正交分频多工」（orthogonal frequency division multiplexing，简称 OFDM）。此实体要稍加修改方能在日本使用，亦即后来的 802.11j 标准。

第十四章〈802.11g：延伸速率物理层〉主要在探讨一种使用 OFDM 技术但与 802.11e 共用 2.4 GHz 频段的物理层，802.11g 大幅压缩了 802.11e 的生存空间，也是新式笔记型电脑常见的内建连网方式。此物理层与 802.11a 物理层几乎完全相同。差别在于 802.11g 可以回溯相容于使用相同频段的旧设备。

第十五章〈802.11n 前瞻；MIMO-OFDM〉描述了目前仍在开发中的物理层。为了提供更高速率，802.11n 所使用的物理层，是以「多进多出」（multiple-input/multiple-output，简称 MIMO）为基础。本书即将付梓之际，这两份标准建议书尚在委员会中角力。两者在本章均有探讨。

第十六章〈802.11 硬件〉开始从理论性议题过渡到标准的实作议题。802.11 算是比较宽松的标准，留给实作上相当大的空间。不同的网卡可能具有不同的效能，协议的实作上也可能有所差异。这些差异主要来自于硬件的建构方式。

第十七章〈802.11 与 Windows〉描述了 Windows 驱动程序基本的安装程序，以及安全方面的配置设置。

第十八章〈802.11 与 Macintosh〉描述了如何在 MacOS X 上使用 AirPort 网卡连接至 802.11 网络。焦点放在 Mac OS X 10.3，因为这是首次支持 802.1X 的版本。

第十九章〈802.11 与 Linux〉描述了如何让 Linux 系统支持 802.11 网络。交待了如何让作业系统支持 PC Card 之后，本章会接着说明如何使用无线延伸功能（wireless extension）的 API。于此将探讨两种常见的驱动程序，一种支持旧式的 Orinoco 802.11b 网卡，另一种则支持使用 Atheros 芯片组的新式网卡，称为 MADwifi。最后，本章将说明如何使用 xsupplicant 进行 802.1X 安全性配置设置。

第廿章〈使用 802.11 基站〉探讨了 802.11 基础型（infrastructure）网络所使用的设备。商用基站产品功能各不相同。本章描述了基站上常见的功能、提供采购建议以及两个实际的设置范例。

第廿一章〈无线网络逻辑架构〉是本书论述层次的第三次转变，从 802.11 个别设备的实作层面，过渡到如何配置较大规模的 802.11 网络。配置网络时有几种不同的做法可供选择，这些做法各有其优缺点。除了列举常见的网络拓朴形式，本章还会提供选择上的建议。

第廿二章〈安全性架构〉应该接着上一章阅读。安全性架构的主要挑战，在于如何以开放性介质提供网络访问，又能同时兼顾网络安全。安全性的选择与架构上的选择彼此互相影响。本

章提出了设计网络时必须面临的几项重要抉择：打算使用何种身份认证方式？如何与现有的使用者数据库整合？如何加密以确保数据安全？以及如何处理未经授权的基站部署问题。

第廿三章〈网络规划与专案管理〉是针对网管人员的最后一章。设计大规模的无线网络之所以困难，是因为要求访问的使用者数量太多・如何确保网络具备足够频宽以满足来自四面八方的使用者需求，免不了需要事先规划。基站的区位选择，绝大部分取决于无线波环境。传统上，这是配置网络时最耗时的工作。

第十四章<802.11 网络分析>主要在教导网络管理人员如何得知 Wireless LAN 发生了什么事。不论在有线或无线网络中，网络分析软件都具有相当的价值。本章探讨了如何使用网络分析软件，以及各种症状的意涵。其次，描述如何编译 **Ethereal** 分析软件，以及如何著手进行一般问题的障碍排除。

第廿五章〈802.11 效能调校〉主要探讨网管人员如何提升传输量。一开始，本章将描述如何计算原始数据（payload data）的整体传输量，以及提升效能的一般做法。有时候，调整一些常见的 802.11 参数或许会有所帮助。

第廿六章<结论与展望>用来总结 802.11 工作小组目前正在进行的标准化任务。综述这些进行中的任务之后，至少我可以预见与希望，本来本书改版时可以不必大费力气的。

与第一版的主要差异

2002 至 2005 三年间，无线局域网络历经相当大的变动。标准本身持续演进，提供更高的安全性与互通性。依「更快・更好、更便宜」的典型技术发展形式，大多数 802.11 的数据传输率，已经从 802.11b 的 2 或 11 Mbps，跃升为 802.11a 与 802.11g 的 54Mbps。即便在大规模网络的应用上仍有其限制，「速度更快」与「回溯相容」已经证明是 802.11g 在商业上致胜的配方。即将标准化的 802.11n 意在进一步提升速度。使用者莫不迫切期待物理层技术的进一步发展，由「前标准」（pre-standard）产品相当受到欢迎即可印证。本书增加了两个全新的章节，分别探讨 802.11g 与 802.11n。在 802.11h 的频谱管理发展过程中，欧洲采用 802.11a 纯属偶然事件，因此管理章节必须大幅改写。

本书第一版于 2002 年发行时，802.11 的安全性经常受到质疑。WEP 显然有所不足，不过当时并没有更好的替代方案。大多数网管人员比较习惯应付内置（而非外设）的远端访问系统。802.11i 的发展大幅简化了网络的安全防护工作。如今，安全性的考虑已经内置于规格书中，不像以往需要假以外求。安全性的改良散见全书，从说明新协议如何运作的全新章节，到如何将之运用于用户端，以至于配置网络时如何筛选不同的选项。比起三年前，筛选适当的安全性选项如今变得更为复杂，因此有必要从初版的一节，扩增为独立的一章。

三年前，基站大多十分昂贵。而且数量一多，基站的表现就如人意。进行网络部署时，通常得试着突破当时既有设备的种种限制。三年后，基站的功能更强、选择更多，部署时也更具弹性。如今已经有多种选项可供选择，不再需要屈就「一体适用」（one size fits all）的部署模型。安全性协议已有长足的改善，如今探讨部署技术时，已经可以著眼于它能够为组织贡献什么，不必再担心或聚焦于如何防止失控的情况发生。因此，原本有关网络部署的篇幅扩增为三章，分别探讨部署程序的各个主要部分。

本书字型惯例

斜体字型用于：

- 路径名称、文档名称以及路径
- Internet 地址，例如网域名称与 URL

粗体字型用于：

- 值得使用者注意的名词

定宽字型用于：

- 屏幕上应该键入的命令列及其参数
- 所列出的程序码

定宽斜体字型用于：

- 可以代换成实际值之处

定宽粗体字型用于：

- 程序码范例中由使用者键入的文字

建议与问题

欧莱礼公司是世界性的电脑信息出版公司。我们永远乐意听到读者对出版品的意见包括如何让本书可以更好的建议、指正本书的错误 • 或是读者建议本书往后改版时，应该再加进来的其它主题。以下是本公司的联络数据：

美商欧莱礼股份有限公司台湾分公司

电话：(02) 2709-9669 传真：(02) 2703-8802

网址：<http://www.oreilly.com.tw>

电子邮件：mail@oreill.com.tw

与本书有关的网上信息（包括勘误、范例程序、相关联结）

原文书

<http://www.oreilly.com/catalog/802dot112/>

中文书

http://www.oreilly.com.tw/product_network.php?id=a183

致谢

尽管乐于相信各位阅读本书是因为它的娱乐价值，我还不至于如此天真。相较于枯燥的技术规格，技术类书籍的价值在于能够正确地呈现细节，并且用比较容易理解的方式加以表达。每一本技术类书籍背后，都有一个审稿团队负责检视初稿并协助改善。我的审阅小组找出了一堆错误，使本书更加完备。Tropos Networks 的 Malik Audeh 博士堪称我的无线良知（找不到更好的字眼可以形容）。我并非无线方面的专家—我所拥有的无线知识，都是因为对 802.11 咨询学习而来。802.11 问世之前，Malik 就已经通晓无线技术，而我一直有幸可以分享他的洞见，Texas A&M 的 Gerry Greager 在 FCC 法规与免照设备的管制方面提供了不少洞见，由于无线局域网络近年来不断颠覆这些法规。因此这些洞见愈发显现其价值，Glenn Fleishman 答应为本书写序时，我压根想不到他竟然会耗费那么多心力，从更为宏观的脉络来检视 802.11。他所建议的一些细节，是参考过去几年他在自己的 Wi-Fi Networking News 网站上所发表的一些文章。同样身为作家，Gleen 指出几个地方可以提供更好的范例，让我的论点更加清楚。最后要感谢 Open1X 专案的 Terry Simons，他在 Linux 的 802.11，以及几乎所有主要作业系统的 802.1X supplicant 上花费了不少功夫。Terry 同时也是 Utah 大学「无线身份认证系统」的架构设计师。本书中论及安全性规格，以及使用 supplicant（申请者）与建构 authentication system（身份认证系统）的实务部分，在此可以感受到他的专长。

至于协助我赶上目前 802.11 发展潮流，以及与我分享他们所知的其他人士。2002 年起，我有幸能够参与 Interop Lab 无线安全性与 802.1X 的相关会议，与课堂相比，现实世界总是太过混乱。每年从这些自愿参与的活动中所学习到的，远比参加特定的课程来得更多。通过 Interop Labs，我认识了 xsupplicant 专案的开发首席 Chris Hessing。Chris 总是慷慨倾囊相授，为我解释密钥如何在 802.11 中传递。这可没有想像中简单！我的同事 Sudheer Matta 总是不吝对我说标准世界发生什么新鲜事，以及 MAC 小组的工作纪录细节。

感谢 O'Reilly 所提供的各式各样协助。2001 年开始写作本书第一版时，Ellie Volckhausen 所设计的封面就挂在我的座位前面，以及我所拥有的大部分电子设备上头。（在我的手机上看起来一样很好！）Jessamyn Read 将我成堆的速描转为可供陈列的插图，而且是在相当紧凑的期限内完成。我不知道产品编辑 Colleen Gorman 花了多少时间才完成本书，希望她的家人和她的猫咪 Phineas 能够原谅我。如同以往，我得感谢编辑 Mike Loukides 所展现的智慧。Mike 让整个专案保持在以往我们合作时所习惯的方式。他所具备的业余无线背景，在我写到天线与 RF 传输相关章节时特别有所帮助。（还有很多很多必须感谢他的，例如有关 Aricebo 电波望远镜的注解！）

写作和生命中其他事情没有两样，魔鬼都在细节里。要保持正确，通常意味著重写、重写、再重写。进学院之前，我并没有任何大型写作计划的经验，直到修了一门 Brad Bateman 教授所开的美国金融体系 (U.S. Financial System) 课程。虽然的确学到货币在经济系统的流通，以及联邦准备理事会 (Federal Reserve) 用以形成政策的工具，回顾既往，我觉得最有价值的，是掌握到如何撰写结构严谨之长篇论文的程序。除了写作，Bateman 教授十分强调重写过程，在写作本书时，我不时用到这个技巧。不过，我并不只是将 Bateman 教授当做杰出的写作导师，或者仅止于在复杂的经济议题上为学生解惑的经济学家。Bateman 教授不会受限于自己的学术专长。准备写作本书第二版时，我参加了他的一场演讲，主题和我的母校社会史有关。在令人神驰的一个小时中，他追溯了母校的历史，以及其与较广泛的社会运动之间的关系，这解释了我的母校何以拥有目前的文化，如此深入的剖析，远超过我当学生时所能理解的程度。并非所有教授



华为 3COM

都会考量如何让学生为进入研究所先作准备，也不是所有教授都会将他们的教诲局限于课堂中。在他的影响之下，我学到如何成为一个更好的作家、经济学家以及公民。

写作一本书时，感谢其他人有形的贡献总是比较容易。然而在每个作家背后，都有一些默默付出的亲人与朋友。如同以往，我的妻子 Ali 以无比幽默感纵容我的写作习惯，特别是为本书所牺牲的无数周末。一些朋友以各种形式的鼓励与协助支持本书的写作：对此，我必须感谢 Annie、Aramazd • Brian • Dameon • Kevin 以及 Nick（依字母顺序排列）。

— Matthew Gast

加州，旧金山

2005 年 2 月

第1 章 无线网络导论

近五年来,整个世界逐渐走向移动化。因此,传统的连网方式已经无法应付新生活形式所带来的挑战。如果非得通过实体线缆才能够连上网络,使用者的活动范围势必大幅缩小。无线网络便无此限制,使用者可以享有较宽广的活动空间。因此,无线技术正逐渐侵蚀传统「固定式」(**fixed**)或「有线式」(**wired**)网络所占有的领域。这种改变对每天开车的人来说分外明显,因为边开车边使用移动电话的驾驶行径,已经让他们随时都得面对攸关生死的挑战。

语音通信的无线化,造就了一个全新的产业,为电话注入移动性,已经对于语音通信事业造成深刻的影响。因为如此一来,人与人之间就可以直接联系,不必受限于设备(**connected to people, not devices**)。在电脑网络领域,我们面临同样深刻的巨变。无线话之所以如此受到欢迎,是因为人们可以丝毫不受地点的影响而彼此沟通。针对电脑网络所发展的种种新技术,让**Internet**连接得以提供相同的无线功能。到目前为止,**802.11**算是最成功的无线网络技术。

在本书第一版,我曾经提到**802.11**将是引领移动数据网络的顶尖趋势。当时,**802.11**正与第三代行动技术竞逐主流地位(**mindshare**),无庸置疑的是,如今**802.11**算是略胜一筹。

1.1 为何需要无线?

然而,如果我们现在就一头栽进特定技术的细节,未免有些言之过早·不论其所使用的协议如何设计,不论其所传送的数据属于何种形式,各种无线网络之间,其实具备许多共同的优点。

无线网络最明显的优点,在于提供人们移动性(**mobility**)。无线网络的使用者可以连接至既有网络,而后随意漫游。通过基站(**cell tower**),使用者可以一面开车,一面利用手机通话。起初手机十分昂贵,价格因素使得手机用户局限在销售经理(需要高度的移动性)以及重要的决策阶层(需要随时能够联络得上)。移动电话已经证实是一项十分有用的服务,如今手机在美国已相当普及,至于欧洲就更不在话下。

同样地,无线数据网络(**wireless data network**)让软件开发人员从此不必再受**Ethernet**网线的束缚。他们可以在图书馆、会议室、停车场甚至对街的咖啡馆工作。只要使用者不走出基站(**base station**)的覆盖范围,即可使用网络资源。唾手可及的无线网络设备能够轻易涵盖整个公司;只要花些工夫,用点特殊设备,就可以让**802.11**网络的覆盖范围延伸至想要的地区,距离甚至可以长达数里。

无线网络通常具备相当大的弹性,换个说法就是部署快速。无线网络可以通过基站让使用者连接到既有的网络;在**802.11**网络中,基站(**base station**)又称为接入点(**access point**)。然而不论用户多少,无线网络基础建设在本质上并没有什么差异。要在某个地区提供无线网络服务,必须先将基站与天线定位。一旦完成基础建设之后,要在无线网络中加入新用户只不过是授权(**authorization**)之劳。虽然基础建设完工之后,仍须经过设置的步骤,才能够辨认用户身份以及提供服务,不过单就授权本身而言,并不需要新增额外的设备。要在无线网络中新增一位用户只须设置基础设备的配置,不必拉线、打洞与配置网络插座。

弹性对服务供应商（service provider）而言十分重要。hot spot（热点）连接市场是 802.11 设备厂商必争之地。班机或列车误点时，在机场与车站等候的商务人士或许会有上网的需求。咖啡馆以及其他公众聚集的社交场合亦然。有些咖啡馆已经开始提供 Internet 访问服务；通过无线网络访问 Internet 不过是现有服务的自然延伸。虽然 Ethernet 的插座一样能够提供访问服务，但是通过有线网络的做法也并非全然没有问题。主要是布线既贵且费时，有时甚至需要重新装璜。此外，要辨别哪条线路出现问题，通常是艺术的成份大于科学。如果使用无线网络，不但可以省下装璜的工夫，也无庸费神分析（或瞎猜）损坏何在。只要基础设施的有线网络可以连上 Internet，不论使用人数多少，无线网络都可以满足每个人的需求。虽然无线局域网络的频宽有限，但实际上 WAN（广域网络）的频宽成本才是小型 hot spot 网络的瓶颈所在。

弹性对老旧建筑而言特别重要，因为可以避免大兴土木。一旦建筑物被列为古迹，改建就更加困难。除了满足业主需求，改建工程还必须符合古迹维护单位的限制，以免破坏历史文物。无线网络在类似环境中可以快速部署，因为有线网络的安装通常只占其中一小部分。

另一方面，弹性造就了草根性社区网络（grassroots community networks）的发展。随著 802.11 设备价格的快速滑落，各式各样的自愿团体开始设置开放给公众使用的无线共享网络。社区无线网络也打破了 DSL 的限制，让以往不敢如此奢望的社区，也能够以高速访问 Internet。在传统有线网络难以企及的化外之地，社区无线网络特别成功。

802.11 早期使用概况

虽然呈现爆炸性成长，不过 802.11 并非全面均衡发展。有些下场成长较快，因为无线网络对这些市场而言特别有价值。通常，愈重视移动性与弹性的市场。局域网络的兴趣就愈大。

负责物流的组织（如 UPS、FedEx 或者航空公司）或许是率先采用 802.11 的使用者。在 802.11 之前，包裹追踪系使用专属的无线局域网络。标准化使得产品价格下滑，也使得网络设备供应商彼此更加竞争，因此以标准化产品取代专属产品。可说是简单不过的决定。

医疗产业也是无线网络的早期使用者，因为医疗器材通常需要较大的弹性。病患需要在医院中移来移去，而照料病患的医疗专业人员，算是经济体系中最机动的一群工作者。技术先进的医疗组织早就采用无线局域网络传递病历，让医生更方便取得病历相关信息，有助于医疗品质的改善。电脑化病历可以跨部门传送，无需费神再去解读某些传奇大夫鬼画符似的笔迹。在纷扰嘈杂的急诊室，能否快速取得影像数据有时会成为救命的关键。有些医院已经采用个人电脑，通过无线局域网络，让具有特殊配备的「急授车」（crash cart）可以即时访问 X 光片，这样医师就可以即时诊断，不必等到 X 光片显影完成。

有些教育机构对于无线局域网络十分狂热。十年前，为了吸引学生，各家学院无不吹嘘自家校园网络如何如何。能够提供愈多高速上网的场所，就能够更吸引学生。如今，教育界的要闻是各学院已经开始在整个校园布建无线局域网络。学生通常是移动网络的重要使用者，可以受惠于课堂间，或者「第二个家」（homes away from home，如图书馆、工作室、实验室，视主修而定）随处可用的网络。

和所有网络一样，无线网络同样是通过网络介质传送数据。无线网络所使用的介质属于某种形式的电磁辐射。为了满足移动网络的使用需求，此介质必须能够涵盖较广的区域，好让使用者能够在其所覆盖的范围内移动。早期无线网络通常使用红外线（infrared light）。不过红外线本身有其限制，容易受到墙壁、隔间以及其他办公室设备阻隔。无线波可以穿透大部分办公室设备，提供较广的服务范围。因此，市面上绝大多数的 802.11 产品均采用无线波做为物理层。

1.1.1 无线频谱：关键资源

无线设备被限定在某个特定频段（frequency band）上操作。每个频段都有相应的频宽（bandwidth），亦即该频段可供使用的频率空间总和。频宽是评价链路（link）数据传输能力的基准。种种数学、信息以及信号处理理论均可证明，较大的频宽可以传输更多的信息。举例而

言，类比式移动电话频道需使用 20 kHz 的频宽。电视信号比较复杂，因此需要用到 6 MHz 的频宽。

无线频谱（radio spectrum）的使用受到主管当局严格控管，主要是通过核发使用执照的方式。在美国，主管机关是联邦通信委员会（Federal Communications Commission，简称 FCC）。美洲有些国家直接采用 FCC 法规。欧洲主管机关是 CEPT 旗下的欧洲无线通信局（European Radiocommunications Office，简称 FRO）。至于其他地区，则由国际电讯联盟（International Telecommunications Union，简称 ITU）把关。为了防止重复使用无线波，通常以频段（band）来配置频率（frequency）。所谓频段，其实就是分配给特定应用的频率范围。美国地区常用的频段列于表 1-1。

表 1-1：美国地区常用频段

频段	频率范围
UHF ISM	902–928 MHz
S-频段	2–4 GHz
S-频段，ISM	2.4–2.5 GHz
C-频段	4–8 GHz
C-频段卫星下行链路	3.7–4.2 GHz
C-频段，雷达（气象）	5.25–5.925 GHz
C-频段 ism	5.725–5.875 GHz
C-频段，卫星上行链路	5.925–6.425 GHz
X-频段	8–12 GHz
X-频段，雷达（警用 / 气象）	8.5 — 10.55 GHz
Ku-频段	12 — 18 GHz
Ku-频段，雷达（警用）	13.4–14 GHz 12 — 18 GHz 15.7 — 17.7 GHz

ism 频段

表 1-1 中，有三个标识为 ISM 的频段。所谓 ISM，分别代表工业(industrial)科学(scientific)与医疗(medical)。大致而言，ISM 频段是保留给产业、科学或者医疗设备使用的。波炉是大家熟悉的 ism 设备，使用的是 2.4-GHZ ISM 频段，因为该频率的电磁幅射特别有利于加热含水物质。

之所以特别提到 ism，是因为只要设备符合功率限制，这些频段不需要申请使用执照(license-free)802.11 和许多其他设备均使用 ism 频段。常见的无线电话(cordless phone)亦同样使用 ism 频段。802.11b 与 802.11g 设备使用 2.4 GHz ISM 频段，而 802.11a 设备使用 5 GHz 频段。

较常见的 802.11b/g 设备使用 ISM 的 S-频段。只要设备所使用的功率不高，ISM 频段、一般而言不须经过授权使用。毕竟，使用微波炉还得申请使用执照并没有太大的意义。同样地，无线网络的组建与使用也无须申请使用执照。

1.2 无线网络的特色

无线网络对固定式网络而言是绝佳的互补，而非取而代之的技术。就像移动电话与固网，无线局域网络提供用户移动性，和固定式网络形成互补。数据的访问还是得通过服务器与数据中心的设备，不过服务器位于何处并不重要。由于服务器通常无须移动，因此可以使用固定缆线彼此相连。另一方面，无线网络在设计上必须能够覆盖较大的范围，以服务快速移动的用户。**802.11** 基站的覆盖范围不大，因此无法服务于快速移动交通工具上的用户。

1.2.1 没有实体界限

传统网络安全的主要重点，在于防护网络设备的实体安全。网络数据通常是流动于铜线或光纤等事先规划好的路径上。至于网络的基础建设，则是通过坚固的实体访问控制加以保护。设备通常被安全地锁在集线槽（wiring closet），使用者也不会有重新设置的机会。安全性基本上来自于物理层的防护（当然有其限度）。虽然还是有可能被窃听或转接，通过实体的访问控制，要想鬼鬼祟祟地访问网络就比较困难。

相较于一般网络，无线网络所使用的介质更为开放。定义上，无线网络所使用的介质不像实体线缆有明确定义的路径，而只是经过特殊编码与调制过的无线波链路。既然这些原本就是众所皆知的开放标准，任何对无线技术有所了解的人均可随意收送信号。只要手上拥有正确的网络卡，劫取数据本来就是轻而易举，何况这些网卡可以在任何消费性电子卖场，以不到 50 美元的价钱购得。仔细在网络上找找，说不定花不到一半的价钱。

此外，无线波通常会偏离原来的目的地。无线介质没有明显的实体界限，何况收送端还可以使用高增益天线来延长传输距离。配置无线网络时，各位必须仔细思考如何防范未经授权的使用（unauthorized use）、流量注入（traffic injection）以及流量分析（traffic analysis）。随著无线通信协议的成熟，验证无线用户身份与适当加密数据的工具目前已经随处可得。

1.2.2 动态实体介质

有线网络一经设立，就开始变得无趣。这意味着说，它是可预测的。一旦将网线拉至定位，它们就日复一日做同样的事，不会有所改变。只要网络是根据规格所记载的工程规则设计的，运作上就不会有什么问题。提升有线网络的容量也不是什么难事，只要将线槽中的交换器升级即可。

相对地，无线局域网络所使用的实体介质就比较动态。无线波遇到物体会反射，可以穿墙，而且通常有点难以预料。无线波可能遭遇到传播上的问题（比如多重路径干扰与死角），并因而断线。既然所使用的介质不可靠，无线网络就必须仔细验证所接收到的帧，以防止帧漏失。**802.11** 以正面回应（positive acknowledgment）来因应，牺牲一些流量以确保帧的传送。

无线电波链路存在着有线网络所没有的种种限制。由于无线频谱属于相对稀少的资源，因此必须谨慎管制。要使无线网络速度更快有两种方式。要不就是配置更多频谱，要不就是提升链路的编码能力，使它在单位时间内可以传输更多数据。额外配置频谱比较罕见，特别是对免照网络而言。**802.11** 网络将工作站之无线频道的频宽维持在予 30MHz 不变，它是以大幅改良的编码方式来提升速度。较快的编码方式可以提升速度，不过也有潜在的缺点。编码方式愈快，接收器就必须分辨愈细微的信号差异，因此需要愈高的讯噪比（signal-to-noise ratio）。数据率愈高，工作站就愈要尽可能靠近基站。表 1—2 显示了 802.11 各种物理层标准及其速度。

表 1-2: 802.11 各种物理层 (PHY) 标准之比较

IEEE 标准	速度	频段	附注
802.11	1 Mbps 2 Mbps	2.4 GHz	首份 PHY 标准 (1997)。同时支持跳频与直 线序列调制技术。
802.11a	最大可到 54 Mbps	5 GHz	第二份 PHY 标准 (1999)，产品迟至 2000 年末才推出。
802.11b	5.5 Mbps 11 Mbps	2.4 GHz	第三份 PHY 标准不过是第二波主流产品。 这是本书第一版时最常见的 802.11 设备， 也是本书第二版完成后，设备数量最多的 老旧产品。
802.11 g	最大可到 54 Mbps	2.4 GHz	第四份 PHY 标准 120031。它在 2.4 GHz 频段上采用 802.11 a 的编码技术，以期达到更高的速度。它回溯相容于现有的 802.11b，网络，也是 2005 年笔记本电脑上最常见的技术。

无线本质上属于一种广播介质。一个工作站进行传送时，所有其他工作站只能聆听。基站的角色有点像是以往的分享式 Ethernet 集线器，每部基站的传输能力固定，且必须由所有连接用户共享。要增加网络的容量，网管人员必须添加基站，同时缩小现有基站的覆盖范围。

1.2.3 安全性

许多无线网络以无线波为介质，这种介质本质上就是开放而易遭拦截。如何适当地保护无线网络传输，向来就是通信协议设计者的主要考量。802.11 本身并未纳入安全性协议为因应无线介质本身的不可靠性以及提供移动性，需要使用一些协议，以提供帧送达确认、省电以及移动性的功能。安全性的优先性相当低，早期的规格书所提出的协议也被证明并不适用。

无线网络必须进行身份认证，以防未经授权的使用者访问。经过认证的连接作业也必须予以加密，以防止数据遭人拦截，或遭未经授权用户灌注数据。本书第一版问世后，用来提供强势加密和认证的技术已经浮现，它们是本书（第二版）改版的主要重点。

1.3 各种无线网络

无线网络是个热门产业。有些无线技术主要针对数据传输。蓝牙 (Bluetooth) 标准主要是在周边设备之间建立微型网络 (small network)，或某种形式的无线缆线 (wireless wire)。业界人士大多十分熟悉有关蓝牙的种种宣传 (hype)，虽然在实际产品问世前，蓝牙似乎就已经阵亡。第一版中，我曾提到很少见到有人使用蓝牙产品，不过近来蓝牙已经相当普遍。（我现在经常使用蓝牙耳机。）

第 2.5 代与第三代 (3G) 移动电话也是大家所熟悉的无线技术。它们承诺可以在每个细胞台 (cell) 提供百万位元 (megabit) 的数据传输率，以及提供获得 DSL 与 cablemodem 用户高度评价的随时连接 (always on) 服务。经过 3G 设备厂商这几年的宣传与推动，3G 商用服务终于开始进行。2.5 代服务，像是 GPRS，EDGE 以及 1xRTT。如今已经相当普遍，采用 UMTS 或

EV-DO 的第三代网络也很快即将问世。（为了通勤时能够在电车上连网，我最近才申请“吃到饱”的 GPRS 服务。）有些文章引用这些技术的峰值，以为它们可以达到每秒数百 kilobits 甚至 megabits，其实这些频宽必须由细胞台的所有用户共享。实际的下行速度大概相当于数据机拨接，无法与 802.11 的 hot spot 相提并论。

本书的主题是 802.11 网络。802.11 有不少称谓。有人称 802.11 为无线以太网络 (wireless Ethernet)，强调其与传统有线以太网络 (802.3) 之间的血缘关系。本书第一版问世之后，突然爆红的一种称谓是 Wi-Fi。Wi-Fi 是 Wi-Fi 联盟所推广的互通性认证计划。至于 Wi-Fi 联盟，乃是由 802.11 设备厂商所组成的主要商业组织。Wi-Fi 联盟的前身称为无线以太网络相容联盟 (Wireless Ethernet Compatibility Alliance，简称 WECA)，负责检测会员的产品是否与 802.11 标准相容。【注】执行相容性测试的尚有其他组织；例如 New Hampshire 大学的互通实验室 (InterOperability Lab，简称 IOL) 最近就推出了一个无线测试联盟。

1.2.4 标准的好处

有许多标准团体参与 802.11 相关标准的制定过程，因为 802.11 跨越许多网络的界限。大部分的任务还是落在 IEEE 身上，不过实际对无线局域网络标准做出重要贡献的，有以下几个主要单位。

首先是电子电机工程协会 (IEEE)。除了专业社团活动，IEEE 也制定电子设备的标准，包括各种不同的通信技术。IEEE 制定标准时是以专案进行，每个专案均以编号代表。到目前为止，最著名的 IEEE 专案就是负责开发局域网络标准的 802 专案。每个专案还会另外划分许多工作小组 (working group)，负责解决标准某个特定面向的问题。工作小组同样会被赋予一个编号，位于专案编号的点号之后。举例而言，使用最广泛的 IEEE LAN 技术 Ethernet，是由第三个 工作小组 802.3 负责标准化。WirelessLAN 则是由第十一个工作小组负责，因此称为 802.11。每个工作小组又会另外细分出许多任务小组 (task group)，以英文字母代表。 (有些英文字母不容易区别，例如小写的“1”，则不予使用) 在无线网络领域，第一个广为人知的是任务小组 B (TGb)，负责制定 802.11 b 规格书。表 1-3 列出了一些比较基本的 802.11 标准。

每隔一段时间，这些非独立的任务小组所做的增补，就会被汇整到主要的母规格书里。802.11 首度改版于 1997 年。针对文字所做的一些细微修正，盛行于 802.11-1999，过去一段很长时间，都是以它为依据。最近一次修订为 802.11-2003。。

表 1-3：各种 802.11 标准

IEEE 标准	附注
802.11	首份物理层标准 (1997)。制定 MAC 以及原本速度较慢的跳频与直接序列调制技术。
802.11 a	第二份物理层标准 (1999)。产品迟至 2000 年底才推出
802.11 b	第三份物理层标准 (1999) 不过是第二波主流产品。本书第一版撰写当时最常见的 802.11 设备
TGc	负责更正 802.11a 编码范例的任务小组。既然只是更正标准，因此并没有所谓的 802.11c
802.11 d	扩充跳频物理层的功能使之能在不同的管制区域 (regulatory domains) 中使用

TGe (未来的 802.11 e)	为 MAC 制定「服务品质：奔 quality-of-service，简称 Qos）延伸功能的任务小组。在标准制定之前 1 将会先制定出称为 Wi-Fi 多介质（Wi-Fi Multi-Media 简称 WMM）的过渡性版本
802.11 F	改善基站间漫游功能的「基站间协议」（Inter-access point protocol）
802.11 g	最近才标准化厂 2003 1，使用 ISM 频段的物理层
802.11 h	使 802.11 a 符合欧洲无线电管制的标准。其他管制当局亦采用此机制，做为不同用途
802.11i	改善链路层安全性
802.11j	修改 802.11a，使之符合日本无线电波管理的标准
TGk	改善工作站与网络间的通信，使无线电波稀有资源的管理与运用更有效率
TGm	负责将 802.11 a、802.11 b、802.11 d 以及 TGc 所做的变动整合至 802.11 主规格的任务小组。可将 m 想成 maintenance（维护）
TGn (未来 802.11n)	为了制定高速传输 (high-throughput) 标准所成立的任务小组。它的设计目标是超越 100Mbps 的传输量。未来的标准将称谓 802.11n
TGp (未来的 802.11 p)	负责让 802.11 适用于汽车环境的任务小组。一开始的用途，可能是做为电子收费的标准协议
TGr (未来的 802.11r)	加强漫游 (roaming) 的效果
TGs (未来的 802.11s)	负责让 802.11 适用于网状网络技术 (mesh networking technology) 的任务小组。
TGT (未来的 802.11 T)	负责篇 802.11 设计测试与量测标准的任务小组。因为这是一份独立的标准，因此以大写字母表示。
Tgu (未来的 802.11 u)	负责让 802.11 与其他不同网络技术互通的任务小组

当无线网络的认证显然已经出现基本的破绽时，IEEE 采用了一些最初开发自 IETF 的身份认证标准。Wireless LAN 的身份认证相当依赖由 IETF 所制定的协议。

Wi-Fi 联盟系由贸易协会、测试机构以及标准制定机构所组成。Wi-Fi 联盟主要扮演贸易协会的角色，服务所属会员，不过它亦以 Wi-Fi 认证而广为人知。接受 Wi-Fi 认证的产品，会与一些大厂的产品测试互通性，通过测试的产品，即有权使用 Wi-Fi 标章。

Wi-Fi 联盟在标准化方面所做的努力，主要是为了支持 IEEE。当无线网络的安全性开始受到质疑，Wi-Fi 联盟出面制定了一项过渡的安全性规格，称为 Wi-Fi 防护访问 (Wi-Fi Protected Access，简称 WPA)。WPA 基本上是 IEEE 安全性任务小组的阶段性工作成果。它比较像是一种行销性而非技术性的标准，毕竟技术面是由 IEEE 所主导开发。不过，在安全之无线局域网络解决方案的开发过程中，它扮演了一种推手的角色。

第2 章 802.11 网络概论

凡事若能综观形势 (lay of the land) 通常有助于细节的进一步探究。研究网络相关议题时，导论性的基本介绍通常在所难免，因为所使用的缩略术语 (acronyms) 可能不在少数。不幸的是，802.11 所使用的缩略术语数量创下历来新高，因此披荆见林的介绍也就更加重要了。要深入了解 802.11，各位必须习惯这些晦涩的专有名词，以及一系列由三个字母所组成的缩略术语。本章相当于连贯整本书的背胶。阅读本章，不仅能初步认识 802.11 与一些重要的概念、也可以了解通信协议背后的设计原理，以及它们如何提供类似 Ethernet 的使用经验。之后，各位大可根据本身的兴趣与需要，深入探究低价协议的细节，或者直接跳至实际网络部署的相关章节。

本导之所以重要，部分是因为在此所介绍的缩略术语散见全书各处。就 802.11 而言，本章还肩负其他更重要的任务。802.11 与 Ethernet 十分类似。熟悉 Ethernet 的来龙去脉虽然有助于理解 802.11，不过要了解 802.11 如何将传统 Ethernet 技术应用到无线领域，还需要具备一些其他的背景知识。为了弥补有线网络与 802.11 无线介质的差距，必须另外加入一些管理功能。802.11 的核心，本质上属于一种善意的谎言(a white lie)，这关系到介质访问控制 (media access control，简称 MAC) 的真实含义。每片无线网络界面卡均会被赋予一个 48 位元的 MAC 地址，看起来与 Ethernet 网络界面卡没有两样。事实上，指派给 802.11 网络卡的 MAC 地址来自同一个地址库(address pool)，因此就算与有线 Ethernet 工作站部署在同一网络，也必然具备独一无二的地址。

对外面的网络设备而言，这些 MAC 地址看起来是固定的，与其他 IEEE 802 网络没有什么差别。如同 Ethernet 地址，802.11 的 MAC 地址一样会出现在 ARP 列表中，使用相同的厂商首码 (vendor prefix)，两者根本无从区分。熟知内情的 802.11 网络设备（基站与其他 802.11 设备）所悉不只如此。802.11 与 Ethernet 设备之间存在许多差异，最明显的莫过于 802.11 设备具备移动性；它们可以轻易在不同网络区段间自由移动。802.11 设备对此了然于胸，因此能够根据移动式工作站所在位置传送帧 (frame)。

2.1 IEEE 802 网络技术规格

IEEE 802 家族是由一系列局域网络 (local area network，简称 LAN) 技术规格所组成，802.11 属于其中成员之一。从图 2-1 可看出 802 家族成员的关系，以及它们在 OSI 模型中的角色定位。

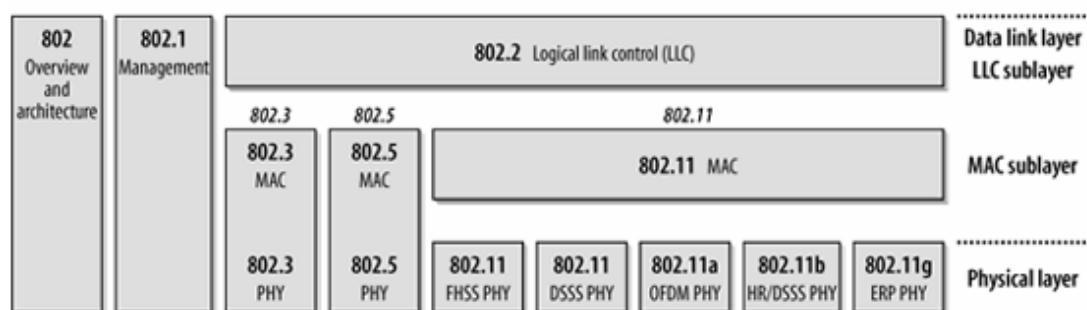


图 2-1：IEEE 802 家族，以及其与 OSI 模型的关系

IEEE 802 规格的重心放在 OSI 模型最底下的两层，因为它们同时涵盖了实体(physical，简称 PHY)与数据链路 (data link) 元件。只要是 802 网络，就必然会同时具备 MAC 与 PHY 两种元件。MAC 是一组用以决定如何访问介质与传送数据的规则，至于传送与接收的细节则交由 PHY 负责。

载波检测多重访问 / 碰撞检测 (Carrier Sense Multiple Access network with Collision Detection，简称 CSMA/CD) 规格，与 (通常误称的) Ethernet 有关，802.5 则是 Token Ring 规格。此外，802 协议堆叠还包括其他成员。802.2 所规范的链路层(link layer)，称为逻辑链路控制层(Logical Link Control，简称 LLC)，可供所有底层局域网络技术所使用。802 网络管理功能规范于 802.1。而 802.1 的范围涵盖桥接(802.1D)以及虚拟局域网络 (802.1Q)。

说穿了，802.11 只不过是另一种可以利用 802.2/LLC 封装(encapsulation)的链路层。802.11 基本规格涵盖了 802.11 MAC 以及两种物理层 (physical layer)：一是跳频展频 (frequency-hopping spread-spectrum，简称 FHSS) 物理层，另一是直接序列展频 (direct-sequence spread-spectrum，简称 DSSS) 物理层。后来改版时，802.11 陆续加入了其他不同的物理层 802.11b 规范了高速直接序列展频(HR/DSSS)物理层；802.11b 产品在 1999 年问世，是第一款于大众市场销售的物理层。802.11a 所规范的物理层，主要是以正交分频多工 (orthogonal frequency division multiplexing，简称 OFDM) 技术为基础；802.11a 的产品在本书第一版完成之际已经开始发行。802.11g 是目前最新开发的物理层。它采用 OFDM 以便提升连接速度，但同时也能够回溯相容于 802.11b。不过，回溯相容是需要付出代价的。如果 802.11h 与 802.11g 的使用者同时访问一部基站，将需要用到额外的机制，因此会拖累 802.11g 使用者的连接速度。

802.11 只不过是 802.2 的另一种链路层：这种说法，其实抹煞了本书其他部分所交待的细节。然而，这些细节正是 802.11 所以动人之处。802.11 允许在行动间访问网络；为此，802.11 在 MAC 中加入了许多额外的功能。因此，相较于 IEEE 802 MAC 规格，802.11 MAC 有若巴洛克风格一般繁复。

以无线波(radio wave)为物理层，还需要比较复杂的 PHY。802.11 将 PHY 进一步划分为两个组成元件：一是物理层收敛程序 (Physical Layer ConvergenceProcedure，简称 PLCP)，负责将 MAC 帧对映到传输介质；另一是实际搭配介质 Physical Medium Dependent，简称 PMD)，负责传送这些帧。PLCP 横跨 MAC 与物理层，如图 2-2 所示。在 802.11 网络中，PLCP 将帧传至空中之前，会在其中加入一些栏位。

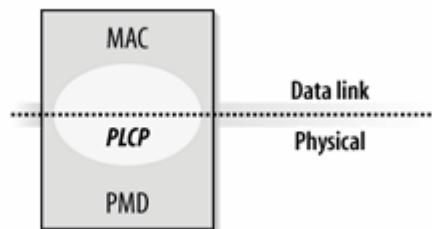


图 2-2 PHY 的组成元件

凡此种种，不免让人有「知也无涯，何为止境」之间。不过随着认识的深入，理解地就越深，任何技术皆然。虽然 802.11 协议中可供调校之处 (knobs and dials) 颇多，但为了降低复杂度，实际产品大多刻意加以隐藏。只有在网络拥塞时，例如如流量异常或用户过多，这些功能

的用处才会被突显出来。时至今日，网络在上述两方面几乎已经濒临极限。各位或许想要跳过与协议有关的章节，直接了解如何规划与配置 802.11 网络，对此我不能苛责。读完本章之后，各位可以直接跳至第 17-23 章，等到需要（或想要）进一步了解这些协议的内部运作时，再回过头来阅读这些章节也成。

2.2 802.11 相关术语及其设计

802.11 网络包含四种主要实体元件，如图 2-3 所示

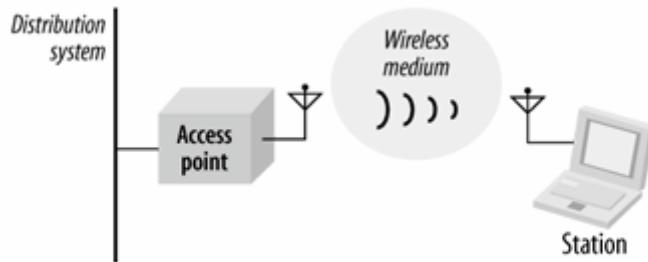


图 2-3：802.11 LAN 的组成元件

这些组成元件包括：

- 工作站（Station）

配置网络的目的，是为了在工作站间传送数据。所谓的工作站（station），是指配备无线网络界面的计算设备。通常，工作站是以电池供电的膝上型（laptop）或手持式（handheld）电脑。然而，工作站不见得就是携带型（portable）计算设备。有时候，使用无线网络之目的是为了省去拉线的麻烦，桌上型(desktop)电脑一样可以使用无线局域网络。较宽广的开放空间也可以受惠于无线网络，例如生产线可以使用无线局域网络来连接彼此。在消费性电子产品方面，802.11 也快速成为一种连接标准。Apple 的 Airport Express 可以让电脑通过 802.11 与音响连接。TiVo 数位录影机也可以连接到无线网络。有些消费性电子产品厂商已经加入 802.11 工作小组，显然是为了借助 802.11 的高速传输能力来传送多介质数据。

- 基站（Access Point）

802.11 网络所使用的帧必须经过转换，方能被传递至其他不同类型的网络。具备无线至有线（wireless-to-wired）桥接功能的设备称为基站（access point，简称 AP）；基站的功能不仅于此，但桥接（bridging）最为重要。起初，厂商倾向于将基站的所有功能置于单一设备，不过一些较新的产品则是将 802.11 协议切割为两部分：“精简型”基站（thin AP）与基站控制器（AP controller）。

- 无线介质（Wireless medium）

802.11 标准以无线介质（Wireless medium）在工作站之间传递帧。其所定义的物理层不只一种；这种架构允许多种物理层同时支持 802.11 MAC - 802.11 最初标准化了两种射频（radio frequency，简称 RF）物理层以及一种红外线（infrared）物理层，然而事后证明 RF 物理层较受欢迎。此外，一些其他的射频物理层也已经标准化了。

- 传输系统（Distribution system）

当几部基站串连以覆盖较大区域时，彼此之间必须相互通信，才能够掌握移动式工作站的行踪。而传输系统(**distribution system**)属于 802.11 的逻辑元件，负责将帧(**frame**)转送至目的地。802.11 并未规范传输系统的技术细节。大多数商用产品，是以桥接引擎(**bridging engine**)和传输系统介质(**distribution system medium**)共同组成传输系统。传输系统是基站间转送帧的骨干网络，通常就称为骨干网络(**backbone network**)。所有在商业上获得成功的产品，几乎都是以 Ethernet 为骨干网络。

2.2.1 网络类型

基本服务组合(**basic service set**简称 BSS)是 802.11 网络的基本元件(**buildingblock**)，由一组彼此通信的工作站所构成。工作站之间的通信，在某个模糊地带进行，称为基本服务区域(**basic service area**)，此区域受限于所使用无线介质的传播特性。【注】只要位于基本服务区域，工作站就可以跟同一个 BSS 的其他成员通信。BSS 分为两种，如图 2-4 所示。

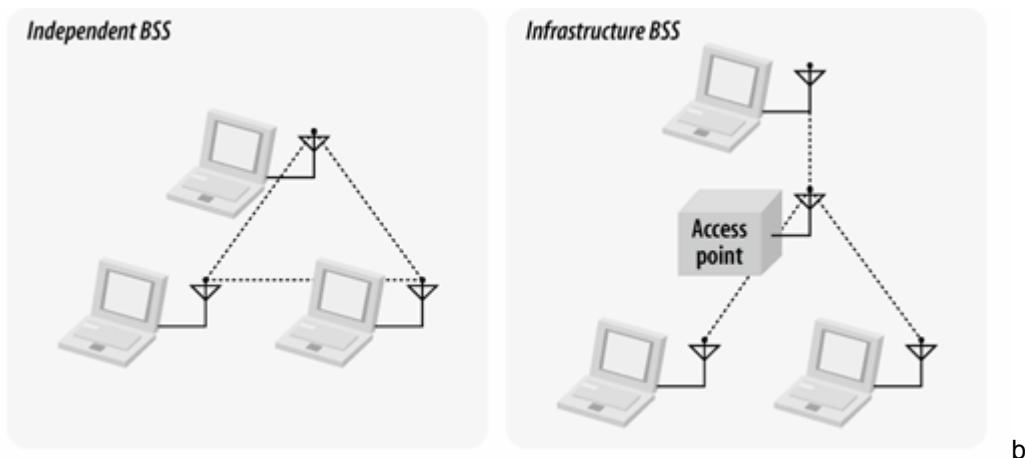


图 2-4：独立型与基础型基本服务组合

2.2.1.1 独立型网络

图左为独立式基本服务组合(**independent BSS**，简称 IBSS)。在 IBSS 中，工作站彼此可以直接通信，两者间的距离必须在可以直接通信的范围内。最低限度的 802.11 网络，是由两部工作站所组成的 IBSS。通常，IBSS 是由少数几部工作站针对特定目的而组成的临时性网络。常见的情况是在会议室中支持个别会议之用。会议一开始，与会人员彼此会形成一个 IBSS 以便传递数据。当会议结束，IBSS 随即瓦解。【注】正因为持续时间不长、规模甚小且目的特殊，IBSS 有时被称为特设 BSS(**ad hoc BSS**)或特设网络(**ad hoc network**)。

2.2.1.2 基础型网络

图右为基础型基本服务组合(为了避免混淆，不可将 **infrastructure BSS** 简称为 IBSS)。判断是否为基础型网络，只要检视是否有基站参与其中。基站负责基础型网络所有的传输，包括同一服务区域中所有行动节点之间的通信。位于基础型基本服务组合的移动式工作站，如有必要跟其他移动式工作站通信，必须经过两个步骤。首先，由始对话的工作站将帧传递给基站。其次，由基站将此帧转送至目的地。既然所有通信都必须通过基站，基础型网络所对应的基本服务

区域就相当于基站的传送范围。虽然这种做法比直接传送耗费较多的资源，不过它有两个主要的优点：

- 基础型基本服务组合被界定在基站的传输范围。所有移动式工作站都必须位于基站的传输范围之内，不过移动式工作站之间的距离则无限制。允许移动式工作站彼此直接通信虽然可以省下一些频宽，不过代价是相对提高了物理层的复杂度，因为每部工作站都必须维护与服务区域中其他工作站的邻接关系。
- 基站在基础型网络里的作用是协助工作站节省电力。基站可以记住有哪些工作站处于省电状态，并且为之暂存帧。以电池供电的工作站可以关闭无线收发器，只有在传输或接收来自基站的暂存帧时才会加以开启。

在基础型网络里，工作站必须先与基站建立连接，才能取得网络服务。所谓连接（association），是指移动式工作站加入某个 802.11 网络的程序。逻辑上，这相当于 Ethernet 插上网线。整个程序并不对称，因为开始连接秩序的必然是移动式工作站。IBSS 在 LAN 方面也有类似的用法。备注：，基站只是基于连接要求的内容，判定是否准许该工作站访问网络。对移动式工作站而言，连接必须独一无二：每部移动式工作站同时只能与一部基站连接。【注】802.11 标准并未限制基站可服务的移动式工作站数量。当然，实作上还是必须以限制。不过实际上，无线网络的传输量相对较低，很少需要予以限制。

2.2.1.3 延伸式服务区域

BSS 的服务范围，可以涵盖整个小型办公室或家庭，不过无法服务较广的区域。802.11 允许我们将几个 BSS 串联为延伸式服务组合（extended service ESS），藉此延伸无线网络的覆盖区域。所谓 ESS 就是利用骨干网络将几个在一起。所有位于同一个 ESS 的基站将会使用相同的服务组合识别码（set identifier，简称 SSID），通常就是使用者所谓的网络「名称」。

802.11 并未规范非得使用何种骨干技术，只要求骨干必须提供一组特定的服务功能。图 2-5 所示的 ESS 系四个 BSS 的联集（只要所有基站均隶属同一个 ESS）。实际部署时，BSS 之间的重叠程度可能较图 2-5 为高。在实际生活中，总是希望延伸式服务区域是连续的；不可能要求使用者从 BSS1 走到 BSS2 时还要绕道 BSS3。

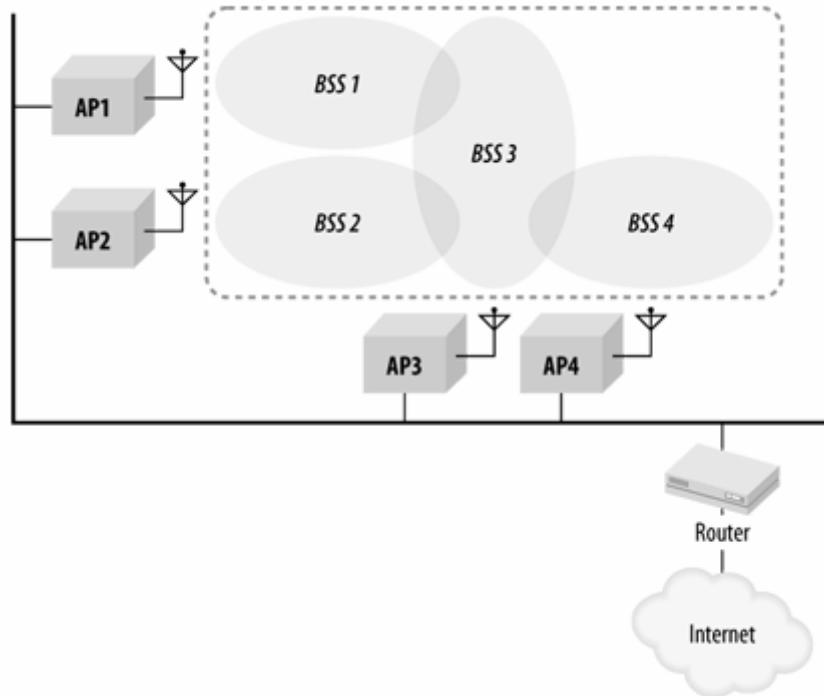


图 2-5: 延伸式服务组合

隶属同一个 ESS 的工作站可以相互通信，即使这些工作站位于不同的基本服务区域，或是在这些基本服务区域中移动。为了让 ESS 里的工作站能够彼此通信，无线介质必须能够在第二层（链路层）进行连接。由于基站扮演著桥接器的角色，因此 ESS 里的工作站若要彼此通信，则骨干网络也必须能够在第二层进行连接。第一代基站必须通过集线器（hub）或者虚拟局域网络（virtual LAN）才能与第二层直接连接；不过，较新型的产品当中通常已经内建某种穿隧（tunneling）技术，可以模拟出第二层的连接环境。

延伸式服务区域是 802.11 网络所支持的最高价抽象概念。ESS 所属的基站会彼此合作，让外界能够使用单一 MAC 地址与 ESS 里其他工作站通信，不论其置身何处。在图 2-5 中，路由器可使用单一 MAC 地址传递帧给移动式工作站；由该工作站所连接的基站负责传送帧。路由器无须在意移动式工作站位于何处，而是靠基站传送帧。

2.2.1.4 多组 BSS 所构成的环境：虚拟 AP

早期的 802.11 芯片只能够建立单组 BSS（基本服务组合）。而单一 AP（基站）只能为使用者提供一个“无线网络”，而且该网络上所有用户的权限，纵非完全相同，也相去不远。在早期使用者寥寥可数的环境里，单一逻辑网络可能就已足够。不过当无线网络逐渐普遍，单一网络开始不敷使用。

举例而言，各机关单位总会有固定的访客，其中许多人手上就有 802.11 设备，而且需要（或者强烈想要）与网际网络连接。这些访客并非可信的用户，通常为了满足这些访客的上网需求，将会在相同的实体设施上另辟两个延伸服务组合。目前的 802.11 芯片组已经可以使用相同的物理层来建立多组网络。以当前的芯片组而言，每部基站的硬件设备可以建立两组 BSS，其中一组可供客户访问，称之为 guest 另外一组则供内部使用，称之为 internal。在此 AP 当中，各 SSID

被分别连接至不同的 **VLAN guest** 网络会被连接至为不知名或不可信用户所准备的 **VLAN**，而且被置于防火墙外。

此电波领域内，无线设备将会发现两组不同的网络，然后依其所需连接至适合的网络。(当然，要访问内部网络必须经过身份认证，以防止未经授权人士使用) 连接至 **guest** 网络的使用者会被引导至访客所使用的 **VLAN**，而连接至 **internal** 网络的用户则必须经过身份认证，然后被引导至内部网络。

上述所虚构的例子，说明了虚拟基站的扩展情况。每个 **BSS** 就像一部自给自足的 **AP**，拥有自己的 **ESSID**、**MAC** 地址。身份认证配置以及加密设置。虚拟基站也可以用来建立具不同安全等级 (**security level**) 的平行网络(**parallel network**)，对此第 22 章将会有深入的讨论。目前，802.11 芯片组最多可以建立 32 甚至 64 组 **BSS**，对各种情况而言，应该都已经够用了。

2.2.1.5 固安网络 (Robust Security Network)

早期无线局域网络内建的安全机制已被证明是不堪一击。2004 年 6 月成为标准的 802.11i，规范了一组经改良的安全机制，目的是提供坚固而安全的网络连接。一旦使用 802.11i 所定义的、经改良的身份认证与私密性协议，就可称之为固安网络连接(**robust security network associations**，简称 **RSNAs**)。产品可以通过硬件・软件或软硬件兼具的方式支持 802.11i，这取决于该设备所使用的架构。不支持此协议的硬件被归类为 **pre-RSN**。有些 **pre-RSN** 设备可以通过升级的方式来支持 802.11i，不过大多数较旧的设备是无法升级的。

2.2.2 再论传输系统

既然读者已经了解如何建构延伸式服务组合，我打算回过头来重新检视传输系统这个概念。802.11 是以能提供无线工作站哪些服务来描述传输系统。虽然本章稍后即将深入探讨这些服务，不过仍值得我们从较高层次的角度来检视其运作方式。传输系统可藉由串连基站来提供移动性 (**mobility**)。当帧传送至传输系统，随即会被送至正确的基站，而后由基站转送至目的地。

传输系统必须负责追踪工作站实际的位置，以及帧的传送。若要传送帧给某部移动式工作站，传输系统必须负责将之传递给服务该移动式工作站的基站。以图 2-5 的路由器为例。该路由器仅会以某移动式工作站的 **MAC** 为目的地址・如图 2-5 所示，**ESS** 的传输系统必须负责将帧传递给正确的基站・显然，有部分传递机制属于 **Ethernet** 所构成的骨干网络，不过该骨干网络并不代表整个传输系统，因为它无法在多部基站间做出选择。以 802.11 的语言来讲，**Ethernet** 所构成的骨干网络是个「传输系统介质」，但并非传输系统的全部。

要找出传输系统的其他成份，我们必须检视基站本身。目前市面上大部分基站都是扮演桥接器的角色。这些基站至少具备一个无线网络界面，以及一个 **Ethernet** 界面。**Ethernet** 界面可用来连接既有的网络，而无线界面则成为该网络的延伸。这两种网络介质之间的帧转送，是由「桥接引擎」加以控制。

基站、骨干网络以及传输系统之间的关系如图 2-G 所示。基站具备两种不同的界面，分别连接至同一个桥接引擎。图中的箭头代表往返桥接引擎的可能路径。帧将会通过桥接器送至无线网络；任何由桥接器的无线点所送出的帧都会传给所有已连接的工作站。每部已连接的工作站均可传递帧至基站。最后，桥接器的骨干点可以直接与骨干网络互动。在图 2-6 中，传输系统是由桥接引擎及有线骨干网络所组成。

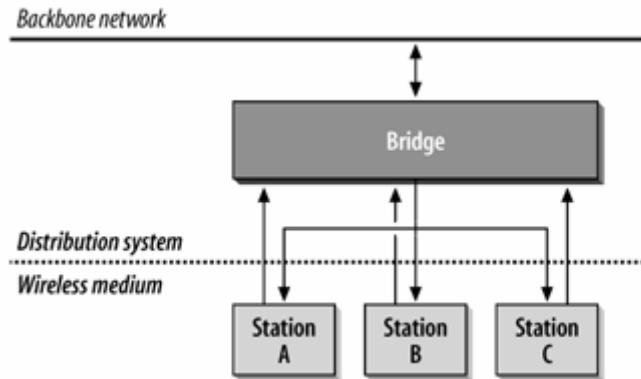


图 2-6：在一般 802.11 基站中常见的传输系统

在基础型网络里，移动式工作站所送出的每个帧都必须用到传输系统。这并不难理解。毕竟，每部工作站都必须连接至传输系统。无线工作站在基础型网络里必须依赖传输系统才能彼此通信，因为它们无法直接连系。工作站 A 要传送帧给工作站 B 的惟一方式，是通过基站里桥接引擎的转达（relay）。不过桥接器本身属于传输系统的组成元件。虽然传输系统所使用的是哪些组成元件似乎纯粹是技术上的考量，但实际上 802.11 MAC 里某些功能与传输系统有十分密切的关系。

2.2.2.1 基站间的通信是传输系统的一部分

传输系统包含了管理连接的方式。一部无线工作站在同一时间只能与一部基站连接。如果某工作站已经与某基站连接，位于同一个 ESS 的其他基站必须能够得知此工作站。如图 2-5 所示，AP4 必须得知所有与 AP1 连接的工作站。如果一部与 AP4 连接的无线工作站送出帧给一部与 API 连接的工作站，AP4 的桥接引擎必须通过 Ethernet 所构成的骨干网络将此帧送给 API，如此 AP1 才能够将之传递至最终目的地。要实作整个传输系统，基站必须通知其他工作站所连接的基站。当然，市面上有许多基站会在骨干介质中采用基站间协议（inter-access point protocol，简称 IAPP）。有些厂商自行开发专属协议，以便在基站间传递连接数据。目前所制定的 IAPP 标准称为 802.11E，不过还没听说有哪些产品已经实际采用。

2.2.2.2 无线桥接器与传输系统

到目前为止，我都假定传输系统介质就是既有的固定式网络。虽然情况通常如此，但 802.11 规格有明确提到，无线介质本身也可以做为传输系统。此种无线传输系统（wireless distribution system，简称 WDS）的配置通常称为「无线桥接器」（wireless bridge）配置，因为它允许网络工程师在链路层连接两个局域网络。无线桥接器可用来快速连接不同的网段，十分适合访问供应商（access provider）使用。市面上大部分的 802.11 基站均支持无线桥接功能，不过有些较旧的机型可能必须更新软件。

2.2.3 网络界限

由于无线介质的性质使然，802.11 网络的界限（boundary）可说是相当模糊。事实上，某种程度的模糊是必要的。和移动电话网络一样，允许基本服务区域彼此重叠，不仅可让工作站转换基本服务区的成功机率提高，也可以提供最高层次的网络覆盖率。图 2-7 右边的基本服务区域彼此重叠地十分明显。这意味着，当工作站从 BSS2 移动至 BSS1 时不致失去信号；这也同时

意味，就算 AP3（或者 AP4）失灵，也不致瘫痪整个网络。另一方面，如果 AP2 故障，则整个网络就会被分割为两个彼此隔开的区域，位于 BSS1 的工作站只要离开 BSS1 所涵盖的范围而进入 BSS3 或 BSS4，就会失去与 BSS1 的连接。如何填补这些「空隙」(coverage holes) 以避免网络瘫痪，乃是网络设计阶段必须注意的事项；有些新产品提供动态电波调整功能，可以在实际运作时自动填补基站间的空隙。

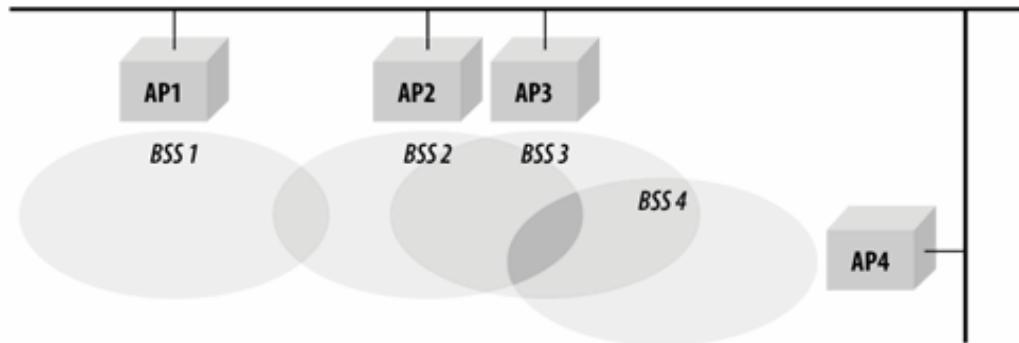


图 2-7：ESS 中彼此重叠的 BSS

不同类型的 802.11 网络彼此亦可重叠。在基站所涵盖的基本服务区域中，亦可以另辟独立型 BSS。图 2-8 显示了此二者在空间上的重叠。一部基站位于图 2-8 的上方，其基本服务区域以阴影表示。两部工作站以中控模式运作，通过基站彼此通讯。三部工作站设置为独立型 BSS，彼此间可以直接通信。虽然这五部工作站被指派至两个不同的 BSS，它们所使用的还是相同的无线介质。工作站只有通过 802.11MAC 所规范的规则才能够访问介质；这些规则在设计上就已考虑到，如何能够让多个 802.11 网络并存于相同的空间中。这两个 BSS 必须分享单一无线频道的频宽，因此共存的 BSS 之间必然会有效能上的消长。

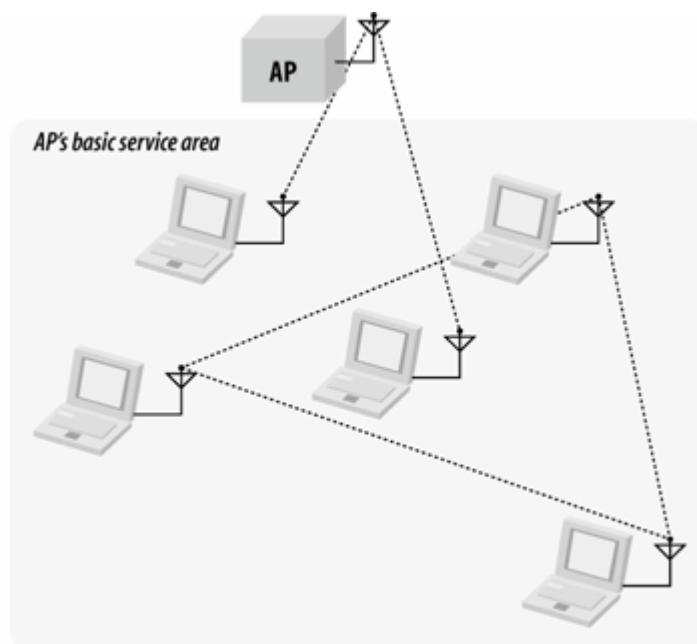


图 2-8：不同类型的无线网络彼此重叠

2.3 802.11 网络的运作方式

802.11 在设计之初就是做为较上层协议的另一个链路层。熟悉 Ethernet 的网管人员应该马上就可适应 802.11。其与 Ethernet 源远流长，有时甚至被称为「无线 Ethernet」802.11 里同样可以找到 Ethernet 的核心成份。它同样是以长度 48 个位元的 IEEE802 MAC 地址来区别工作站。概念上，帧的传递是根据 MAC 地址。虽然 802.11 为了克服无线频道可靠度不够的缺点，【注】纳入了某些机制以确保基本的可靠度，但帧传递实际上是不可靠的。

从使用者的观点来看，802.11 跟 Ethernet 没有两样。不过，网管人员须对 802.11 有更进一步的了解。既要提供 MAC 层次的移动性，又要依循之前 802 标准所规划的道路，所以必须加入一些额外的服务与较复杂的帧格式。

2.3.1 网络服务

定义网络技术的方式之一，就是看它能够提供哪些服务，不论设备制造商如何实现这些服务。802.11 总共可以提供九种服务。其中三种用来传送数据，其馀六种均属管理作业，目的是让网络能够追踪行动节点以及传递帧。以下说明这九种服务，并摘录于表 2-1：

- 传输 (Distribution)

只要基础型网络里的移动式工作站传送任何数据，就会使用这项服务。一旦基站接收到帧，就会使用传输服务将帧送至目的地。任何行经基站的通信都会通过传输服务，包括连接至同一部基站的两部移动式工作站彼此通信时。

- 整合 (Integration)

整合服务系由传输系统提供；它让传输系统得以连接至非 IEEE 802.11 网络。整合功能将因所使用的传输系统而异，因此除了必须提供的服务，802.11 并未加以规范。

- 连接 (Association)

之所以能够将帧传递给移动式工作站，是因为移动式工作站会向基站登记，或与基站建立连接。连接之后，传输系统即可根据这些登录信息判定哪部移动式工作站该使用哪部基站。未连接的工作站不算「在网络上」，好比拔掉 Ethernet 网线的工作站。802.11 虽有规范使用这些连接数据的传输系统必须提供哪些功能，但对于如何实作这些功能并未强制规定。如果使用固安网络协议(robust security network protocol)，连接之后才能进行身份认证。在身份认证完成之前，基站会将丢弃来自工作站的所有数据。

- 重新连接 (Reassociation)

当移动式工作站在同一个延伸服务区域里的基本服务区域之间移动时，它必须随时评估信号的强度，并在必要时切换所连接的基站。重新连接是由移动式工作站所发起，当信号强度显示最好切换连接对象时便会如此做。基站不可能直接开始重新连接服务。（有些 AP 会刻意将工作站剔除，强迫它们进行重新连接程序；未来，随著更优秀网管标准的发展，重新连接会更密切依赖底层的基础建设。）一旦完成重新连接，传输系统会更新工作站的位置纪录，以反映出可通过哪个基站连络上工作站。和连接服务一样，在固安网络中，除非已经成功完成身份认证，否则来自工作站的数据均会被弃置。

- 解除连接 (Disassociation)

要结束现有连接，工作站可以利用解除连接服务。当工作站启动解除连接服务时，储存于传输系统的连接数据会随即被移除。一旦解除连接，工作站即不再附接在网络上。在工作站的关机程序中，解除连接是个礼貌性的动作。不过 MAC 在设计时已经考虑到工作站未正式解除连接的情况。

- 身份认证 (Authentication)

实体安全防护在有线局域网络安全解决方案中是不可或缺的一部分。网络的接续点 (attachment point) 受到限制，通常只有位于外围访问控制设备 (perimeter access control device) 之后的办公区才能加以访问，网络设备可以通过加锁的集线槽 (locked wiring closet) 加以保护，而办公室与隔间的网络插座只在必要时才连接至网络。无线网络无法提供相同层级的实体保护，因此必须依赖额外的身份认证程序，以保证访问网络的使用者已获得授权。身份认证是连接的必要前提，惟有经过身份辨识的使用者才准许使用网络。工作站与无线网络连接的过程中，可能必须经过多次身份认证。连接之前，工作站会先以本身的 MAC 地址来跟基站进行基本的身份辨识。此时的身份认证，通常称为 802.11 身份认证，有别于后续所进行、牢靠而经过加密的使用者身份认证。

- 解除认证 (Deauthentication)

解除认证用来终结一段认证关系。因为获准使用网络之前必须经过身份认证，解除认证的副作用就是终止目前的连接。在固安网络中，解除认证也会清除密钥信息。

- 机密性 (Confidentiality)

在有线局域网络中，坚固的实体控制可以防止刺探数据的绝大部分攻击。攻击者必须能够实际访问网络介质，才有可能窥视往来的内容。在有线网络中，网线与其他计算资源一样，也要受到实体保护。在设计上，实际访问无线网络，相对而言较为容易，只要使用正确的天线与调制方式就办得到。802.11 初次改版时，机密性 (confidentiality) 服务原本称为私密性 (privacy) 服务，而且是由目前已经毫无可信度的有线信号 (Wired Equivalent Privacy，简称 WEP) 协议所提供。除了新的加密机制，802.11 提供了两种 WEP 无法解决的关键服务来加强机密性服务，亦即基于使用者的身份认证 (user-based authentication) 以及密钥管理服务。

- MSDU 传递

一个网络如果无法传递数据给接收端，大概也没有什么用。工作站所提供的 MSDU (全名为 MAC Service Data Unit) 递送服务，负责将数据传送给实际的接收端。

传输功率控制 (Transmit Power Control，简称 TPC)

TPC 是在 802.11h 所定义的新服务。欧洲标准要求作业于 5 GHz 频段的工作站必须能够控制电波的传输功率，避免干扰其他同样使用 5 GHz 频段的用户。传输功率控制也有助于避免干扰其他无线局域网络。传输距离是传输功率的函数；工作站的传输功率愈高，传输距离就愈远，也就愈容易干扰邻近的网络。如果可以 将传输功率调到“刚刚好” (just right)，就可以避免干扰到邻近的工作站。

- 动态频率选择 (Dynamic Frequency Selection，简称 DFS)

某些雷达系统的作业范围位于 5 GHz 频段。因此，有些管制当局强制要求无线局域网络必须能够检测雷达系统，以及选择未被雷达系统所使用的频率。有些管制当局甚至要求无线局域网

络必须能够均衡使用（uniform use）5 GHz 频段，因此网络必须具备重新配置频道（re-map channels）的能力。

表 2-1：网络服务

服务	此服务属于工作站或传输系统？	说明
传输	传输系统	系统递送帧时，可使用此服务来决定目的地位于基础网络上的地址
整合	传输系统	用来将帧递送至无线网络以外的 IEEE 802 LAN
连接	传输系统	用来建立 AP（做为闸道器之用）与特定移动式工作站间的连接。
重新连接	传输系统	用来变更 AP（做为闸道器之用）与特定移动式工作站间的连接。
解除连接	传输系统	用来从网络移除无线工作站。
身份认证	工作站	建立连接之前，用来进行身份认证（利用 MAC 地址。）
解除认证	工作站	用来终结一段认证关系，其副作用是终止目前的连线。
加密性	工作站	用来防止窃听。
MSDU 递送	工作站	用来递送数据至接收端
传输功率控制（TPC）	工作站/频谱管理	降低工作站传输功率以减少干扰。
动态频率选择（DFS）	工作站/频谱管理	避免在 5 GHz 频段干扰雷达作业。

2.3.1.1 工作站服务

每部与 802.11 相容的工作站都必须提供工作站服务，任何宣称符合 802.11 规格的产品也都必须具备这项功能。移动式工作站与基站的无线界面都会提供工作站服务。工作站提供「帧传递 J（frame delivery）服务让信息得以传递，为了支持此项任务，工作站还必须以「身份认证」服务来建立连接。工作站或许也希望利用「机密性」功能，在信息行经容易遭受侵害的无线链路时，加以保护。

2.3.1.2 传输系统服务

传输系统服务负责将基站连接至传输系统。基站的主要功能是将有线网络所提供的服务延伸至无线网络；方法是对无线端提供「传输」与「整合」服务。传输系统另外一项重要的功能是

管理移动式工作站的连接。为了维护连接数据以及工作站的位置信息，传输系统还提供了「连接」、「重新连接」以及「解除连接」等服务。

2.3.1.3 机密性与访问控制机密性与访问控制

服务彼此密不可分。除了传输数据的私密性 (secrecy)，「机密性」服务也提供帧内容的完整性 (integrity)。私密性与完整性均仰赖共享式加密密钥 (shared cryptographic keying)，因此「机密性」服务必然仰赖其他服务提供身份认证与密钥管理。

身份认证与密钥管理 (Authentication and key management，简称 AKM)

如果无法防范未经授权的使用者，密码学上的完整性就没有什么价值可言。「机密性」服务仰赖身份认证与密钥管理的配套来确定使用者的身份和建立加密密钥。身份认证也可以通过其他外部协议完成，比如 802.1X 或者预设共享密钥 (pre-shared key)。

加密演算法 (Cryptographic algorithm)

帧的保护可以通过传统的 WEP 演算法，使用长度 40 或 104 个位元的密钥；或者 TKIP (临时密钥完整性协议)；或者 CCMP (计数器模式 CBC-MAC 协议)。我们将于第 5 与第 7 章详细探讨这些演算法。

- 来源真实性 (Origin authenticity)

TKIP 与 CCMP 让接收端得以验证传送者的 MAC 地址，以避免伪装攻击 (spoofing attack)。来源真实性只能保护单点传播数据 (unicast data)。

- 重演攻击检测 (Replay detection)

TKIP 与 CCMP 会使用序号计数器 (sequence counter) 来验证所接收的帧，以防范重演攻击 (replay attack)。“太旧”的帧就会被丢弃。

- 其他外部协议与系统

「机密性」服务极其仰赖其他外部协议。密钥管理系由 802.1X 所提供，而 802.1X 则会搭配 EAP 来传递认证数据。802.11 并未限制使用何种协议，不过最普遍的做法是以 EAP 提供身份认证，并以 RADIUS 介接认证服务器。

2.3.1.4 频谱管理服务

频谱管理服务是工作站服务的一部分。这项服务让无线网络得以回应环境，以及动态变更电波的设置值。为了符合电波管制的要求，802.1h 定义了两种服务。

第一种服务称为传输功率控制 (TPC)，用来动态调整工作站的传输功率。基站可以利用 TPC 作业，通知工作站最大容许功率，如果工作站所使用的功率不符合电波管制的要求，也可以拒绝连接。工作站可以利用 TPC 调整功率，使传输距离“刚刚好”可以连上基站。数位移动电话系统 (Digital cellular system) 也有类似功能，被设计来延长手机电池的使用时间。【注 1】较低的传输功率也有助于延长电池的使用时间，但是效果取决于手机能够降低多少传输功率。

第二种服务称为动态选频 (DFS)，开发的目的主要是为了避免干扰 5GHz 频段的雷达系统。虽然原本是为了符合欧洲管制当局的要求，不过背后所依循的原则，还是跟其他管制当局的要求没有两样。DFS 是美国于 2004 年决定在 5 GHz 频段开放更多频谱的重要关键。[57127] 基站可藉助 DFS 所提供的功能，让某个频道噤声 (quiet the channel) 后不受干扰地搜

索雷达。不过，DFS 最重要的功能在于，可以为基站动态配置频道。切换频道之前，工作站均会接到通知。

2.4 移动性的支持

移动性是采用 802.11 网络的主要动机之所在行进间用手机通话。在工作站移动时传送数据，就好比在移动时用手机通话。

802.11 所提供的移动性，存在于链路层的基本服务组合之间。链路层以上究竟发生什么事，它并无法理解。在部署规划 802.11 时，网络工程师必须特别小心，好让网络层的工作站 IP 地址，可以在物理层进行无间隙转换(**seamless transition**)时被保存下来。就 802.11 而言，基站之间可能出现三种转换：

- 不转换

如果工作站并未离开目前基站的服务范围，就无须转换。这种状态之所以发生，可能是因为工作站并未移动，或是仍在目前所连接之基站的基本服务区域中移动。【注】（当然，这种说法可能会引起争论，不过规格就是如此定义的。）

- BSS 转换

工作站持续监控来自所有基站的信号强度与信号品质。在延伸服务区域中，802.11 提供了 MAC 层次的移动性。附接至「传输系统」的工作站，可以将所送出的帧，定位到某部移动式工作站的 MAC 地址，并让基站充当该移动式工作站的最终转运点（**final hop**）。传输系统上的工作站无须知道某部移动式工作站的确切位置，只要该移动式工作站位于同样的服务区域。

图 2-9 展示了 BSS 转换的过程。本图有三部基站被赋予相同的 ESS。一开始，以 $t=1$ 表示，配备 802.11 无线网卡的膝上型电脑，位于 AP1 的基本服务区，并与 AP1 处于连接的状态。当该膝上型电脑离开 AP1 的基本服务区，并于 $t=2$ 进入 AP2 的范围时，就发生所谓的 BSS 转换。该移动式工作站会使用「重新连接」服务与 AP2 连接，而 AP2 则会开始送出帧给该移动工作站。

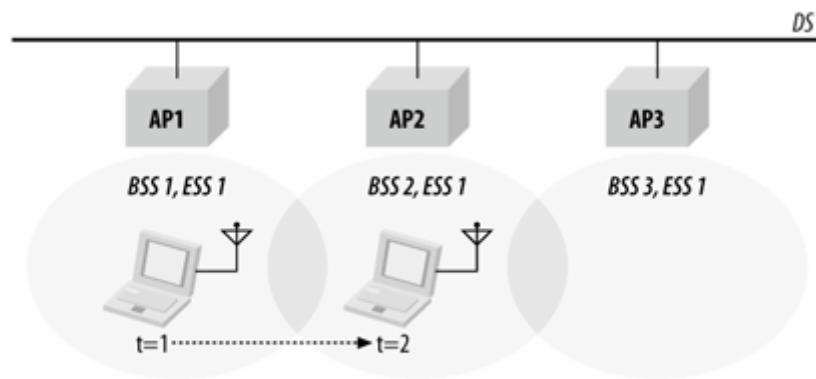


图 2-9：BSS 转换

BSS 转换必须通过基站彼此合作。在上述状况下，AP2 必须通知 AP1 该移动式工作站现在已经与 AP2 连接。802.11 并未规范 BSS 转换过程中基站之间如何通信的细节。

值得注意的是，即使这两部基站隶属于同一个延伸组合，它们之间却可能是由一部路由器所连接，亦即受限于第三层协议。在这种情况下，仅使用 802.11 协议并无法保证可以达到无间隙漫游。

- ESS 转换

所谓 ESS 转换，是指从某个 ESS 移动至另一个 ESS。802.11 并未支持此类转换，不过允许工作站在离开第一个 ESS 的范围之后，与第二个 ESS 里的基站连接。可以确定的是，较上层的连接必然会因此而断线。比较正确的说法是，802.11 所支持的 ESS 转换，仅能够让工作站比较容易与新的「延伸服务区域」之基站连接。要能够维持较高层次的连接，必须得到协议族的支持。以 TCP/IP 写例，要支持无间隙的 ESS 转换，必须使用 Mobile IP。图 2-10 展示了 ESS 的转换过程。图 2-10 中，四个基本服务区组成了两个延伸服务区。目前尚未支持，从左边的 ESS 无间隙地转换至右边的 ESS。之所以支持 ESS 转换，是因为移动式工作站会立即与第二个 ESS 里的基站连接。只要离开第一个 ESS 的范围，任何作用中的网络连接都会随之断线。

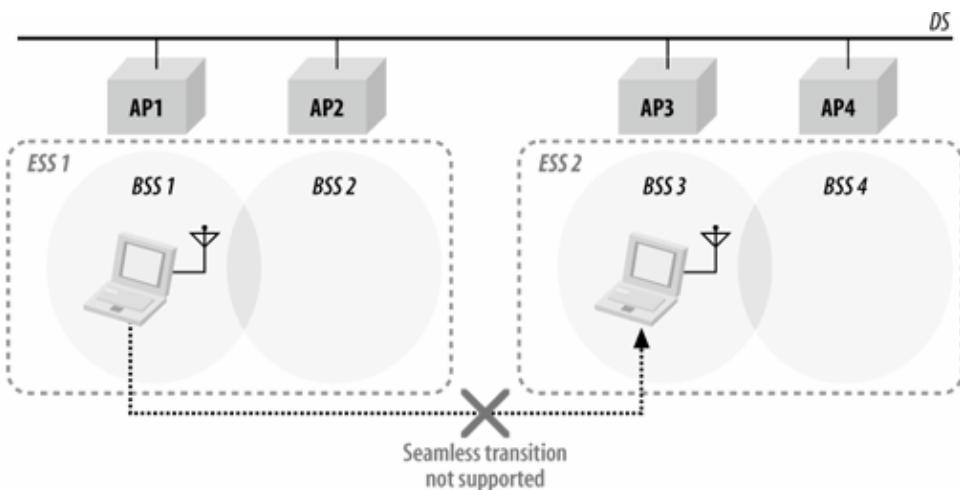


图 2-10: ESS 转换

2.4.1 移动性网络设计

在设计上，绝大多数的网络都采用一组基站访问一组资源。同一组所管理的所有基站均会被赋予相同的 SSID，使用无线网络时，工作站就以此 SSID 进行连接。

工作站四处移动时，除了持续监视网络连接状态，也会在不同基站间进行切换。802.11 可以确保工作站经过不同基站时维持连接。只要这些基站属于同一个 SSID，但是网络设计人员在组建网络时必须将移动性纳入考虑。较小的网络通常是由单一的 VLAN、单一的网络所构成，这时就不必担心移动性问题。跨网段的较大网络则必须使用额外技术，能够支持移动性。有些产品仅支持单一的 VLAN，工作站不论身在何处均连接到相同的 VLAN。较新的产品甚至会根据身份认证数据为工作站动态指定 VLAN。因此不论置身何处，只要使用者一连接，就会被引到相同的 VLAN；这类交换式网络只会要求无线局域网络设备必须正确标识帧。有些产品支持 Mobile IP 标准，或者自创不同的 VPN 技术。这些机动策略的取舍，将于第 21 章深入讨论。

事实上，ESS 转换相当罕见，通常只发生在使用者离开某个区域，进入到另一个区域时(例如，某个 hot spot 的公司网络)。此时，两个网络可能使用不同的 IP 地址，两者之间也不存在信赖关系，不足以在不中断网络连接的情况下无间隙地移动工作站。

2.4.1.1 专属的移动系统

为了提供移动性，有些厂商会设计自家专属的协议与程序，特别是那些专门设计用来建设大规模网络的设备厂商。在我着手修订本书时，802.11 尚存一个大问题是，必须在同一个 IP 子



华为 3COM

网来提供漫游。如此一来，无线局域网络的部署除了必须在架设上实际的规划，在骨干网络之上也免不了要有所调整。有些厂商为了尽快填补这些空隙，让工作站能够在各种形态的网络之间来去自如，以及在基站之间快速漫游，早已著手开发自家的专属协议。这些解决方案的基本观念，将会在本书后半段与部署相关的章节中加以探讨。

第3 章 802.11 MAC

本章节开始深入探讨 802.11 标准，第二章从宏观的角度概述了 802.11，同时还涉及到标准本身所具备的一些属性。过了这个分水岭，本书将分为理论与实务两个部分。往后连接几章的内容大多与 802.11 规格，以及其所采用的相关标准有关。然而，不是非要巨细无遗的了解相关协议，才能够构建有线或者无线网络。不过，有时还是要对底层得运作机制有比较深入的了解。

- 虽然 802.11 已广泛且迅速地被人们所接受，但是安全问题仍然占据了新闻地头条。人们无疑会征求网络管理人员对安全议题地见解，特别是在无线网络相关地提议中。要了解并参与这些讨论，请参阅第五和第六章。使用静态密钥 WEP 加密机制已遭到破解。使用 802.1X 与动态 WEP 密钥的方案显然更安全，如果辅以第七章所探讨地 802.11i 相关协议，那就更加牢靠了。
- 无线网络的故障排除和有线网络类似，不过比较复杂。封包监测软件 (packet sniffer) 向来是排除故障的有利工具。不过，各位必须知道每种封包的含义，才能正确了解网络的行径，完全发挥封包检测软件的功效。
- 校准无线网络，离不开规格所列举的种种参数，以及底层无线电技术。要了解你的网络以及可能优化到什么程度，需要对这些参数有所认识，以及这些无线电波在所使用的环境中的如何传播。
- 有些设备驱动程序会开放一些可供调整的简单设置。大部分的驱动程序都会为这些参数提供校准过的预设值，少数驱动程序允许使用者自由设定。如果用户拥有开放的源码就可以随意试验。
- 无线网络的技术日新月异，随时都会推出新的协议。深入了解这些基本的协议，有助于了解这些新功能的运作方式，以及它们在你现有网络中的含义。

和生命中其他的事物一样，了解越多，掌握的越好。以太网通常不会带来什么麻烦，不过许多的网管人员都有经验，一旦遇上问题，没有什么比得上充分了解网络运作的经验与知识。本书第一版本问世时，802.11 网络有点免费奉送的味道。因为 802.11 够酷，就算一时断线，使用者也通常不以为然；无线连网是一种特权而不是一种权利。另一方面，无线网络与使用者的数量相对而言并不多，因此很少遇到负载的问题。服务半打使用者的以太网大概不成什么问题；一旦在网络中加入了几步高用量的服务器、几百个用户，以及连接彼此的桥接器与路由器，问题就会开始出现。无线网络亦然，几部接入点服务和半打使用者也不成问题。当使用者倍速增长，而且有几个无线网络彼此重叠时，每个无线网络各自拥有一组接入点，负载问题必然也会出现。

这就是为什么要阅读本章的理由。接下来让我们仔细瞧瞧。802.11 规格的关键在于 MAC(介质访问控制层)。MAC 位于各种物理层之上，控制数据的传输。不同的物理层可以提供不同的传输速度，不过物理层之间必须彼此互通。

802.11 并未大幅偏离之前的 IEEE 802 标准。802.11 成功地将以太网形式的网络应用到无线链路之上。和以太网一样，802.11 采用载波侦听 (carrier sense multiple access, 简称 CSMA) 机制，来控制传输媒质的访问。不过，碰撞会浪费宝贵的传输资源，因此 802.11 转而使用冲突避免 (CSMA/CA) 机制，而非使用以太网所采用的碰撞检测 (CSMA/CD) 机制。和以太网一样，802.11 采用的是不具中枢控制功能的分散式访问机制，因此每部 802.11 工作站访问媒质的方式都一样。802.11 与以太网之间的差异，在于所使用的底层介质不同。

本章首先会描述当初设计 MAC 时所必须克服的难题，以便洞悉 MAC 设计人员的动机，随后说明这些介质的访问规则，以及基本的帧结构。如果各位只想了解 802.11 网络上的基本帧序列，可直接跳至本章结尾。要进一步了解 MAC，可以参阅 802.11 标准第九章所列的正式规格；详细的 MAC 结构图列于附录 C。

3.1 MAC 所面临的挑战

无线网络环境与传统有线网络环境的差异性，为网络协议设计人员带来了种种挑战。本章节将检视 802.11 设计人员所面临的一些难题。

3.1.1 射频链路质量

在有线的以太网中，假定对方必然会收到所传送的帧是合理的。无线链路则不然，特别是使用无须授权的 ISM 频段时。窄频（narrowband）传输将会受到噪声与干扰的影响，而不必使用执照的装置（unlicensed device）也必须假定干扰的存在，并且提供克服干扰的办法。为了克服微波炉及其他射频干扰源所导致的辐射问题，802.11 设计人员曾经考虑过几种解决方案。除了噪声问题，多径衰落（multipath fading）所造成的传输死角（dead spot），也可能导致帧的无法传递。

和其他链路层协议不同，802.11 采用正面回应机制。所有传送出去的帧都必须得到回应，如图 3-1 所示，只要任何一个环节失败，该帧即视为已经丢掉。

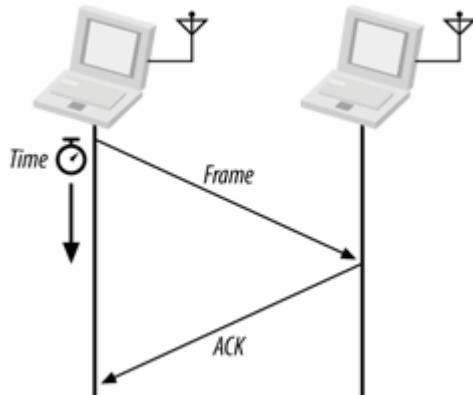


图 3-1：数据传输的正面应答

图 3-1 所列出的步骤称为基本操作，指不可分割的单一处理单元。虽然整个处理过程包含好几个步骤，但还是会被视为单一不可分割的过程。基本处理单元可说是“非成即败”。若不完成所有步骤，整个过程就被视为失败。数据帧的传送者必须收到应答，否则该帧即被视为已经丢失。从传送者的角度而言，究竟是一开始的数据帧，或者是回应信息在传输过程中丢失并不重要。因为无论如何，数据帧还得必须重传。

将帧传送视为基本操作让事情变得比较复杂，因为如此一来，整个连接就分为两个步骤，分别由两部不同的工作站所控制。在整个交易过程中，这两部工作站必须彼此合作，依次取得网络媒质的控制权，以便进行传输处理。802.11 允许工作站在基本处理期间锁定媒质，避免基本操作被其他试图竞争传输媒质的工作站打断。

无线电波的链路品质也会影响网络连接的速度。信号质量较好就可以用较高的速度来传送数据。信号质量通常随着距离的拉长而有所衰减，亦即 802.11 工作站的数据传输速度，取决于他和接入点之间的相对位置。工作站必须具备某种机制，可以判定何时因环境的不变化来调节速率的变换。支持多种速率的规则，将于本章稍后探讨。

3.1.2 隐藏节点的问题

在以太网络中，工作站是通过接收传输信号来行使 CSMA/CD 载波侦听的功能。空中的介质线路中包含了信息，而且会传输到各网络节点。无线网络的界线比较模糊，有时候并不是每个节点都可以跟其他节点直接通信，如图 3-2 所示。

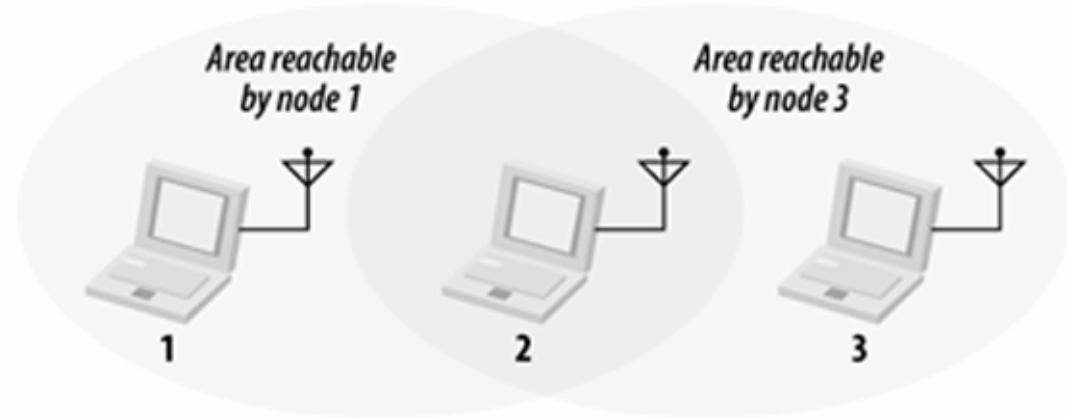


图 3-2: 节点 1 与节点 3 互为隐藏节点

如图 3-2 所示，节点 2 可以之间跟节点 1 和节点 3 通信，不过某些因素导致节点 1 与节点 3 无法直接通信。（这与障碍物的关系并不大：节点 1 与 3 之间可能只是因为距离远，无法收到对方的无线电波。）从节点 1 的角度来看，节点 3 属于隐藏节点。如果使用简单的 transmit-and-pray 协议，节点 1 与节点 3 有可能在同一时间传送数据，这会造成节点 2 无法辨识任何信息。此外，节点 1 与节点 3 将无从得知错误发生，因为只有节点 2 才知道有冲突发生。

在无线网络中，由隐藏节点所导致的碰撞问题相当难以监听，因为无线收发器通常是半双工工作模式，即无法同时收发数据。为了防止碰撞发生，802.11 允许工作站使用请求发送（RTS）和允许发送（CTS）帧来清空传送区域。由于 RTS 与 CTS 帧会延长数据交易过程，因此 RTS 帧、CTS 帧、数据帧以及最后的应答帧均被视为相同基本连接的一部分。图 3-3 说明了整个过程。

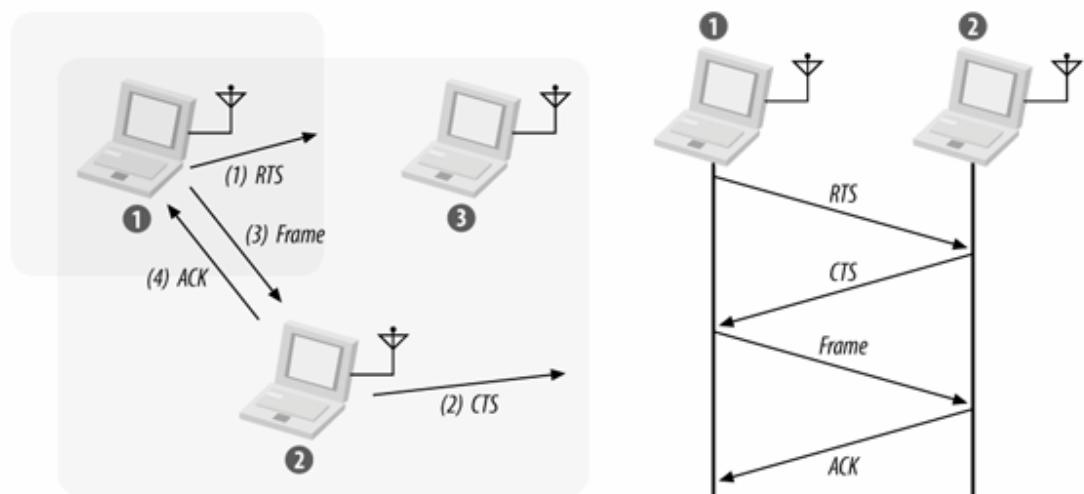


图 3-3:RTS/CTS

如图 3-3 所示，节点 1 有个数据帧待传送，因此送出一个 **RTS** 帧启动整个过程。**RTS** 帧本身带有两个目的：预约无线链路的使用权，并要求接收到这一消息的其他的工作站停止发言。一旦收到 **RTS** 帧，接收端会以 **CTS** 帧应答。和 **RTS** 帧一样，**CTS** 帧也会令附近的工作站保持沉默。等到 **RTS/CTS** 完成交换过程，节点 1 即可传送上面要传送的帧，无须担心来自其他隐藏节点的干扰。

整个 **RTS/CTS** 传输过程会用到好几个帧，实际开始传输数据之前的延迟也会消耗相当的频宽。因此，它通常只用在高用量的环境，以及传输竞争比较显著的场合。对低用量的环境而言，通常无此必要。

随着 802.11 逐渐成熟，隐藏节点已经不成问题。在小型、不太活跃、只有几部客户端共享一个接入点的网络里，很少会有同时进行传输的情况，何况还有不少闲置频宽可供重传之用。在比较大型的网络环境里，由于覆盖范围内有相当密集的接入点，客户端就有可能坐落在好几台接入点的共同覆盖范围内。（事实上，有些工作站的传输距离对大多数网络而言可能太远，这一点将留在本书网络规划章节中再进行讨论。）

如果 802.11 网卡的驱动程序支持，使用者可以通过调整 **RTS** 门限值来控制 **RTS/CTS** 程序。只要大于此门限值，就会进行 **RTS/CTS** 交换程序。小于此门限值则会直接传送数据帧。

3.2 MAC 访问控制与时钟

无线介质的访问，是由协调功能所管控。以太网之类的 **CSMA/CA** 访问，是由分布式协调功能（**distributed coordination function**，简称 **DCF**）所管控。如果需要用到免竞争服务，则可通过架构于 **DCF** 之上的点协调功能（**point coordination function**，简称 **PCF**）来管控。在各取所需的 **DCF** 与精确管控的 **PCF** 之间，也可以选择使用介于两种极端之间，采取中庸之道的混和式协调功能（**hybrid coordination function**，简称 **HCF**）。免竞争服务只提供于基础网络（**infrastructure network**），不过只要工作站支持 **HCF**，就可以在网络中提供服务质量（**quality of service**，简称 **QoS**）。协调功能的细节，请见图 3-4 以及下列说明：

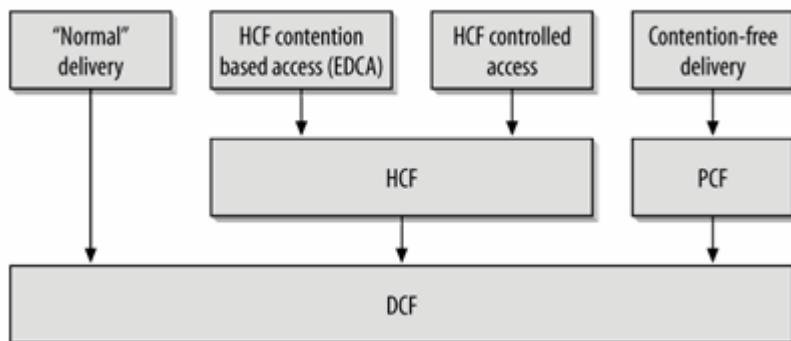


图 3-4:MAC 协调功能

- **DCF(分散式协调功能)**

DCF 是标准 CSMA/CA 访问机制的基础。和以太网一样，在传送数据之前，它会先检查无线链路是否处于空闲状态。为了避免冲突发生，当某个传送者占据频道时，工作站会随机为每个帧选定一段延后时间。在某些情况之下，DCF 可利用 CTS/RTS 空闲技术，进一步减少碰撞发生的可能性。

- **PCF(点协调功能)**

点协调功能提供的是免竞争服务。称为点协调者的特殊工作站可以确保不必通过竞争即可使用介质。点协调者位于基站，因此只有基础型网络才会使用 PCF。为了赋予比标准竞争式还高的优先性，PCF 允许工作站经过一段较短的时间即可传送帧。PCF 在实际上并不常见，第 9 章对此有详细说明。

- **HCF(混和式协调功能)**

有些应用需要尽力传达更高一级的服务质量，却又不需要用到 PCF 那么严格的管控。HCF 允许工作站维护多组服务队列，针对需要更高服务品质的应用，则提拔更多的介质访问机会。HCF 尚未完全标准化，不过最终将成为 802.11 标准的一部分。

将服务质量纳入 802.11 MAC 中是项艰巨的任务。由于涉及到帧封装、队列管理以及信号产生种种复杂层面，撰写本书时，标准委员会还在为服务质量规格书争论不休，因此相关议题将留待未来改版时再予以讨论。

3.2.1 载波监听功能与网络分配矢量

载波监听主要用来判定介质是否处于可用状态。802.11 具备两种载波监听功能：物理载波监听与虚拟载波监听。只要其中有一个监听功能显示介质处于忙碌状态，MAC 就会将此报告给高层的协议。

物理载波监听功能是由物理层所提供，取决于所使用的介质与调制方式。要为射频介质打造物理载波硬体相当不易（更确切的说法是十分昂贵），原因是除非采用昂贵的电子零件，否则收发器将无法同时进行收发的动作。此外，由于隐藏结点随处可见，物理载波监听并无法提供所有必要的信息。

虚拟载波监听是由网络分配矢量（Network Allocation Vector，简称 NAV）所提供。802.11 的帧通常会包含一个 duration 位，用来预定一段介质使用时间。NAV 本身就是一个计时器，用

来指定预计要占用介质多少时间，以微秒为单位。工作站会将 **NAV** 设定为预计使用介质的时间，这包括完成整个处理必须用到的所有帧。其他工作站会由 **NAV** 值倒数至零。只要 **NAV** 的值不为零，代表介质处于忙的状态，此即虚拟载波监听功能。当 **NAV** 为零时，虚拟载波监听功能会显示介质处于闲置状态。

利用 **NAV** 可保证工作站的基本操作不被中断。例如，图 3-3 所示的 **RTS/CTS** 程序即属一种基本操作。图 3-5 说明了 **NAV** 如何保障整个程序不受干扰。（这是本书图解所使用的标准格式，用以说明多部工作站之间的互动，每部工作站各自有相应的计时器。）工作站对介质的访问操作可用加上阴影的条状图来表示，每个条状图均会标上帧类型。没有任何操作之处会标上帧间隔。此图底部，**NAV** 线上的条状图代表 **NAV** 计时器。**NAV** 是由 **RTS** 与 **CTS** 帧之标头来载送的；此处之所以特别画出一条 **NAV** 线，是为了显示 **NAV** 与空中实际传输状况的关系。只要在 **NAV** 线上出现 **NAV** 条状图，工作站就必须暂缓访问介质，因为虚拟载波监听机制将会指出，介质正处于忙碌状态。

为了确保整个过程不受中断，节点 1 会在 **RTS** 帧中设定 **NAV**，防止传送 **RTS** 时其他工作站将对介质进行访问。所有收到 **RTS** 帧的工作站均会暂缓访问介质，直到 **NAV** 消失。

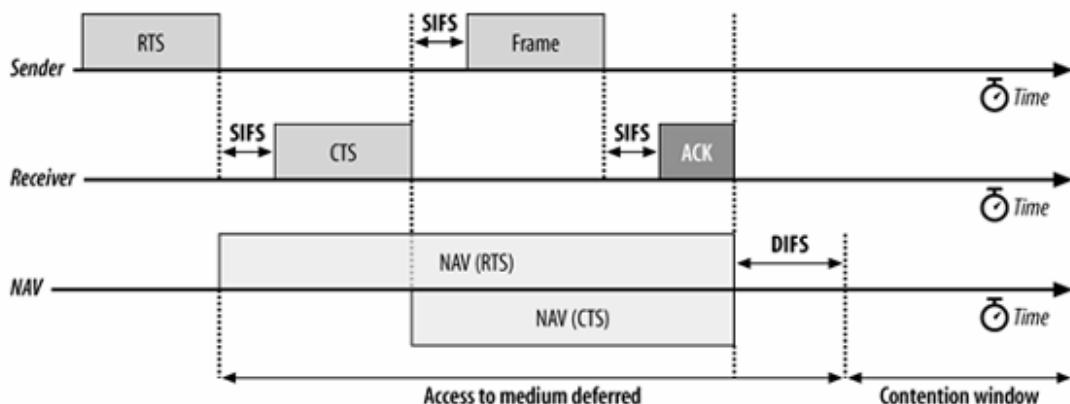


图 3-5：利用 **NAV** 进行虚拟载波监听

然而，不见得网络上每一部工作站均会收到这些 **RTS** 帧。因此，接收端会以 **CTS** 帧加以应答，其中亦包含 **NAV**，不过为时较短。此 **NAV** 可防止其他工作站在传输过程中访问介质，直到传输过程结束。一旦完成整个程序，经过一段分布式帧间隔（distributed interframe space，简称 **DIFS**）时间之后，任何工作站均可对介质进行访问，此时便进入竞争期间，如图 3-5 右边所示。

在有多个网络交接的拥挤地区，**RTS/CTS** 交换程序也可以派上用场。位于相同物理频道的工作站均会收到 **NAV**，因而会适当地延迟对介质地访问，就算这些工作站分别配置于不同的网络之上。

3.2.2 帧间隔

和传统的以太网一样，帧间隔在协调介质的访问上扮演着重要的角色。**802.11** 会用到四种不同的帧间隔。其中三种用来判定介质的访问；他们之间的关系如图 3-6 所示。

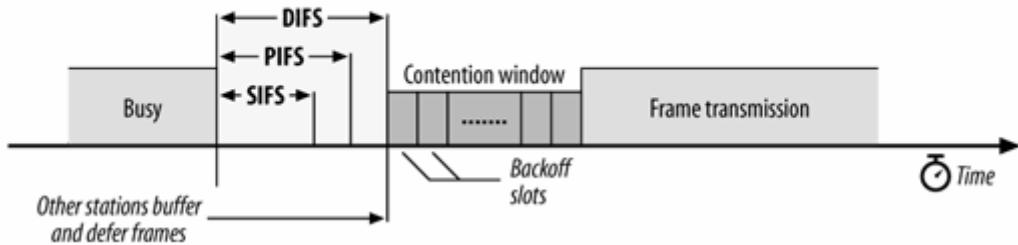
Figure 3-6. Interframe spacing relationships

图 3-6: 各种帧间隔的关系

现在我们已经知道，因为 802.11 MAC 内建避免碰撞的功能，所以工作站会延迟介质的访问，直到介质再度空闲。不同的帧间隔，会为不同类型的传输产生不同的优先次序。其后的决定逻辑十分简单：当介质闲置下来时，高优先级的数据所等待的时间较短。因此，如有任何高优先级的数据待传，在低优先级的帧试图访问介质之前，优先级较高的数据早就将介质据为己用了。为了维持不同数据传输率的互通性，帧间隔的时间值都是固定的，而与传输率无关。（这只是使用相同无线资源的不同物理层所导致的问题之一，因为不同的物理层会使用不同的调制技术。）不过，不同的物理层可以指定不同的帧间隔时间。

- 短帧间隔（Short interframe space，简称 SIFS）

SIFS 用于高优先级的传输场合，例如 RTS/CTS 以及正面应答帧。经过一段 SIFS（时间），即可进行高优先级的传输。一旦高优先级传输开始，介质即处于忙碌状态，因此相较于必须等待较长时间才能传输的帧，SIFS 消逝后即可进行传输的帧优先级较高。

- 点帧间隔（PCF interframe space，简称 PIFS）

PIFS 主要被 PCF 使用在免竞争过程，有时被误解为优先性帧间隔。在免竞争时期，有数据传输的工作站可以等待 PIFS 期间过后加以传送，其优先程度高于任何竞争式传输。

- 分布式帧间隔（DCF interframe space，简称 DIFS）

DIFS 是竞争式服务中最短的介质闲置时间。如果介质闲置时间长于 DIFS，工作站可以立即对介质进行访问。

- 扩展的帧间隔（Extended interframe space，简称 EIFS）

图 3-6 并没有表明 EIFS，因为 EIFS 并非固定的时间间隔。只有在帧传输出现错误时才会用到 EIFS。

3.2.3 帧间隔与优先程度

一开始，基本操作和一般传送并无不同：在可以开始传送之前，基本操作同样必须等待一段帧间隔（通常是 DIFS）时间。不过，其后的步骤即开始使用 SIFS，而非 DIFS。由于 SIFS 短于其他帧间隔，一项基本操作的第二（以及之后的）步骤会在其他类型的帧被传送之前将介质占为己用。利用 SIFS 与 NAV，工作站可以视需要占用介质一段时间。

如图 3-5 所示，SIFS 被应用在不同单位的基本操作之间。当传送取得介质访问权，接收端会在 SIFS 之后应答 CTS。任何试图在 RTS 结束之后访问介质的工作站，至少必须等候一段 DIFS 时间。若 DIFS 进行途中，SIFS 已先行结束，则会开始传送 CTS。

3.3 利用 DCF 进行竞争式访问

大部分的传输均采用 DCF (分布式协调功能)，DCF 提供了类似以太网的标准竞争式服务。DCF 允许多部独立的工作站彼此互动，无须通过中央管控，因此可以运用于 IBSS 网络或基础型网络。

试图传送任何数据之前，工作站必须检查介质是否处于闲置状态。若处于忙碌状态，工作站必须延迟访问，并利用指型退避 (orderly exponential backoff) 算法来避免碰撞发生。

我们可从 802.11 MAC 的规则中归纳出一组常使用的基本规则，其他额外规则的应用则视状况而定。在所有使用 DCF 的传输当中，将会运用到两项基本原则：

1. 如果介质闲置时间长于 DIFS，便可立即进行传输。载波监听同时可通过物理与虚拟(NAV)方式进行。

a. 如果之前的帧接收无误，介质至少必须空出一段 DIFS 时间。

b. 如果之前的传输出现错误，介质至少必须空出一段 EIFS 时间。

2. 如果介质处于忙碌状态，工作站必须等候至频道再度闲置。802.11 称之为访问延期。一旦访问延期，工作站会等候介质闲置一段 DIFS 时间，同时准备指型退避访问程序。

在特定状况下，会应用到一些额外的规则。其中有一些规则取决于“线上”的特殊状况，与之前传送的结果有关。

1. 错误复原 (error recovery) 属于传送端的责任。传送端预期每个帧均应收到应答信息，而且必须负责重传，直到传送成功为止。

a. 只有收到正面应答讯息，才表示传送成功。基本交换操作必须完成才算成功。如果某个预期的应答迟迟未到，传送端即会认定其已丢掉，必须加以重送。

b. 所有单点传播数据必须得到应答。（因此，即使无线电波链路本质上属于广播介质，相较于广播数据，单点传播数据基本上还是具备较高的服务质量。）

c. 只要传送失败，重传计数器就会累计，然后重新加以传送。传送失败有可能是因为访问介质失败，也可能是因为得不到应答。不论如何，重传时会等待一段较长时间（详见下一节）。

2. 涉及多个帧的传送，可以在传输过程的每个步骤更新 NAV。当所收到的介质预定时间比目前的 NAV 还长时，工作站即会更新 NAV。设定 NAV 的方式是以个别的帧为基准，对此下一章会有更详细的说明。

3. 以下的帧类型可在 SIFS 之后传输，因此优先程度较高：应答 (acknowledgment)、RTS/CTS 交换程序中的 CTS，以及分段程序中的帧片段。

a. 一旦传送出第一个帧，工作站就会取得频道的控制权。以后帧及其回应均可使用 SIFS 进行传送，以锁定频道不被其他工作站使用。

b. 传送中，后续帧会将 NAV 更新成该介质预计使用的时间。

4. 如果较高层的封包长度超过所设定的门限，必须使用扩展帧格式。

a. 长度超过 RTS 门限的封包，必须使用 RTS/CTS 交换程序。

b. 长度超过分段门限的封包，必须加以分段。

3.3.1 DCF 与错误复原

错误监听与更正是由起始基本帧交换过程的工作站来决定。一旦监听到错误，该工作站必须负责重传。错误监听必须由传送端负责。有时候传送端可根据应答的有无，推论帧是否已经漏失。只要帧被重传，重传器就会累计。

每个帧或帧片段就会分别对应到一个重传计数器。工作站本身具有两个重传计数器：短帧重传计数器与长帧重传计数器。长度小于 RTS 门槛值的帧视为短帧；长度超过该门槛值的数据则为长帧。根据帧的长度，将会分别对应到长短帧重传计数器。帧重传计数由 0 算起，只要帧传送失败即加以累计。

短帧重传计数器会在下列情况发生时归零：

- 之前传送的 RTS 得到 CTS 的应答时
- 之前传送的未分段帧得到 MAC 层的应答时
- 收到广播或组播的帧时

长帧重传计数器会在下列情况发生时归零：

- 之前传送的帧大于 RTS 门限值，并且得到 MAC 层的应答时
- 收到广播或组播的帧时

除了响应的重传计数器，MAC 会赋予每个帧片段最长的『存活期』。传送出第一个帧片段之后，存活计数器随即启动。一旦超过存活时间，该帧便会被丢弃，因此不会重传其余的帧片段。当然，上层协议也可能监听到数据漏失予以重传。不过当上层协议（如 TCP）重传数据，实际上传给 802.11MAC 的乃是新的帧，所有重传计数器也会归零重新计算。

3.3.2 使用重传计数器

和大部分其他的网络协议一样，802.11 是通过重传机制来提供可靠性。数据传送是通过基本次序，整个过程必须完成才算传送成功。当工作站传送帧时，必须得到接收端的应答，否则便认为传送失败。若传送失败则与该帧或帧片段响应的重传计数器累加。如果达到重传限制，该帧随即被丢弃，并将此状况告知上层协议。

之所以要有短帧和长帧，其中一个原因是为了让网络管理人员利用不同长度的帧来调整网络的稳定性。长帧需要较多的缓存空间，所以两种不同重传限制的一个潜在应用，就是放宽长帧的重传限制，以减少所需要的缓存空间。

3.3.3 DCF 与延迟

当帧传送完成并且经过一段 DIFS 时间，工作站便会试图传送之前拥塞的数据。DIFS 之后所紧接的一段时间，称为竞争期间或退避期间。此期间可进一步分割为时槽(slot)。时槽长度因介质而异。速度较高的物理层会使用较短的时槽。工作站会随机挑选某个时槽，等候该时槽到来以便访问介质。所有时槽的选择机会均等。当多部工作站同时试图传送数据，挑到第一个时槽（亦即取得最小随机号码）的工作站可以优先传送。根据 802.11 标准，所有这些时槽号码不应有所差异。唯一值得注意的例外，详见本章稍后有关『spectralink 语音优先性』的相关说明。

3.3.4 Spectralink 语音优先性

要在无线网络上支持语音应用必须面临的挑战之一，就是语音对于网络服务品质的敏感性，远高于数据方面的应用。假设某图形有 1500 个 bit 组的数据迟延了十分之一秒，那就令人无法忍受了。

要在 IP 网络上提供高质量的服务已经相当困难。换成无线局域网络，那更是难上加难。以无线局域网络设计语音网络时，工程师遇到的主要问题在于，无线局域网络对所有数据均一视同仁。假设有一个短语音帧和一个长数据帧，此时无线局域网络并不会特别偏爱哪个帧。Spectralink 是一家 802.11 手持电话制造商，该公司制定了一组特殊的协议延伸功能，称为 Spectralink 语音优先性（Spectralink Voice Priority，简称 SVP），该网络更适合用来传输语音。基站与手机当中均包含 SVP 元件，让语音享有高于数据的优先性，同时在基站中管理语音通话过程。不论是从基站下行或者自手机上行的语音通话，均由 SVP 协助管理。

要支持 SVP，基站必须以零延后机制传递语音帧。选取延后时槽的时候，支持 SVP 的基站并未依循 802.11 标准，而是选择编号为零的时槽。竞争无线介质的时候，取得零延后时槽的语音帧将具备实质的优先性，因为数据帧所取得的时槽编号必定大于零。严格来讲，采用零延后机制的工作站已经不算相容于 802.11，因为它以固定的方式强迫取得特定的延后时槽。（不过，为了维持高度负载时的网络稳定性，重传的语音帧必须依循延后规则。）通过零延后机制，支持 SVP 的基站可以确保语音帧能够优先访问介质。同时，这类基站也必须能够追踪语音帧，以及提供优先队列的处置。SVP 要求语音帧必须被置于传送队列的最前面。基站可以用不同的方式来提供传输队列，重要的是其所提供的功能，必须将语音帧移置传送队列的最前面。有些基站可能只有一个传送队列，此时语音帧会被置于队列的最前面。有些基站会使用多个传送队列，其中将会由一个队列专门用来传送高优先的语音帧。

如同以太网，每当传输失败时，便会从一个范围中挑选出退避时间。图 3.7 以 DSSS（直接序列展频）物理层为例，显示当传送次数增加，竞争期间随之增长的情况。不同物理层会使用不同大小的延后时间，不过原则是相同的。竞争期间的大小通常是 2 的指数倍数减 1（例如 31, 63, 127, 255）。每当重传计数器累增，竞争期间即以移至下一个 2 的指数倍数。竞争期间的大小受到物理层的限制。例如，DS 物理层限制竞争期间最多 1023 个传输时槽。

当竞争期间达到最大极限时，就会维持在该数字，直到被重新设定。允许使用较长的竞争期间，可以在多部工作站同时试图访问介质时，保持 MAC 验算法的稳定，就算负载极大。当帧传送成功，竞争期间即被重设为最小值，如果到达重传计数器上限，该帧则随即被丢弃。

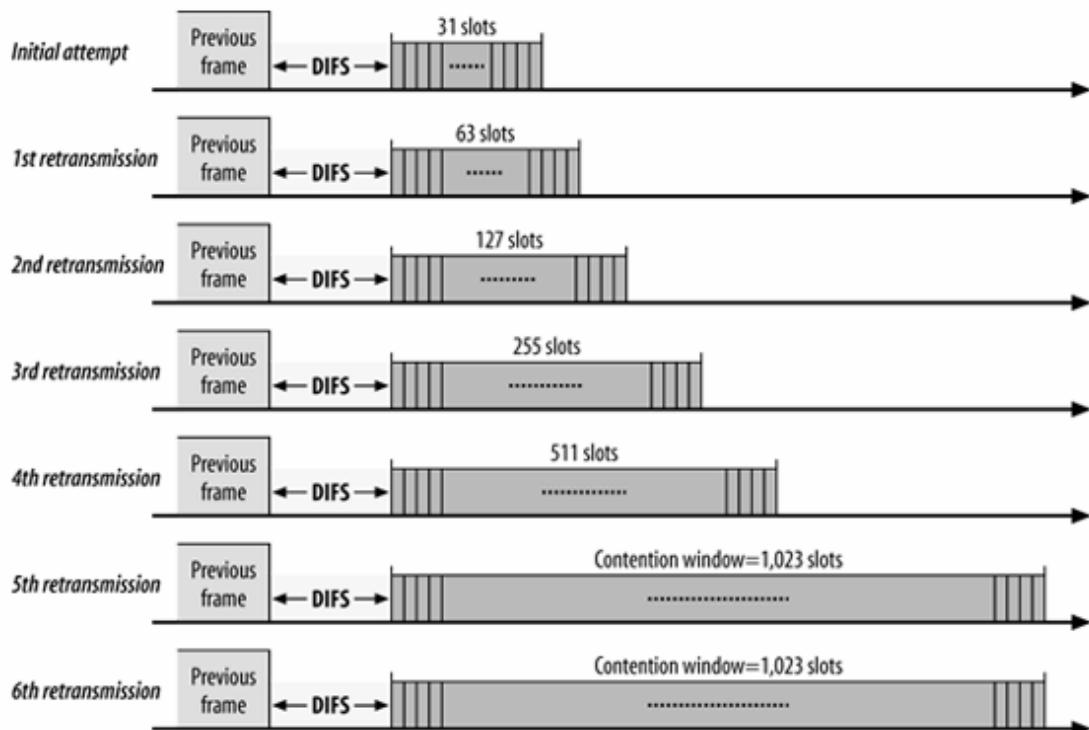


图 3-7: DSSS(直接序列展频)的竞争期间

3.3.5 帧的分段与重组

来自较上层的封包，以及某些较大的管理帧，可能必须经过分段，无线频道才有办法加以传输。当干扰存在时，分段封包同时有助于提升可靠性。利用帧的分段，无线局域网络的工作站可将干扰局限于较小的帧片段，而非较大的帧。由此降低可能受干扰的数据量，帧分段可以提高整体的有效传输量。干扰可能有不同来源。虽然并非全部，还是有些微波炉会对 2.4GHZ 网络造成干扰。从交流电振幅升起到下降这段时间，电磁管会产生电磁辐射，因此会有一半时间受到微波的干扰。

注 1：在美国，家电产品使用 60HZ 交流电，因此在每 16 毫秒的周期中，微波炉所造成的干扰有 8 毫秒。其他国家使用 50HZ 交流电，因此在每 20 毫秒周期中大约有 10 毫秒会受到干扰。

当上层封包超过网络管理人员所设定的分割门限，就会进行帧的分割。帧控制信息用来指示是否还有其他帧片段待接收。构成整个帧的所有帧片段通常会在所谓的片段宣泄期传输，如图 3-8 所示，其中包含了一个 RTS/CTS 交换过程，因为 fragmentation 与 RTS/CTS 门限通常会设定为相同的数值。此图同时显示了如何以 NAV 与 SIFS 的组合来控制介质的访问。

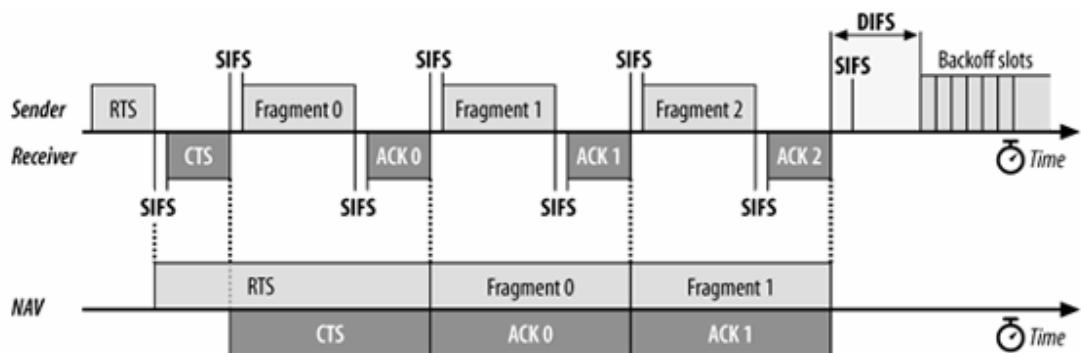


图 3-8: 片段宣泄期 (fragmentation burst)

帧片段与其应答之间以 SIFS 区隔，因此工作站在分段宣泄期 (fragmentation burst) 会一直持有频道的掌控权。NAV 可确保其他工作站在此 fragmentation burst 期间不致使用该频道。正如任何的 RTS/CTS 交换，RTS 与 CTS 会将 NAV 设定成从预定时间到第一个帧片段结束。其后的帧片段会彼此串通。每个帧片段都会设定 NAV，继续掌握介质的使用权，直到下一个帧的应答结束。图中，fragment0 设定了 NAV，并继续掌握介质直到 ACK 1，而 Fragment 1 也设定了 NAV，并继续掌控介质直到 ACK 2，依此类推。当最后一个帧片段及其应答送出时，NAV 即会设定为 0，代表介质即将在“片段宣泄期”完成之后释放。

3.3.6 帧格式

因为无线数据链路所带来的挑战，MAC 被迫采用了许多特殊的功能，其中包括使用四个地址位。并非每个帧都会用到所有的地址位，这些地址位的值，也会因为 MAC 帧种类的不同而有所差异。不同类型的帧使用哪种地址位的细节，会在第 4 章加以说明。图 3-9 展示了一般的 802.11 MAC 帧。本节所有图示均依循 IEEE 802.11 的格式。位的传送顺序由左至右，最高效 bit 将会最后出现。

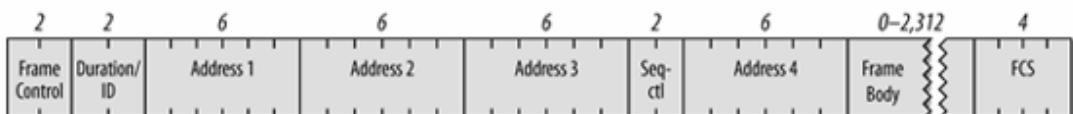


图 3-9: 一般的 802.11 MAC 帧

802.11 MAC 帧并未包含以太网帧的某些典型功能，其中最显著的是 type/length 位以及 preamble (同步信号)。Preamble 属于物理层，而封装细节 (如 type 与 length) 则出现在 802.11 帧所携带的标头 (header) 中。

3.3.7 Frame Control 位

所有帧的开头均是长度两个元组的 Frame Control (帧控制) 位，如图 3-10 所示。Frame Control 位包括以下次位：

Protocol 位

协议版本位由两个 bit 构成，用以显示该帧所使用的 MAC 版本。目前，802.11 MAC 只有一个版本；它的协议编号为 0。未来 IEEE 如果推出不同于原始规格的 MAC 版本，才会出现其他版本的编号。到目前为止，802.11 改版尚不需用到新的协议编号。

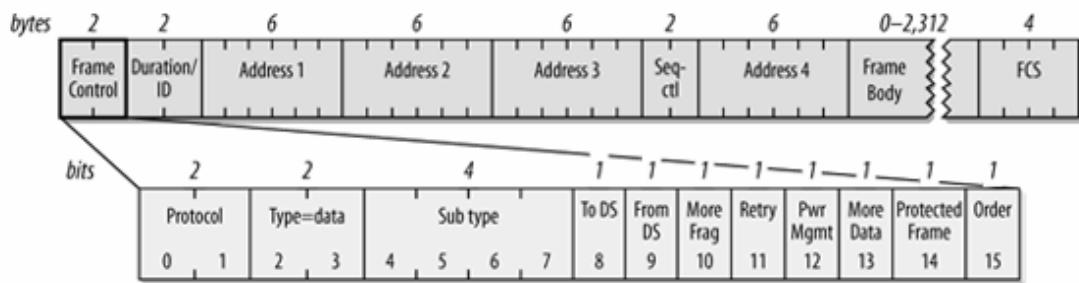


图 3-10: Frame control 位

Type 与 Subtype 位

类型与次类型位用来指定所使用的帧类型。为了抵抗噪声与提升可靠性, 802.11 MAC 内建了一些管理功能, 有些功能之前已经提过, 如 RTS/CTS 与应答。表 3-1 显示了 type 与 subtype 位跟帧类型的对应关系。

如表 3-1 所示, 最高效 bit 会最先出现, 恰好与图 3-10 相反。因此, Type 次位是 frame control 位的第三个 bit 之后跟着第二个 bit (b3 b2) , 而 Subtype 次位则是第七个 bit 之后跟着第六、第五以及第四个 bit (b7 b6 b5 b4) 。

表1 表 3-1: Type 与 Subtype 位的值与名称

Subtype 的值	Subtype 的名称
Management frames (管理帧: Type=00) 【注 a】 ^a	
0000	Association request (连接要求)
0001	Association response (连接应答)
0010	Reassociation request (重新连接要求)
0011	Reassociation response (重新连接应答)
0100	Probe request (探查要求)
0101	Probe response (探查应答)
1000	Beacon (导引信号)
1001	Announcement traffic indication message (ATIM) (数据代传指示通知信号)
1010	Disassociation (解除连接)
1011	Authentication (身份验证)
1100	Deauthentication (解除认证)
Control frames (控制帧: Type=01) 【注 b】	
1010	Power Save-Poll (省电模式一轮询)

表1 表 3-1: Type 与 Subtype 位的值与名称

Subtype 的值	Subtype 的名称
1011	RTS (请求发送)
1100	CTS (允许发送)
1101	ACK (应答)
1110	CF-End (免竞争期间结束)
1111	CF-End (免竞争期间结束) + CF-Ack (免竞争期间回应)
Data frames (数据帧: Type=10) 【注 c】	
0000	Data (数据)
0001	Data+CF-Ack
0010	Data+CF-Poll
0011	Data+CF-Ack+CF-Poll
0100	Null data (无数据: 未发送数据)
0101	CF-Ack (未发送数据)
0110	CF-Poll (未发送数据)
0111	Data+CF-Ack+CF-Poll
1000	QoS Data 【注 c】
1001	QoS Data + CF-Ack 【注 c】
1010	QoS Data + CF-Poll 【注 c】
1011	QoS Data + CF-Ack + CF-Poll 【注 c】
1100	QoS Null (未发送数据) 【注 c】
1101	QoS CF-Ack (未发送数据) 【注 c】
1110	QoS CF-Poll (未发送数据) 【注 c】
1111	QoS CF-Ack+CF-Poll (未发送数据) 【注 c】

(帧类型 11 保留尚未使用)

【注 a】管理帧之 subtype 值 0110-0111 与 1110-1111 目前保留尚未使用

【注 b】控制帧之 subtype 值 0000-0111 目前保留尚未使用

【注 c】由 802.11e 任务小组所提议, 但尚未标准化。注意这些帧均为 1 开头,

表1 表 3-1: Type 与 Subtype 位的值与名称

Subtype 的值	Subtype 的名称
------------	-------------

因此有人称第一个 bit 为 QoSbit。

TO DS 与 From DSbit

这两个 bit 用来指示帧的目的地是否为传输系统。在基础网络里，每个帧都会设定其中一个 DS bit。你可以根据表 3-2 来解读这两个 bit。第四章将会说明，地址位的解读取决于这两个 bit 的设定。

表2 表 3-2: To DS 与 From DSbit 所代表意义

To DS=0	To DS=1
From DS=0 所有管理与控制帧 IBSS (非基础型数据帧)	基础网络里无线工作站所发送的数据帧
From DS=1 基础网络里无线工作站所收到的数据帧	无线桥接器上的数据帧

More fragments bit

此 bit 的功能类似 IP 的 More fragments bit。若较上层的封包经过 MAC 分段处理，最后一个片段除外，其他片段均会将此 bit 设定为 1。大型的数据帧以及某些管理帧可能需要加以分段；除此之外的其他帧则会将此 bit 设定为 0。实际上，大多数数据帧均会以最大的以太网长度进行传送，不过帧分段并不常用。

Retry bit

有时候可能需要重传帧。任何重传的帧会将此 bit 设定为 1，以协助接收端剔除重复的帧。

Power management bit

802.11 网卡通常以 PC Card 的型式出现，主要用于以电池供电的膝上型或手持式电脑。为了提高电池的使用时间，通常可以关闭网卡以节省电力。此 bit 用来指出传送端在完成目前的基本帧交换之后是否进入省电模式。1 代表工作站即将进入省电模式，而 0 则代表工作站会一直保持在清醒状态。基站必须行使一系列重要的管理功能，所以不允许进入省电模式，因此基站所传送的帧中，此 bit 必然为 0。

More data bit

为了服务处于省电模式的工作站，基站会将这些由“传输系统”接收而来的帧加以暂存。基站如果设定此 bit，即代表至少有一个帧待传给休眠中的工作站。

Protected Frame bit

相对于有线网络，无线传输本质上就比较容易遭受拦截。如果帧受到链路层安全协议的保护，此 bit 会被设定为 1，而且该帧会略有不同。之前，Protected Frame bit 被称为 WEP bit。

Orderbit

帧与帧片段可依序传送，不过发送端与接收端的 MAC 必须付出额外的代价。一旦进行“严格依序”传送，此 bit 被设定为 1。

3.3.8 Duration/ID 位

Duration/ID 位紧跟在 frame control 位之后。此位有许多功用，有三种可能的形式，如图 3-11 所示。

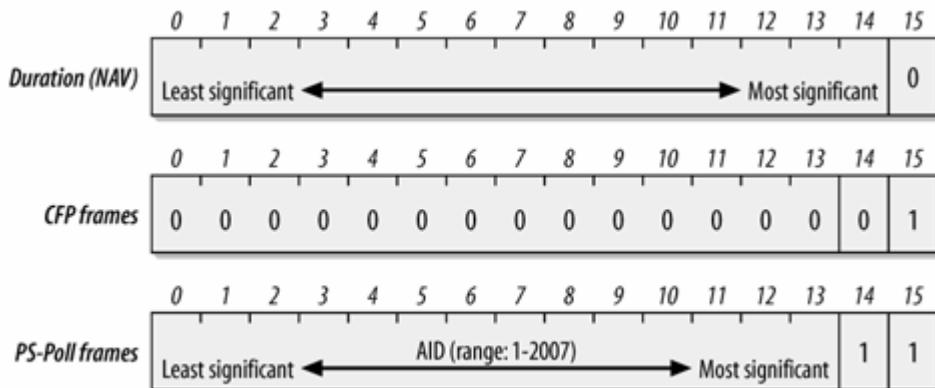


图 3-11: Duration/ID 位

3.5.2.1 Duration: 设定 NAV

当第 15 个 bit 被设定为 0 时，Duration/ID 位就会被用来设定 NAV。此数值代表目前所进行的传输预计使用介质多少微秒。工作站必须监视所收到的任何帧头，并据以更新 NAV。任何超出预计使用介质时间的数值均会更新 NAV，同时阻止其他工作站访问介质。

3.5.2.2 免竞争期间所传送的帧

在免竞争期间（contention-free period，简称 CFP），第 14 个 bit 为 0 而第 15 个 bit 为 1。其他所有 bit 均为 0，因此 duration/ID 位的值为 32768。这个数值被解读为 NAV。它让没有收到 Beacon（信标）帧『注』的任何工作站，得以公告免竞争期间，以便将 NAV 更新为适当的数值，避免干扰到免竞争传输。

注 Beacon 帧是管理帧的次类型（subtype），因此字首以大写表示。

3.5.2.3 PS-Poll 帧

在 PS-Poll（省电模式一轮询）帧中，第 14 与第 15 个 bit 会被同时设定为 1。移动式工作站可以关闭天线以达到省电目的。休眠中的工作站必须定期醒来。为确保不致丢失任何帧，从休眠状态醒来的工作站必须送出一个 PS-Poll 帧，以便从基站取得之前暂存的任何帧。此外，醒来的工作站会在 PS-Poll 帧中加入连接识别码（association ID，简称 AID），以显示其所隶属的 BSS。AID 包含在 PS-Poll 帧中，其值介于 1-2,007。而介于 2,008-16,383 的值目前保留并未使用。

3.3.9 Address 位

一个 802.11 帧最多可以包含四个地址位。这些位地址位均经过编号，因为随着帧类型不同，这些位的作用也有所差异（详见第 4 章）。基本上，Address 1 代表接收端，Address 2 代表传

送端, Address 3 位被接收端拿来过滤地址。举例而言, 在基础网络里, 第三个地址位会被接收端用来判定该帧是否属于其所连接网络。『注』

注 802.11 规定工作站应该忽略那些不属于相同 BSSID 的帧, 不过大多数产品并未正确实现 BSSID 过滤功能, 还是会将接收到的所有帧传给上层协议。

802.11 所使用的定位模式, 乃是依循其他 IEEE 802 网络所使用的格式, 包括以太网。地址位本身的长度有 48 个 bit。如果传送给实际介质的第一个 bit 为 0, 该地址位代表单一工作站 (单点传播[unicast])。如果第一个 bit 为 1, 该地址代表一组实际工作站, 称为组播 (多点传播[multicast]) 地址。如果所有 bit 均为 1, 该帧即属广播 (broadcast), 因此会传送给连接至无线介质的所有工作站。

这些长度 48 个 bit 的地址位有各种不同的用途:

- 目的地址

和以太网一样, 目的地址 (Destination address) 是长度 48 个 bit 的 IEEE MAC 识别, 码, 代表最后的接收端, 亦即负责将帧交付上层协议处理的工作站。

- 源地址

此为长度 48 个 bit 的 IEEE MAC 识别码, 代表传输的来源。每个帧只能来自单一工作站, 因此 Individual/Group bit 必然为 0, 代表来源地址 (Source address) 为单一工作站。

- 接收端地址

此为长度 48 个 bit 的 IEEE MAC 识别码, 代表负责处理该帧的无线工作站。如果是无线工作站, 接收端地址即为目的地址。如果帧的目的地址是与基站相连的以太网结点, 接收端即为基站的无线界面, 而目的地址可能是连接到以太网的一部路由器。

- 传送端地址

此为长度 48 个 bit 的 IEEE MAC 识别码, 代表将帧传送至无线介质的无线界面。传送端地址通常只用于无线桥接。

3.3.10 Basic Service Set ID (BSSID)

要在同一个区域划分不同的局域网络, 可以为工作站指定所要使用的 BSS (基本服务集)。在基础网络里, BSSID (基本服务集标识) 即是基站无线界面所使用的 MAC 地址。而对等 (Ad hoc) 网络则会产生一个随机的 BSSID, 并将 Universal/Localbit 设定为 1, 以防止与其他官方指定的 MAC 地址产生冲突。

要使用多少地址位, 取决于帧类型。大部分的数据帧会用到三个位: 来源、目的以及 BSSID。数据帧中, 地址位的编号与排列方式取决于帧的传送路径。大部分的传输只会用到三个地址, 这解释了为什么在帧格式中, 四个地址位都有其中三个位相邻的。

3.3.11 顺序控制位

此位的长度为 16 个 bit, 用来重组帧片段以及丢弃重复帧。它由 4 个 bit 的 fragment number (片段编号) 位以及 12 个 bit 的 sequence number (顺序编号) 位所组成, 如图 3-12 所示。

控制帧未使用顺序编号，因此并无 sequence control 位。

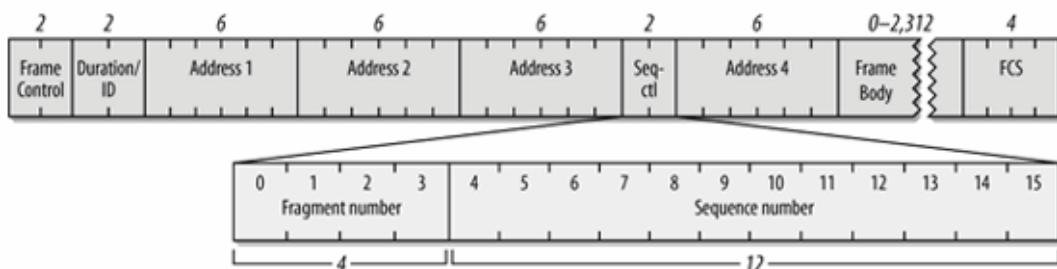


图 3-12: Sequence Control 位

当上层帧交付 MAC 传送时，会被赋予一个 **sequence number**（顺序编号）。此位的作用，相当于已传帧的计数器取 4096 的模（modulo）。此计数器由 0 起算，MAC 每处理一个上层封包就会累加 1。如果上层封包被切割处理，所有帧片段都会具有相同的顺序编号。如果时重传帧，则顺序编号不会有任何改变。

帧片段之间的差异在于 **fragment number**（片段编号）。第一个片段的编号为 0。其后每个片段依序累加 1。重传的片段会保有原来的 **sequence number** 协助重组。

具备 QoS 延伸功能的工作站对 **sequence control** 位的解读稍有不同，因为这类工作站必须同时维护多组传送队列。

3.3.12 帧主体

帧主体（Frame Body）亦称为数据位，负责在工作站间传送高层数据（payload）。在最初制定的规格中，802.11 帧最多可以传送 2304 个 bit 组的上层数据。（实际上必须能够容纳更多的数据，以便将安全性与 QoS 相关标头纳入）802.2 LLC 标头具有 8 个 bit 组，最多可以传送 2296 个 bit 组的网络协议数据。防止分段必须在协议层加以处理。在 IP 网络中，Path MTU Discovery（路径最大传输单位查询；RFC1191）将可避免大于 1500 个 bit 组的帧传递。

802.11 与其他链路层技术不同之处，表现在两个比较显著的方面。首先，在 802.11 帧中并无任何上层协议的标记可供区别。上层协议是以额外标头 type 位加以标记，同时将其作为 802.11 所承载数据的开始。其次，802.11 通常不会将帧填补至最小长度。802.11 所使用的帧并不大，随着芯片与电子技术的进展，目前已经没有填补的必要。

3.3.13 帧检验序列 (FCS)

和以太网一样，802.11 帧也是以帧检验序列（frame check sequence，简称 FCS）作为结束。FCS 通常被视为循环冗余码（cyclic redundancy check，简称 CRC），因为底层的数学运算相同。FCS 让工作站得以检查所收到的帧的完整性。FCS 的计算范围涵盖 MAC 标头里所有位以及帧主体。虽然 802.3 与 802.11 计算 FCS 的方法相同，不过 802.11 所使用的 MAC 标头与 802.3 的不同，因此基站必须重新计算 FCS。

当帧送至无线界面时，会先计算 FCS，然后再由 RF 或 IR 链路传送出去。接收端随后会为所收到的帧计算 FCS，然后与记录在帧中的 FCS 做比较。如果两者相符，该帧极有可能在传输过程中并未受损。

在以太网上，如果帧的 FCS 有误，则随即予以丢弃，否则就会传送给上层协议处理。在 802.11 网络上，通过完整性检验的帧还需接收端送出应答。例如，接收无误的数据帧必须得到

正面应答，否则就必须重传。对于未能通过 FCS 检验的帧，802.11 并未提供负面应答机制；在重传之前，工作站就必须等候应答超时。

3.4 802.11 对上层协议的封装

和所有其他的 802 链路层一样，802.11 可以传输各种不同的网络层协议。和以太网不同的是，802.11 是以 802.2 的逻辑链路控制封装来携带上层协议。图 3-13 显示了如何以 802.2LLC 封装来携带 IP 封包。如该图所示，802.1H 与 RFC 1042 所使用的『MAC 标头』长度为 12 个 bit 组，其内容为以太网上的『源 MAC 地址』与『目的 MAC 地址』，或者前面所提到的长标头（long 802.11MAC header）。

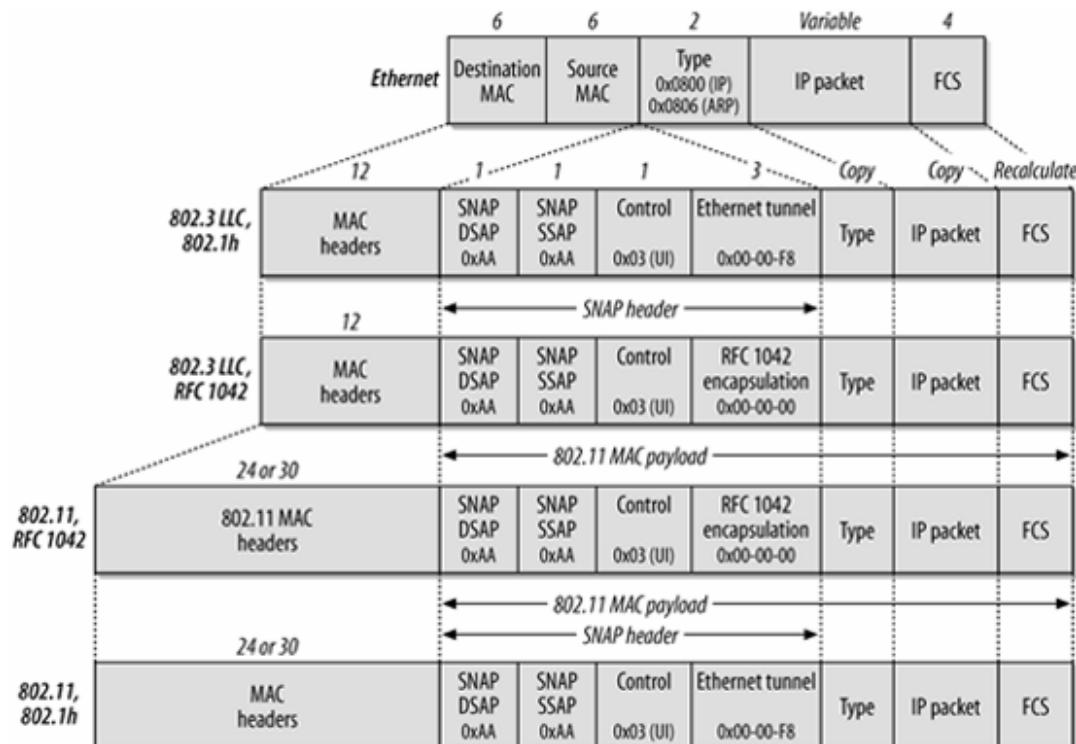


图 3-3: 802.11 里的 IP 封装

传输时，用来封装 LLC 数据的方式有两种。其中一种是 RFC 1042 所描述的方式，另外一种则是 802.1H 所规范的方式。两种标准各自有其别名。RFC 1042 有时候被称为 IETF 封装，而 802.1H 有时候则被称为隧道式封装（tunnel encapsulation）。

这两种方式极为相似，如图 3-13 所示。此图最上方为以太网帧，它具有 MAC 标头（源与目的 MAC 地址），类型代码（type code），内嵌封包（embedded packet）以及帧检验等位。在 IP 领域里，Type code 不是代表 IP 的本身的 0X0800（十进制的 2048），就是代表地址解析协议（简称 ARP）的 0X0806（十进制的 2054）。

RFC 1042 与 802.1H 均衍生自 802.2 的子网络访问协议（sub-network access protocol，简称 SNAP）。MAC 地址会被复制到封装帧（encapsulation frame）的开头，然后插入 SNAP 标头。SNAP 标头一开始是目的服务访问点（destination service access point,简称 DSAP）与源服务访问点（source service access point,简称 SSAP）。然后是一个控制位。和高阶数据链路控制（high-level data link control,简称 HDLC）及其衍生协议一样，此控制位会被设定为 0x03，

代表未编号信息（unnumbered information，简称 UI），对应到 IP datagram 所谓的尽力传送（best-effort delivery）范畴。SNAP 所置入的最后一个位是组织代码（organizationally unique identifier，简称 OUI）。起初，IEEE 希望用一个 bit 组的服务访问点（service access point）来涵盖网络协议编号，不过后来证明这种看法过于乐观。因此，SNAP 只得从原来的以太网帧复制一份类型代码（type code）。802.11H 与 RFC 1042 之间的唯一差异，在于其使用的 OUI。

有些产品可以让使用者在两种封装标准间进行切换，虽然这种功能并不常见。以 Microsoft 操作系统而言，AppleTalk 与 IPX 协议组预设使用 802.11H，其他协议则使用 RFC 1042。目前大部分基站均依循 Microsoft 的做法，不再提供封装方式的切换选项。事实上，由于 Microsoft 所采用的封装方式得到广泛的支持，因此 Wi-Fi 联盟的认证测试计划亦将它包含在内。

3.5 竞争式数据服务

为了增加可靠性，802.11 纳入了许多额外的功能。这些功能导致某些规则上的混淆，因而无法判断何时该允许使用何种类型的帧。这些额外的功能也让网络管理人员更难预测，有哪些帧会往来于所检视的网络中。本节的目的在澄清，802.11 局域网络中负责运送数据的基本交换程序。（大部分的管理帧只会公告给该区域中相关的对象，信息的传递纯粹是单向的。）

本节所陈述的是基本交换程序，也就是说数据的交换过程必须视为单一整体。举例而言，单点传播数据必须得到应答以确保数据传送无误。虽然整个数据的交换过程包含两个帧，但数据交换本身只算第一过程。只要有一方失误，整个过程就必须重新来过。802.11 定义了两组截然不同的基本交换程序。其一为 DCF，用于竞争服务，详见本章。第二种交换方式为 PCF，用于免竞争服务（contention-free service）。免竞争服务所使用的帧交换方式不仅错综复杂，而且还难以理解。有鉴于商业化产品很少实现免竞争服务，其交换过程不再赘述。

DCF 说使用的帧交换方式在 802.11 MAC 中占有决定性的地位。根据 DCF 的规定，所有的产品都必须提供尽力的传递功能。为了实现竞争式 MAC，处于作用状态的工作站都必须处理每个帧的 MAC 标头。整个帧交换过程，始终某部工作站在 DIFS 之后取得闲置介质的使用权。

3.5.1 广播与组播数据或管理帧

广播与组播帧的交换过程最为简单，因为这些帧无须应答。这两种帧也可以视为群组帧，因为其接收对象不限于单一工作站。帧封装（framing）与定位（addressing）在 802.11 中较为复杂，适用此规则的帧类型如下所示：

- 广播数据帧会在 Address1 位中填入广播地址
- 组播数据帧会在 Address1 位中填入组播地址
- 广播 理帧会在 Address1 位中填入广播地址（Beacon、Probe Request 以及 IBSS ATIM 帧）

组播帧无法加以分段，也无须得到应答。整个基本交换过程只牵涉到一个帧，根据竞争式访问控制规则加以传递。传送结束后，所有工作站必须等待一段 DIFS 时间，然后在竞争期间倒数随机产生的延迟时间。

因为帧的交换过程只牵涉到一个帧，所以将 NAV（网络分配矢量）设定为 0。既然此后已无其他帧，也就不必使用虚拟载波监听锁住介质，来防止其他工作站的访问。传送该帧之后，所

有工作站均会等候一段 DIFS 时间，然后通过竞争期间开始为任何遭延迟的帧进行倒数。整个交换过程，详见图 3-14。

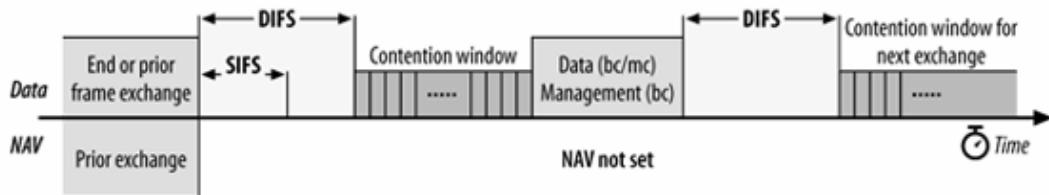


图 3-14: 广播/组播数据以及广播管理的基本帧交换过程

因环境而异，组播帧可能会遇到低劣的服务质量，因为这些帧没有得到任何应答。因此，有些工作站可能会遗漏广播或组播数据。不过 MAC 并未内建任何机制可用以重传广播或组播帧。

3.5.2 单点传播帧

在 802.11 标准中，针对个别工作站所传送的帧称为直接数据（**direct data**）。本书中使用较通俗的字眼，称之为单点传播（**unicast**）。单点传播帧必须得到应答以确保可靠性，亦即可借助各种机制来改善传输效率。本节所描述的交换过程适用于任何单点传播帧，因此也适用于管理帧与数据帧。实际上，这些过程通常只见于数据帧。

3.7.2.1 单一帧（最后一个片段）及其正面应答

两部工作站之间的传输可靠性建立在简单的正面应答上。单点传播数据帧必须得到正面应答，否则该帧即会被认定已经丢失。单一帧及其回应是最基本的例子，如图 3-15 所示。

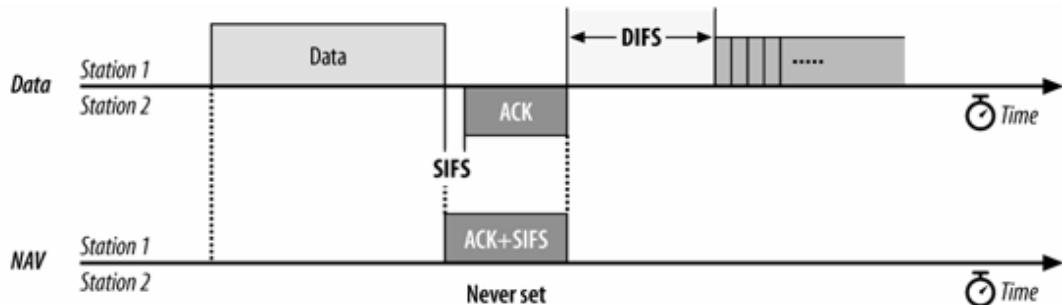


图 3-15: 单一帧及其正面回应

此帧会利用 NAV 为本身、应答及 SIFS 预定介质使用权。设定较长的 NAV，是为了替整个交换程序锁住虚拟载波，以保证接收端可以传送应答。因为此交换程序是以 ACK 做为结束，所以没有必要再锁住虚拟载波，因此该 ACK 中 NAV 会被设定为 0。

3.7.2.2 帧分段

包括 IP 在内，一些较上层的网络协议或多或少都会用到帧分段。在网络层进行分段的缺点是，接收端必须加以重组；如果帧在传输过程中遗失，整个封包就必须重传。在链路层使用分段机制可以提升速度，亦即以较小的 MTU 在转运点（hop）间传送数据。

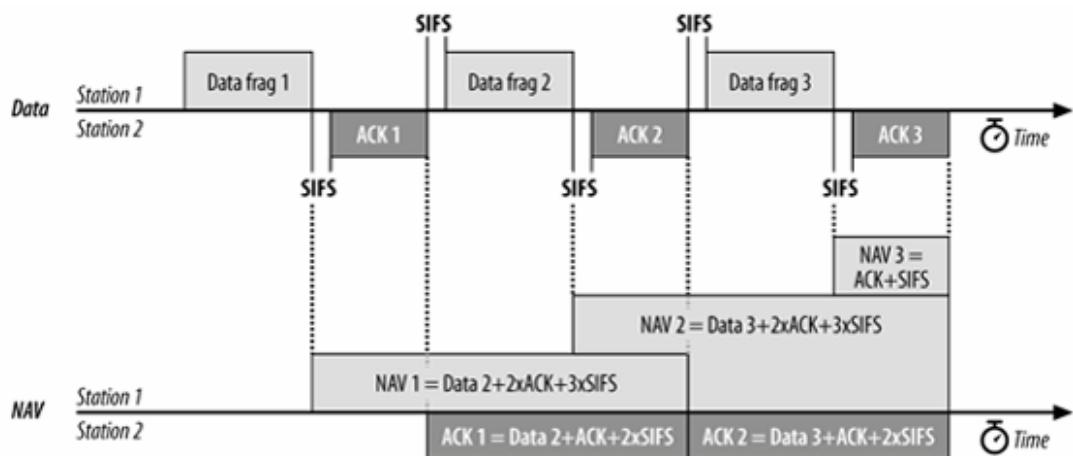


图 3-16: 帧分段

此外，802.11 可以利用帧分段来避免干扰。无线点播干扰通常会以瞬间而高能量的尖波形式出现，而且经常与 AC 电源线同步。将帧加以分段，可保护大部分帧不遭受损害。基本分段机制如图 3-16 所示。

最后两个帧和之前的交换过程没有两样，NAV 的设定也完全相同。不过，倒数第二个帧之前所有帧均会使用 NAV，为下一个帧锁住介质。第一个数据帧会将 NAV 的时间设定至足以涵盖 ACK1，下一个帧片段及其回应（ACK2）。为了表示其为帧片段，MAC 会将帧标头控制位的 More Fragmentsbit 设定为 1。最后一个回应（ACK3）除外，其余回应都会继续为下一个数据片段及其回应延长锁住介质的时间。后续的数据帧会继续延长 NAV 以涵盖后续的回应，直到最后一个数据帧才会将 More Fragmentsbit 设定为 0，而最后一个回应（ACK3）则会将 NAV 设定为 0。帧片段的数目并无限制，不过虚空总长度必须短于 PHY 对交换过程所做的限制。

帧分段是由 MAC 的 fragmentation threshold(切割门限)参数所控制。大部分的网卡驱动程序都允许使用者设定此参数。任何超过分段门限的帧都会被加以分段，分段方式因实际情况而异。调高分段门限意味着帧的传输负担较小，不过帧丢掉和损害的成本较高，因为将会有较多的数据必须丢弃与重传。调低分段门限意味着传输负担较重，不过在面临较恶劣的环境时，这种做法可以提供较佳的稳定性。

3.7.2.3 RTS/CTS

为保证介质使用权以及数据传输不被中断，工作站可使用 RTS/CTS 的交换方式。图 3-17 说明了整个程序。RTS/CTS 交换的做法和帧分段一开始没有什么两样，只是 RTS 帧并未携带任何数据。RTS/CTS 中的 NAV 可让 CTS 完成工作，而 CTS 则可用来为数据帧保留使用权。

RTS/CTS 可用在所有的帧交换、非帧交换或介于两者之间。和帧分段一样，RTS/CTS 是由启动程序中的门限值来控制的。超过该门限的帧由 RTS/CTS 先行清空介质，而较小的帧则直接传送。

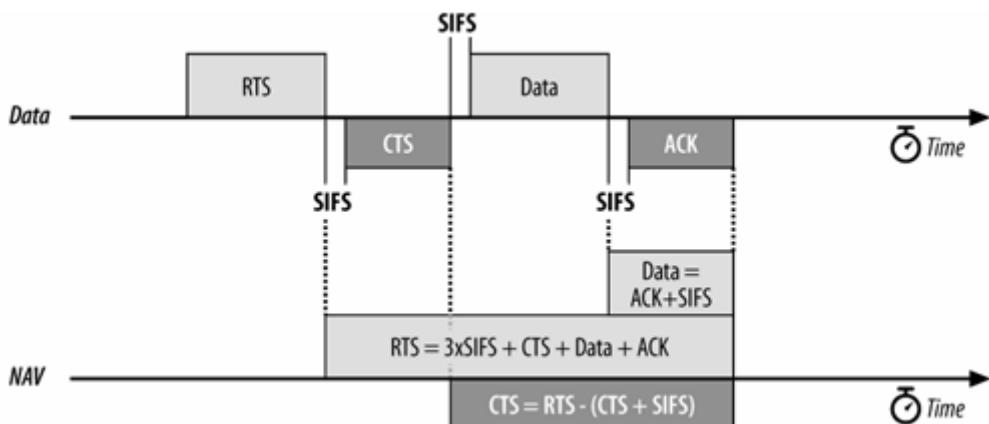


图 3-17: 以 RTS/CTS 锁住介质

3.7.2.4 RTS/CTS 与帧分段

实际上，RTS/CTS 交换过程通常与帧分段并行。虽然经过分段，帧片段还是有一定的长度，因此可受惠于 RTS/CTS 程序所确保的介质独家使用权，免与隐藏节点的竞争。有些厂商将帧分段门限与 RTS/CTS 门限的预设值设成一样。

Figure 3-18. RTS/CTS with fragmentation

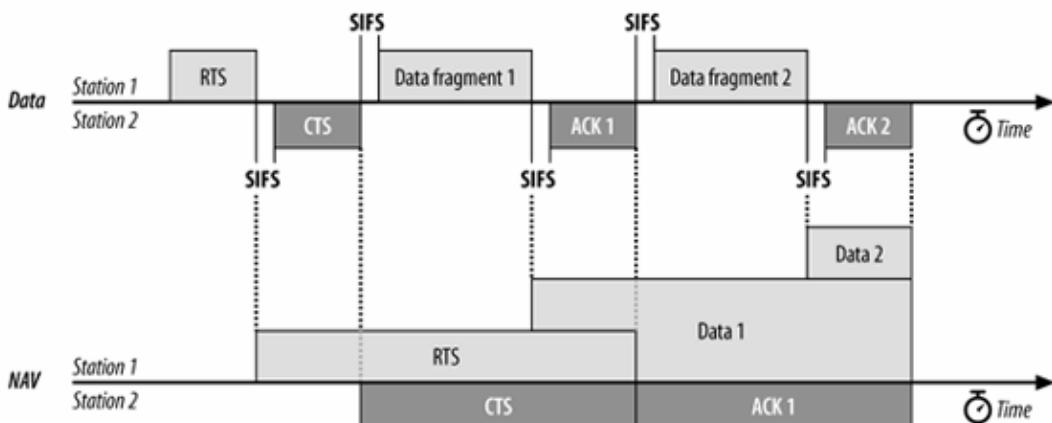


图 3-18: RTS/CTS 与帧分段

3.5.3 省电程序

在 RF 系统中，放大器是最耗电的元件，由它负责将发送出的信号放大，以及将所收到的信号放大到可处理的水平。802.11 工作站可以关闭无线电波收发器，并且定期进入休眠状态，以维持最长的电池使用时间。在这段期间，基站会为每部处于休眠状态的工作站暂存帧。若有暂存帧，基站会在后续的 Beacon 帧中告知工作站。由省电状态唤醒的工作站可以使用 PS-Poll 帧取得这些暂存帧。

接收到 PS-Poll 帧的基站，可以立即采取回应，也可以等到环境许可，比较空闲时再予以应答。有时候，采用哪种 PS-Poll 回应决定自基站所采用的芯片组的厂商。有些芯片组厂商同时支持两种模式，有些则只支持一种。802.11 只要求支持一种方式即可，因此两种做法均符合标准要求。

3.7.3.1 立即应答

基站可以对 PS-Poll (省电模式一轮询) 帧立即作出应答。经过一段 SIFS(短帧间隔)时间，基站即可传送帧。如图 3-19 所示，PS-Poll 帧隐含了一 NAV。PS-Poll 帧的 Duration/ID 位中包含了 Association ID (连接识别码)，因此基站可以判断有哪些帧是为该工作站所暂存的。不过，MAC 规格书要求所有收到 PS-Poll 的工作站都必须更新 NAV，将 NAV 的值设定为一个 SIFS 加上一个 ACK 的时间。虽然此 NAV 对数据帧而言过短，但基站会取得介质使用权，而所有工作站都会为了这个数据帧而延后访问介质。但数据帧传送结束时，NAV 随即更新以反映数据帧标头中的数值。

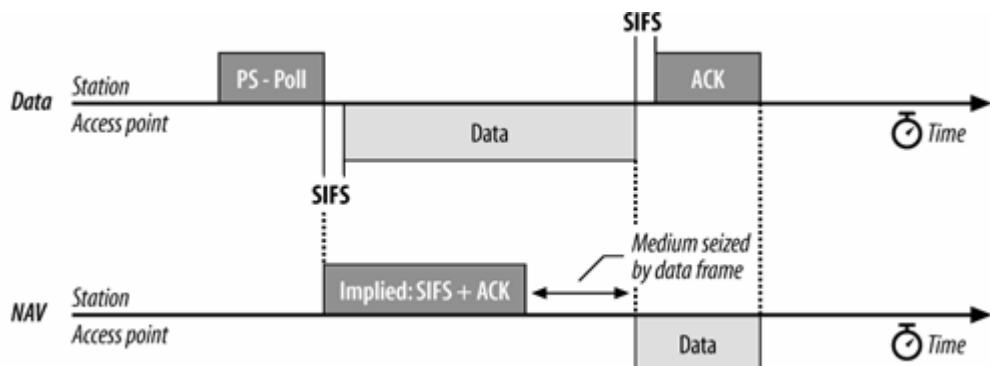


图 3-19：立即的 PS-Poll 回应

如果暂存的帧过大，则必须进行分段。图 3-20 说明了帧分段情况下的 PS-Poll 立即应答。和其他工作站一样，基站的分段门限通常可由使用者来设定。

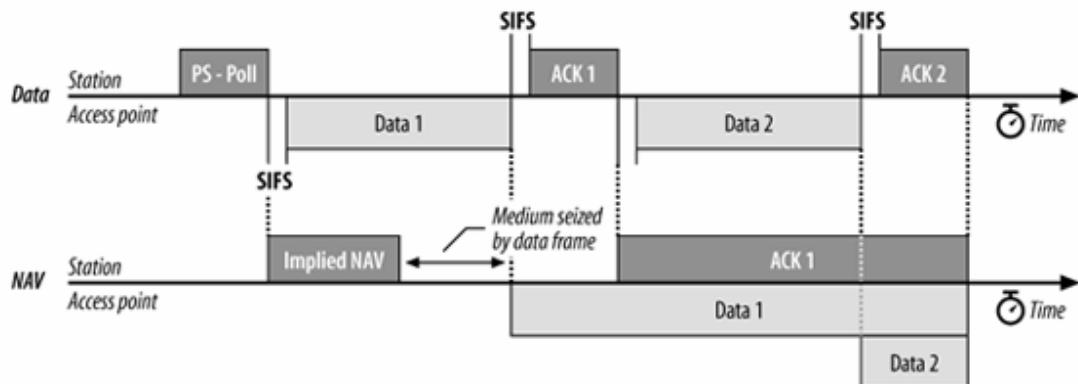


图 3-20：帧分割情况下的 PS-Poll 立即回应

3.7.3.2 延迟应答

除了立即应答，基站可以先回复一个简单应答。这种做法称为延迟应答 (deferred response)，因为基站虽然回应了访问暂存帧的要求，但未并立即采取实际的发送行动。使用延迟应答的优点之一，在于基站方面的软件较易实现，因为应答信息可以通过芯片组立即传送，至于数据则可以先予以暂存，然后依正常过程传输。

通过 PS-Poll 要求帧的工作站必须保持清醒，直到该帧传输完成。不过，在竞争式服务期间，基站可能在任何时间传递帧。此时工作站不能返回省电模式，除非接收到一个 Beacon 帧，其中对该工作站的 TIM (数据待传) bit 已被清除。

图 3-21 说明了整个过程。在此图中，工作站刚由省电模式转变为活动模式，同时注意到基站已经为它暂存了帧。于是工作站会发出 PS-Poll 给基站，要求接收这些暂存帧。不过，基站可能会选择延迟应答，因此只回传了一个 ACK。到目前为止，基站已经回应了工作站的暂存帧访问要求，并且承诺将在某个时间点加以传送。工作站必须处于活动模式等候，也许经过几次基本帧交换之后，基站就会送出工作站所要的数据。虽然在图 3-21 中并未显示，不过暂存帧还是有可能遭到分段的。

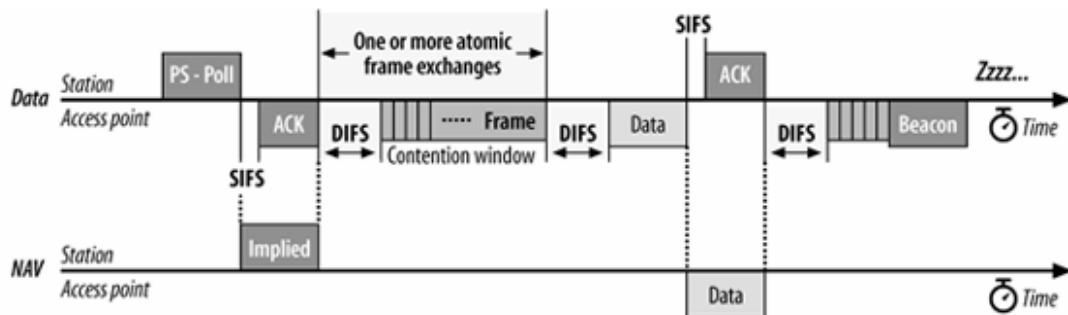


图 3-21：PS-Poll 延迟响应的范例

收到数据帧之后，工作站还是必须停留在清醒状态，直到下一个 Beacon 帧被传送出来。Beacon 帧只是用来提醒，是否有为某部工作站暂存的帧，没有办法告知实际的帧数量。一旦工作站收到的 Beacon 帧中显示已无暂存帧，便可断定已经完成暂存帧的接收，然后返回省电模式。

3.5.4 多种速率支持 (Multirate Support)

能够以不同速度工作的网络技术必须具备一种机制，可以协调出一种收发端彼此均可接受的数据率。速度协商对工作站而言尤其方便。工作站可以经常变化速率，以便回应无线电环境的快速变动。但工作站间的距离改变，速度也会随之变动。工作站必须能够适应随时变动的环境，必要时更改传输速率。和一些其他协议功能一样，802.11 标准并未规范该如何选择传输速率。标准只是提出一般原则，在实际上厂商享有相当大的自由。其中，有些规则适用于所有工作站：

- 每部工作站均保有一份速率清单，其中记录工作站与所连接 BSS 均支持的所有速率。（所谓 BSS，通常相当于一部基站，不过较新的产品可以让使用者依虚拟基站自订速率。）高于速率组合的传输速率是不允许用来传送帧的。
- 每个 BSS 必须负责维护一组基本速率，即打算加入此 BSS 的工作站所必须支持的速率清单。任何传送至群组接收地址的帧必须以基本速率传送，确保所有工作站均可正确解读。
- 用来起始帧交换的控制帧，如 RTS 与 CTS，必须以基本速率组合中的一种速率进行传输。这一规则可以确保必须以 CTS 回应 RTS 帧的工作站，能够以相同速率工作。

控制帧可以用于回溯相容模式 (backwards-compatibility)，又称为防护 (protection) 模式；参见第 14 章。防护模式是为了避免新旧工作站间彼此干扰，因为较旧的工作站或许只支持较慢的调制技术，新式工作站却可以使用较快的调制方式。如果所在地区有些工作站不支持较新的调制方式，则必须以较旧的调制方式传输防护帧 (Protection frame)。

4. 发送给特定工作站的帧，会在 Address 1 位记载单点传播目的地址。单点传播帧（Unicast frame）可以使用目的端支持的任一速率传送。至于数据速率的选择方式，802.11 标准并未加以规范。

免竞争期间所使用的帧可以带有多重目的；参见第 9 章。如果帧中包含 ACK，就是用来应答之前的帧传送者而不是帧接收者。传送端必须确保该帧以接收端及目的端工作站均支持的速率传送。

5. ACK 或 CTS 之类的应答帧必须以基本速率组合所包含的速率传送，但不能高于这次传输所使用的起始帧。应答帧必须使用与起始帧相同的调制方式（DSSS、CCK 或 OFDM）。

3.7.4.1 选速与降速

市面上所有 802.11 界面均支持某种降速机制，可以适应不同网络环境选择所使用的数据率。速率选择主要在决定一张网卡该在何时升速以提高链路质量。802.11 标准并未规范工作站如何决定是否降速（或升速），因此速率选择如何实现，留给芯片厂商自行决定。几乎所有芯片组均有自己一套选择机制，因此，大多数 802.11 界面的工作方式均有所不同。速率选择可以通过程序控制，一般是由驱动界面的程序所控制。速率选择机制可以公国驱动程序或者软件升级。

最常用来判断何时应该变速的算法，其实是通过一些不是那么严谨的信号品质量测量。信号质量可以直接就信噪比（signal-to-noise ratio）加以测量，或者间接观察有多少帧需要重传。直接测量信噪比，可以针对最近一个帧的瞬间信号质量，或者就最近一段期间所接收到之一定数量的帧取平均数。有些芯片组会直接测量信噪比，不过随后会将之转换为相应的“信号质量”（signal quality）。当信号质量变差，芯片就会以降速来适应。

至于间接测量，则是监测瞬间或平均漏失多少帧，然后予以适度补偿。采用间接测量的算法，简单来讲就是：如果帧已经丢失且帧重传计数器已经用尽，那就降速至下一档，然后重试一遍；反复进行以上步骤直到帧送出，或者一直尝试到最低速率都无法成功传递为止。采用间接信号品质量测的芯片组或许会稍微修改上述算法，避免耗费过多时间在物理层所支持的所有速率间逐次降速。尤其近来的芯片组均支持不少的速率，在较低速率上反复重试将会相当费时。

3.6 帧的处理与桥接

无线基站的核心，其实就是桥接器，负责在无线与有线介质之间转换帧。虽然 802.11 并未限制非得使用哪种有线介质技术，放弃以太网不用的基站还真没见过。大多数基站在设计上就是扮演 802.11 与以太网之间的桥梁，因此，了解帧在两种介质之间的传递方式就相当重要。如图 3-22 所示。

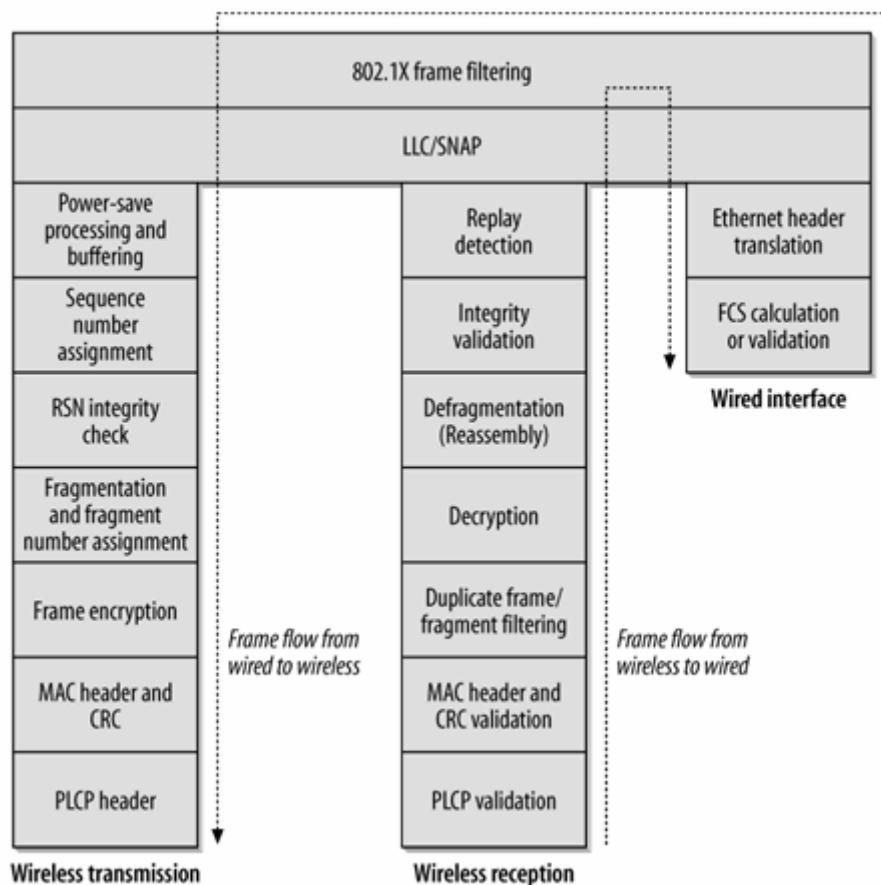


图 3-22：在无线与有线介质之间转换帧

3.6.1 无线介质到有线介质（802.11 至以太网）

当基站的无线界面接收到准备传送至有线网络的帧，基站就必须在两种介质间桥送帧。非正式来讲，以下是基站必须进行的一系列工作：

1. 当基站接收到一个帧，首先会检测该帧基本上是否完整。接下来，基站会针对所使用的物理层，检视本章之前讨论过的物理层标头，然后验证 802.11 帧上的帧检验码。
2. 证帧接收无误后，基站就会继续检视是否应该进一步处理该帧。
 - a. 传送至基站的帧，会将基站的 MAC 地址（即 BSSID）摆在 802.11 MAC 标头的 Address 1 位。不符该基站 BSSID 的帧应予以丢弃。（有些产品并未实现此步骤。）
 - b. 802.11 MAC 接着监测且移出重复的帧。产生重复帧的原因很多，不过最常见的原因是 802.11 应答信息在传送过程中丢失或有所损毁。为了简化上层协议的工作，因此由 802.11 MAC 负责剔除重复的帧。

3. 一旦基站判定需要进一步处理该帧，就必须予以解密，因为该帧会受到链路层安全算法的保护。解密的细节详见后续与安全性有关的章节。
4. 成功解密之后，基站即检视该帧是否为帧片段，需要进一步重组。完整性保护（integrity protection）针对重组后完整帧，而不是个别的帧片段。
5. 如果经过步骤 2a 的 BSSID 检验，判定基站必须桥送该帧，较复杂的 802.11 MAC 标头就会被转换为较简单的以太网 MAC 标头。
 - a. 记录在 802.11 MAC 标头之 Address 3 位里的目的地址，会被复制到以太网的目的地址。
 - b. 记录在 802.11 MAC 标头之 Address 2 位里的源地址，会被复制到以太网的源地址。
 - c. 从 802.11 Data 位里的 SNAP 标头，将（Type）类型代码复制到以太网帧里的 Type 位。如果该以太网帧亦使用 SNAP，就复制整个 SNAP 标头。
 - d. 顺序信息主要供帧片段重组之用，不过当帧被桥送之后即予以丢弃。
 - e. 如果有标准的服务质量处理程序，即在此进行无线与有线的 Qos 对应。不过到目前为止，用来表示服务质量的形式，通常就是在有线帧中使用 802.1p 优先性等级 bit，或者其他控制形式。
6. 重新计算帧检验码。以太网与 802.11 使用相同的算法来计算 FCS，不过 802.11 帧多出一些位，同时为 FCS 所保护。
7. 所产生的新帧交付以太网界面传送。

3.6.2 有线介质至无线介质（Wired Medium to Wireless Medium）

将帧从基站有线端桥接至无线介质的过程刚好相反：

1. 验证以太网 FCS 后，基站首先会检视是否需要进一步处理所接收到的帧，亦即检视该帧的目的地址是否属于目前与基站连接的工作站。
2. 将 SNAP 标头附加于以太网帧的数据之前。上层封包是以 SNAP 标头进行封装，而其 Type 位是自以太网帧里的类型代码复制而来。如果该以太网帧亦使用 SNAP，则复制整个 SNAP 标头。
3. 对帧的传送进行排程。802.11 包含复杂的省电过程，将帧置于传送序列之前，基站可能会将帧暂存于缓存区。省电过程将于第 8 章详述。
4. 一旦帧被置于序列待传，就会被赋予一个顺序编号。如有必要，所产生的数据可以用完整性检验值加以保护。如果帧需要分段，则会根据事先设定好的分段门限进行分段。分段帧时，将会在 Sequence Control 位指定片段编号。
5. 如果帧需要保护，则对帧（或每个帧片段）的本体加密。
6. 802.11 MAC 标头是根据以太网 MAC 标头产生。
 - a. 将以太网 的目的地址复制到 802.11 MAC 标头的 Address 1 位。
 - b. 将 BSSID 置于 MAC 标头的 Address 2，以做为无线介质上之帧的发送者。
 - c. 将帧的源地址复制到 MAC 标头的 Address 3 位。
 - d. 将其他位填入 802.11 MAC 标头。也就是把预计传送时间填入 Duration 位，并把适当的旗标填入 Frame Control 位。
7. 重新计算帧检验码。以太网与 802.11 使用相同的算法来计算 FCS，不过 802.11 帧多出一些位，同时为 FCS 所保护。
8. 所产生的新帧交付 802.11 界面传送。

3.6.3 服务质量延伸功能

服务质量延伸功能会影响帧的传输顺序，但并不会改变帧行径 802.11 MAC 的基本路径。802.11e 服务质量延伸功能并非只使用单一传输序列，而是在上述有线至无线桥接程序中的第 4、5、7 步骤采用多组传输序列。这些步骤会根据优先次序进行帧处理；而优先次序取决于帧的内容以及配置设定中预先指定的优先性分级规则。

第4 章 802.11 帧封装细节

第三章主要在说明帧的基本结构及其组成位，不过并未深入探究各种不同类型帧的细节。以太网的帧封装十分简单，只要为帧加上同步信号、一些地址信息，以及在结尾加上检验码即可。相对而言，802.11 的帧封装就比较复杂，因为无线介质必须将有线网络所没有的帧类型，以及各式管理功能纳入考量。

802.11 帧主要有三种类型。数据帧好比 802.11 的驮马，负责在工作站之间传输数据。数据帧可能会因为所处的网络环境不同而有所差异。控制帧通常与数据帧搭配使用，负责区域的清空、信道的取得以及载波监听的维护，并于收到数据时予以正面的应答，借此促进工作站间数据传输的可靠性。管理帧负责监督，主要用来加入或退出无线网络，以及处理基站之间连接的转移事宜。

本章纯粹只供参考之用。每个作者的生命有限，不可能只是为了将这些细节讲述得活灵活现而投入所有的精力。各位不妨完全略过本章，等到需要深入研究帧结构时再回头来看。帧封装细节通常不在网络管理人员必懂的范围之内，只有一些少数例外，同时，本章使用了大量的缩写名词，不懂之处请参考书后的名词解释。

4.1 数据帧

数据帧会将上层协议的数据置于帧主体加以传递。图 4-1 显示了数据帧的基本结构。会用到哪些位，取决于该数据帧所属的类型。

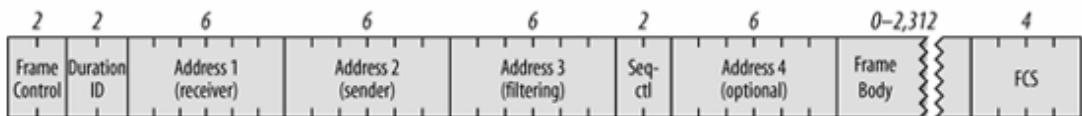


图2 基本的数据帧

不同类型的数据帧可根据功能加以分类。其中一种方式，是将数据帧区分为竞争式服务及免竞争服务两种数据帧。只能在免竞争期间出现的帧，就不可能在 IBSS（独立型基本服务组合）中使用。另一种区分方式，则是对携带数据与提供管理功能的帧加以区别。表 4-1 显示了数据帧的分类方式。免竞争服务所使用的帧，在第九章会有更详细的讨论。

表 4-1：数据帧的各种分类方式

帧类型	竞争式服务	免竞争服务	携带数据	未携带数据
Data	√		√	
Data+CF-Ack		√	√	

帧类型	竞争式服务	免竞争服务	携带数据	未携带数据
Data+CF-Poll		AP only	√	
Data+CF-Ack+CF-Poll		AP only	√	
Null	√	√		√
CF-Ack		√		√
CF-Poll		AP only		√
CF-Ack+CF-Poll		AP only		√

4.1.1 Frame Control (帧控制)

Frame Control (帧控制) 位各个 bit 的用法在第三章早已说明。每个帧控制 bit 都可能影响到 MAC 标头其他位的解读方式。最值得注意的是那些地址位，它们的意义将因 ToDS 及 FromDSbit 的值而异。

4.1.2 Duration (持续时间)

Duration (持续时间) 位用来记载网络分配矢量 (NAV) 的值。访问介质的时间限制是由 NAB 所指定。数据帧之 Duration 位的设定，必须依循四项规范：

1. 免竞争期间所传递的任何帧，必须将 Duration 位设定为 32768。此规范适用于免竞争期间所传递的任何数据帧。
2. 目的地为广播或组播地址的帧（Address 1 位设定了群组 bit），其持续时间为 0。此类帧并非基本交换过程的一部分，接收端也不会加以应答，因此竞争式介质访问可以在广播或组播数据帧结束后立即开始。NAV 在帧交换过程中是用来保护传输介质。既然广播或组播帧之后不会有来自链路层的应答，因此没有必要为后续帧锁住介质使用权。
3. 如果 Frame Control 位中的 More Fragments bit 为 0，表示该帧已无其余片段。最后的帧片段只须为本身的应答预订介质使用权，之后就可以恢复竞争式访问了。Duration 位会被设定为发送一个短帧间隔及片段应答所需要的时间。整个过程如图 4-2 所示。倒数第二个片段的 Duration 位，会为最后一个片段锁住介质使用权。

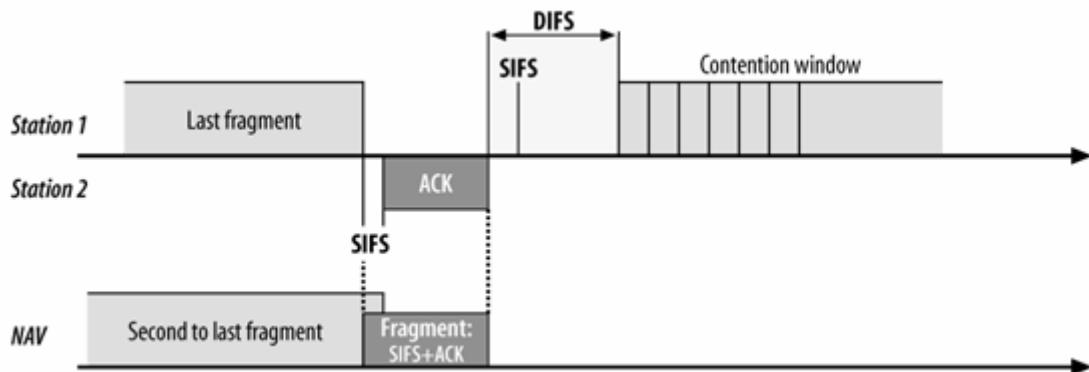


图 4-2：最终片段的 Duration 设定

4. 如果 Frame Control 位的 More Fragments bit 被设定为 1，表示其后还有帧片段。因此，Duration 位便会被设定为发送两个应答、加上三个短帧间隔及下一个帧片段所需要的时间。为非最终片段设定 NAN 的方式本质上与 RTS 相同，所以亦称为虚拟 RTS。

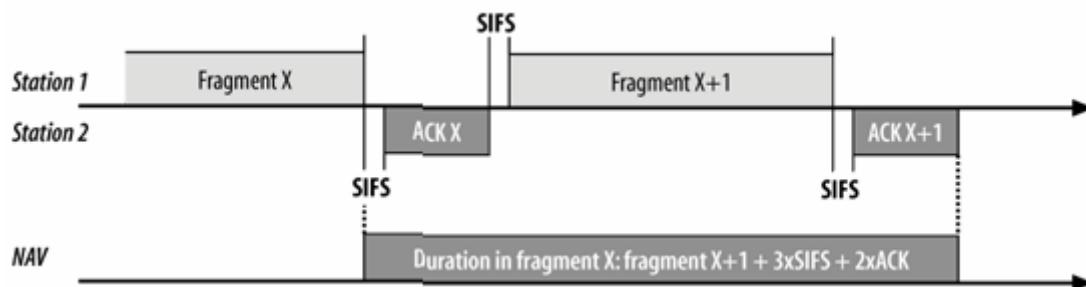


图 4-3：非最终片段的 Duration 设定

4.1.3 地址与 DS Bit

地址位的编号与功能取决于设定了哪个 DS (传输系统) bit, 因此所使用的网络类型会间接影响到地址位的用法。表 4-2 列出了地址位在数据帧中的各种用法。只有无线桥接器才会使用第四个地址位, 因此比较少见。

表 4-2: 地址位在数据帧中的用法

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	Not used
To AP (infra.)	1	0	BSSID	SA	DA	Not used
From AP (infra.)	0	1	DA	BSSID	SA	Not used
WDS (bridge)	1	1	RA	TA	DA	SA

Address 1 代表帧接收端的地址。在某些情况下, 接收端即为目的地, 但不然如此。目的地是指负责处理帧中网络层封包的工作站; 而接收端则是负责将无线电解码为 802.11 帧的工作站。如果 Address 1 被设为广播或组播地址, 则必须同时检查 BSSID (基本服务组合识别码)。工作站只会应答来自同一个基本服务组合 (basic service set, 简称 BSS) 的广播或组播信息; 至于来自其他不同 BSS 者则加以忽略。Address 2 是发送端的地址, 用来发送应答信息。发送端就是源地址。源地址是指产生帧中网络层协议封包的工作站; 而发送端则是负责将帧发送至无线链路。Address 3 位则是供基站与传输系统过滤之用, 不过该位的用法, 取决于所使用的网络类型。

由于 IBSS 并未使用基站, 因此不会涉及传输系统。发送端即为帧的源, 而接收端即为帧的目的地。每个帧都会记载 BSSID, 因此工作站可以检查广播与组播信息。只有隶属同一个 BSS 的工作站, 才会处理该广播或组播信息。在 IBSS 中, BSSID 是由随机数产生器随机产生的。

BSSID

每个 BSS 都会被赋予一个 BSSID, 它是一个长度为 48 个 bit 的二进制识别码, 用来辨识不同的 BSS。BSSID 的主要优点是, 它可作为过滤之用。虽然不同的 802.11 网络彼此间可能重叠, 但即使如此也不应该让相互重叠的网络路收到彼此的链路层广播。

在 infrastructure BSS (基础型基本服务组合) 中, BSSID 就是建立该 BSS 的基站上无线介面的 MAC 地址。而 IBSS (独立型基本服务组合) 则必须建立 BSSID。方能产生网络。为了让所建立的地址尽量不致重复, BSSID 有 46 个 bit 是随机产生的。其所产生的 BSSID,

会将 Universal/Local bit 设定为 1，代表这是一个区域地址，至于 vidual/Group bit 则会设定为 0。两个不同的 IBSS，如果要产生相同的 BSSID，它们所产生的 46bit 数必须完全相同。

有一个 BSSID 会被保留不用，就是所有 bit 均设定为 1 的 BSSID，又称为广播型 BSSID。使用广播型 BSSID 的帧，可以不被 MAC 中任何的 BSSID filter 所过滤。BSSID 的广播只有在移动式工作站送出 probe request（检测要求），试图找出有哪些网络可以加入时才会用到。probe 帧要能够检测现存的网络，就不能被 BSSID filter 过滤掉 probe 帧是惟一允许使用广播型 BSSID 的帧。

802.11 对源与发送端以及目的地与接收端有明确的区分。将帧送至无线介质的发送端，不见得就是帧的产生者。目的地址与接收端地址同样有此区别。接收端可能只是中介目的地，而帧只有到达目的地，才会由较上层的协议加以处理。

图 4-4 展示了一个简单的网络，其中有某个无线用户端通过 **802.11** 网络连接至服务器。用客户端将帧发送给服务器时，地址位的用法如表 4-2 第二列所示。

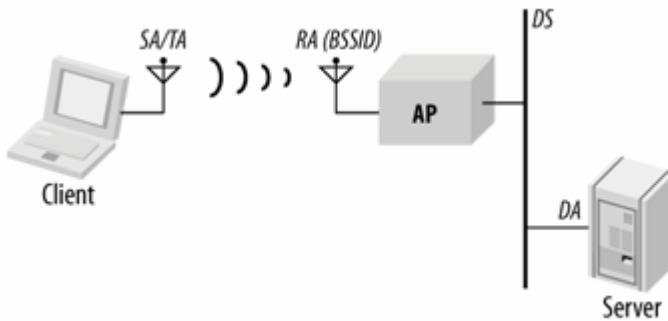


图 4-4：将帧发送至服务器时，地址位的用法

如果帧的目的地位于传输系统，则用户端既是源亦是发送端。至于无线帧的接收端则是基站，不过该基站只是个中介目的地。当帧送到基站时，该帧会经传输系统转送给服务器。因此，基站是接收端，而服务器才是最后的目的地。在基础网络里，基站会以其无线界面的地址建立相应的 BSS，这就是为什么接收端地址（Address 1）会被设定为 BSSID 的原因。

当服务器应答用户端时，帧会通过基站发送给用户端，如图 4-5 所示。这种情况相当于表 4-2 的第三列。

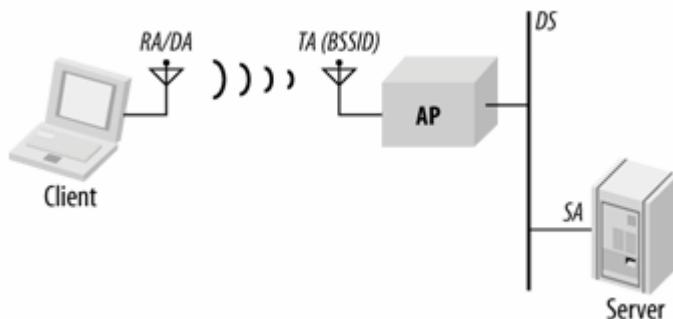


图 4-5: 帧来自传输系统时, 地址位的用法

由于帧产生自服务器, 所以服务器的 MAC 地址即为该帧的来源地址 (简称 SA)。当帧通过基站转送出去时, 基站将会以自己的无线介面做为发送端地址 (简称 TA)。如同前一个例子, 基站的介面地址就是 BSSID。帧最后会被送至用户端, 此时用户端既是目的地又是接收端。

表 4-2 的第四列展示了地址位在无线传输系统 (wireless distribution system 简称 WDS) 中的用法。无线传输系统有时也称为无线桥接器。如图 4-6 所示, 两条有线网络通过扮演无线桥接器角色的基站彼此相连。从用户端送至服务器的帧会经过 802.11 WDS。该无线帧的源与目的地址, 依然对应到用户端与服务器的地址。不过, 这些帧还是会区分无线介质上帧的发送端与接收端。对于由用户端送至服务器的帧而言, 发送端就是用户端这边的基站, 而接收端就是服务器这边的基站。将来源地与发送端分开的好处是, 当服务器这边的基站送出必要的 802.11 应答给对方基站时, 不会干扰到有线链路层。

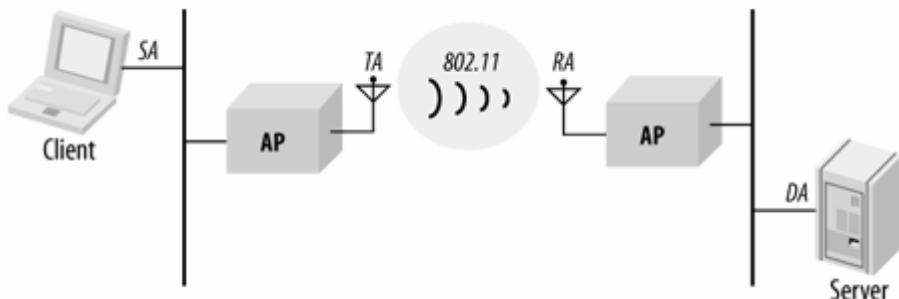


图 4-6: 无线传输系统

4.1.4 数据帧的次类型

802.11 具有数种不同类型的数据帧。要使用何种帧, 取决于服务是属于竞争式或免竞争式服务。基于效率上的考虑, 免竞争帧中可以加入其他功能。只要改变帧的次类型, 免竞争期间的数据帧即可用来应答其他帧, 由此便可省去帧间隔以及一一应答所带来的负担。以下是常见的数据帧次类型:

- Data (数据)

次类型为 Data 的帧, 只有在竞争访问期间才会传输。这类简单的帧只有一个目的, 亦即在工作站间发送帧主体。

- Null (空)

Null 帧看起来有点奇怪。它是由 MAC 标头与 FCS 标尾所组成。在传统的以太网中，Null 帧无非就是额外的负担；在 802.11 网络中，移动工作站会利用 Null 帧来通知基站省电状态的改变。当工作站进入休眠状态，基站必须开始为之暂存帧。如果该移动式工作站没有数据要通过传输系统传输，也可以使用 Null 帧，同时将 Frame Control (帧控制) 位的 Power Management (电源管理) bit 设定为 1。基站不可能进入省电模式，因此不会发送 Null 帧。Null 帧的用法，如图平 7 所示。

此外尚有一些在免竞争期间使用的帧类型。不过，免竞争服务在实际上并不常见，相关帧 (Data+CF-Ack 、 Data+CF-Poll 、 Data+CF-Ack+CF-Poll) 以及 CF-Ack 、 CF-Poll 以及 CF-Ack+CF-Poll 的讨论，详见第九章。

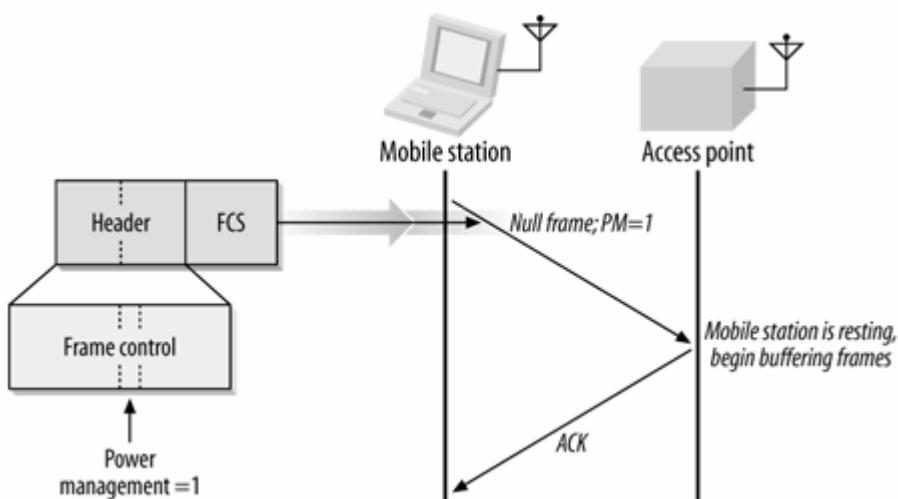


图 4-7：次类型为 Null 的数据帧

4.1.5 数据帧的封装

数据帧的形式取决于网络的形式。帧究竟属于哪种类型，完全取决于 subtype (次类型) 位，而与其他位是否出现在帧中无关。

4.1.5.1 IBSS 帧

在 IBSS 中，所使用的 address 位有三种，如图 4-8 所示。第一个地址代表接收端，同时也是 IBSS 网络中的目的地址。第二个地址是源地址。在这些地址之后，伴随而来的是 IBSS 的 BSSID。当无线 MAC 收到一个帧时，首先会去检查 BSSID，只有 BSSID 与工作站相同的帧，才会交由上层协议加以处理。

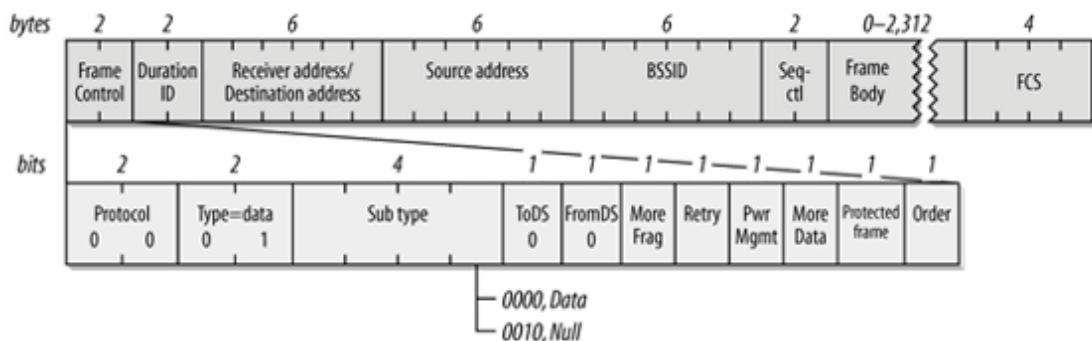


图 4-8: IBSS 数据帧

IBSS 数据帧的次类型不是 **data** 就是 **Null**; 后者只是用来告知目前的电源管理状态。

4.1.5.2 发送自基站 (From AP) 的帧

图 4-9 显示了由基站发送给移动工作站的帧格式。和所有数据帧一样，第一个位代表无线网络中接收该帧的接收端，亦即该帧的目的地。第二个位存放了发送端的地址。在基础网络中，发送端地址即为基站 (AP) 上无线介面的地址，同时也是 BSSID。最后，该帧会记载帧的源 MAC 地址。区分源与发送端所以必要，是因为 802.11 MAC 会将应答送给帧的 Transmitter(发送端 AP)，而较上层的协议会将应答送给帧的 source (来源地)。

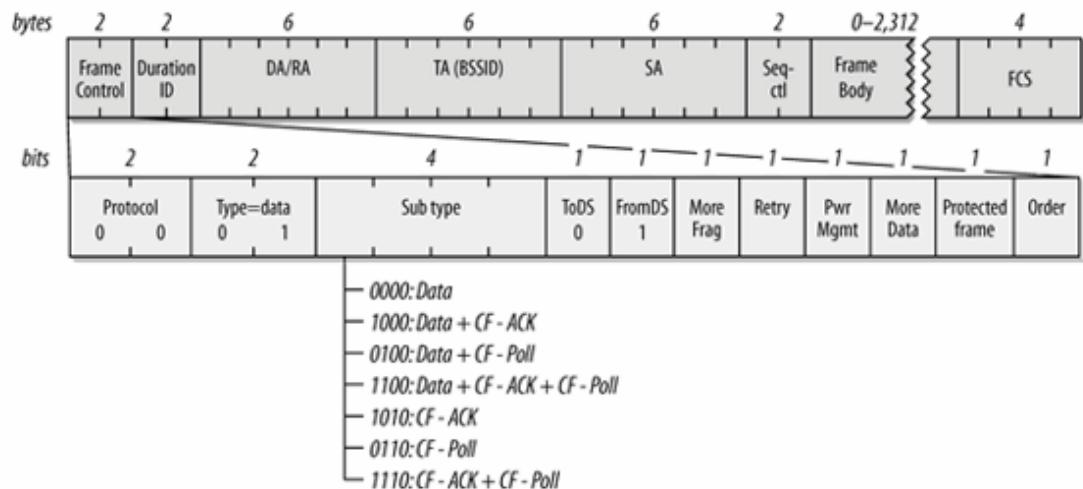


图 4-9: 发送自基站的数据帧

在 802.11 的规格书中并未明文禁止基站发送 Null 帧，不过这么做并没有任何意义。因为基站禁止使用省电程序，所以基站只会应答来自工作站的 Null 帧，而不会在应答中使用 Null 帧。实际上，在竞争式访问期间，基站会使用 Data 帧，而在免竞争期间则是使用包含 CF-Poll 功能的帧。

4.1.5.3 发送至基站 (To AP) 的帧

图 4-10 显示了，在 infrastructure（基础型）网络里，移动工作站发送给所连接基站的帧格式。接收端地址 (RA) 为 BSSID。在基础网络里，BSSID 即为基站的 MAC 地址。送至基站的帧，其源 / 发送端地址 (SA/TA) 得自无线工作站的网络介面。基站并未进行地址过滤的动作，而是使用第三个地址(DA)，将数据转送至位于传输系统的适当位置。

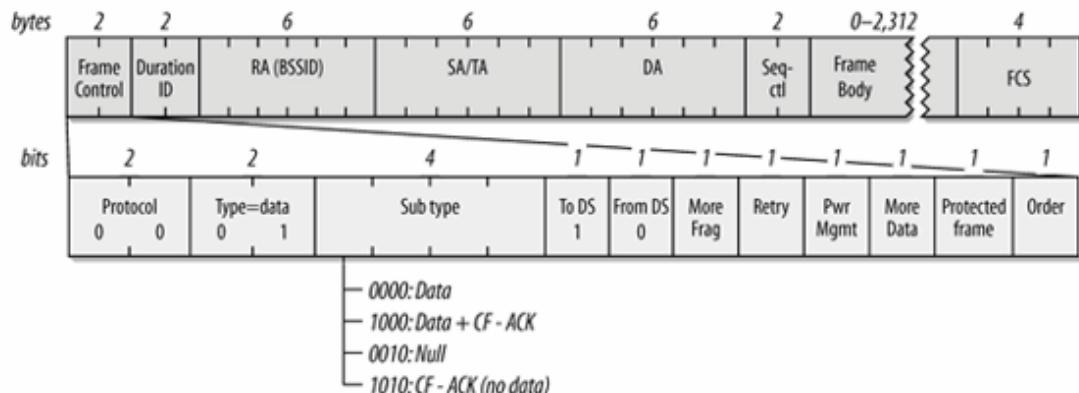


图 4-10：发送至基站的数据帧

发送至传输系统 (Ds) 的帧其 ToDS bit 会被设定为 1，而 FromDS bit 会被设定为 0。在基础网络中，移动工作站不能扮演中枢协调者 (point coordinator) 的角色，因此不能发送含有 CF-Poll (免竞争一轮询) 功能的帧。

4.1.5.4 WDS 中的帧

当基站被部署成无线桥接器 (或者 VUDS) 时，就会用到四个地址位，如图 4-11 所示。和其他数据帧一样，WDS 帧会使用第一个地址 (RA) 代表 receiver (接收端)，第二个地址 (TA) 代表 Transmitter (发送端) MAC 层会使用这两个地址送出应答以及控制流量，例如 RTS、CTS 以及 ACK 帧。另外两个地址位 (SA 与 DA) 则是用来记载帧的 source (源) 以及 destination (目的) 地址，并且将之与无线链路所使用的地址区别开来。

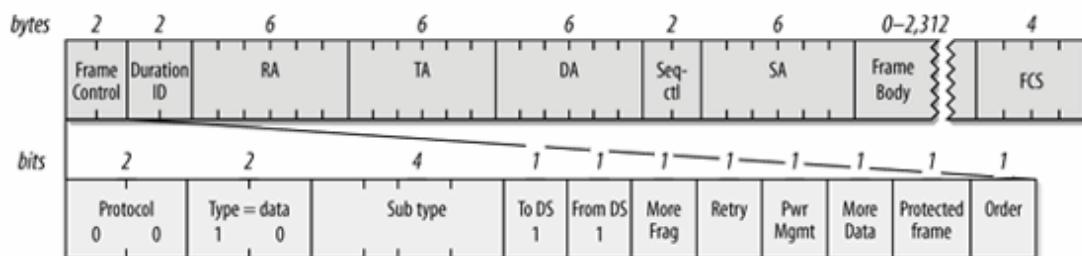


图 4-11：WDS 帧

在无线桥接链路中，通常不会存在移动工作站，也不会使用免竞争期间。基站禁止进入省电模式，因此 power management (电源管理) bit 必然设定为 0。

4.1.5.5 经加密的帧

受到链路层安全协议保护的帧并不算新的帧类型。当帧经过加密处理，Frames Control（帧控制）位的 Protected Frame bit 会被设定为 1，至于帧主体，则是以第五或第七章所描述的加密标头起头，这取决于所使用的何种协议。

4.2 控制帧

控制帧主要在协助数据帧的传递。它们可用来监督无线介质的访问（但非介质本身），以及提供 MAC 层次的可靠性。

4.2.1 一般的帧控制位

所有控制帧均使用相同的 Frame Control（帧控制）位，如图 4-12 所示。

bits	2	2	4	1	1	1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	10	11
Protocol	Type = control		Sub type	ToDS	FromDS	More Frag	Retry	Pwr Mgmt	More data	Protected Frame	Order
0	0	1	0	0	0	0	0	0	0	0	0

图 4-12：控制帧中的 Frame Control 位

- Protocol（协议版本）

在图 4-12 中，协议版本的值为 0，因为这是目前绝无仅有的版本。未来可能会出其他新的版本。

- Type（类型）

控制帧的类型识别码为 01。定义上，所有控制帧均使用此识别码。

- Subtype（次类型）

此位代表发送控制帧的次类型。

- ToDS 与 FromDS bit

控制帧负责处理无线介质的访问，因此只能由无线工作站产生。传输系统并不会收送控制帧，因此这两个 bit 必然为 0。

- More Fragments（尚有片段）bit

控制帧不可能被切割，这个 bit 必然为 0。

- Retry（重试）bit

控制帧不像管理或数据帧那样，必须在序列中等候重送，因此这个 bit 必然为 0。

- Power Management（电源管理）bit

此 bit 用来指示、完成当前的帧交换过程后，发送端的电源管理状态。

- More Data（尚有数据）bit

More Data bit 只用于管理数据帧，在控制帧中此 bit 必然为 0。

- Protected Frame（受保护帧）bit

控制帧不会经过加密。因此对控制帧而言，Protected Frame bit 必然为 0。

Order (次序) bit

控制帧是基本帧交换程序 (atomic frame exchange operation) 的组成要件，因此必须依序发送。所以这个 bit 必然为 0。

4.2.2 RTS (请求发送)

RTS 帧可用来取得介质的控制权，以便传输「大型」帧。至于多大称之为大型：是由网卡驱动程式中的 RTS threshold (门限) 来定义。介质访问权只能保留给单点传播 (unicast) 帧使用，而广播 (broadcast) 与组播 (multicast) 帧只须发送便是了。RTS 帧的格式如图 4-13 所示。就和所有控制帧一样，RTS 帧只包含标头。帧主体中并未包含任何数据，标头之后即为 FCS (帧检查码)。

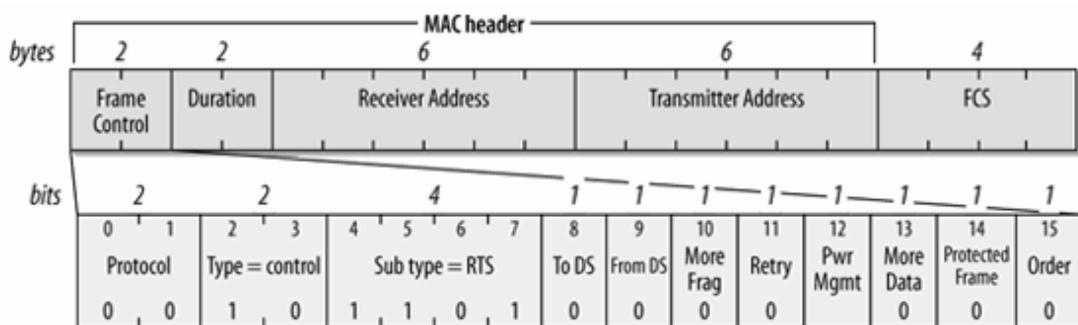


图 4-13: RTS 帧

RTS 的 MAC 标头由四个位构成：

- Frame Control (帧控制)

Frame Control 位并没有任何特殊之处。帧的 subtype (次类型) 位设定为 1011，代表 RTS 帧。除此之外，它与其他的控制帧具备相同位。（在 802.11 规格书中，最高效 bit 乃是最后一个 bit，因此在 subtype 位中，第 7 个 bit 代表最高效 bit。）

- Duration (持续时间)

RTS 帧会试图预定介质使用权，供帧交换程序使用，因此 RTS 帧发送者必须计算 RTS 帧结束后还需要多少时间。图 4-14 说明了整个交换过程，总共需要三个 SIFS、一个 CTS、最后的 ACK，加上发送第一个帧或帧片段所需要的时间。（fragmentation burst (片段宣泄期) 会使用后续的帧片段来更新 Duration 位。）传输所需要的微秒数经过计算后会置于 Duration 位。假使计算的结果不是整数，就会被修正为下一个整数微秒。

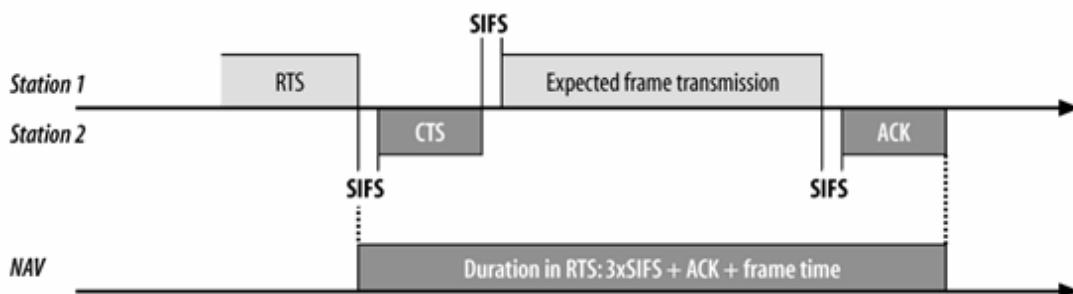


图 4-14: RTS 帧的 Duration 位

Address 1 位: Receiver Address (接收端地址)

接收大型帧的工作站的地址。

Address -2 位: Transmitter Address (发送端地址)

RTS 帧的发送端的地址。

4.2.3 CTS (允许发送)

CTS 帧有两种目的，其格式如图 4-15 所示。起初，CTS 帧仅用于应答 RTS 帧，如果之前没有 RTS 出现，就不会产生 CTS。后来，CTS 帧被 802.11g 防护机制用来避免干扰较旧的工作站。此防护机制和 802.11g 的其他数据，详见第十四章。

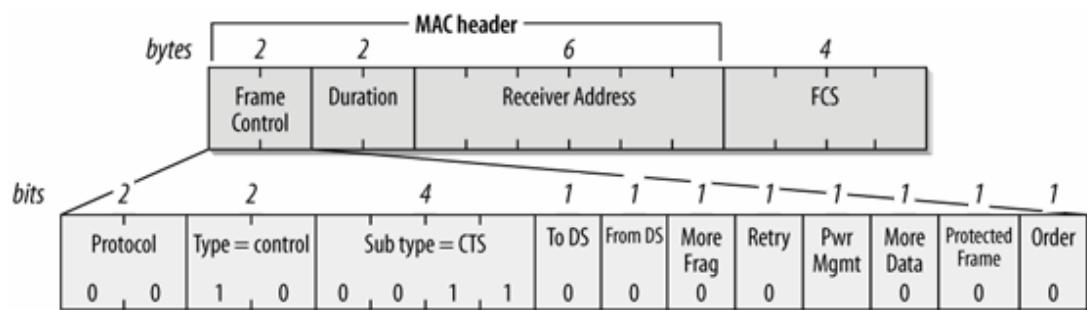


图 4-15: CTS 帧

CTS 帧的 MAC 标头由三个位构成:

- **Frame Control(帧控制)**

帧的 subtype (次类型) 位被设定为 1100，代表 CTS 帧。

- **Duration (持续时间)**

用来应答 RTS 时，CTS 帧的发送端会以 RTS 帧的 duration 值作为持续时间的计算基准。

RTS 会为整个 RTS-CTS-frame-ACK 交换过程预留介质使用时间。不过当 CTS 帧被发送出后，只剩下其他未帧或帧片段及其回应待传。CTS 帧发送端会将 RTS 帧的 duration 值减去发送 CTS 帧及其后短帧间隔所需的时间，然后将计算结果置于 CTS 的 Duration 位。图 4-16 显示了 CTS duration 与 RTS duration 的关系。用于防护交换 (protection exchanges) 时，CTS 帧所遵循的规则将留在防护机制一并讨论。

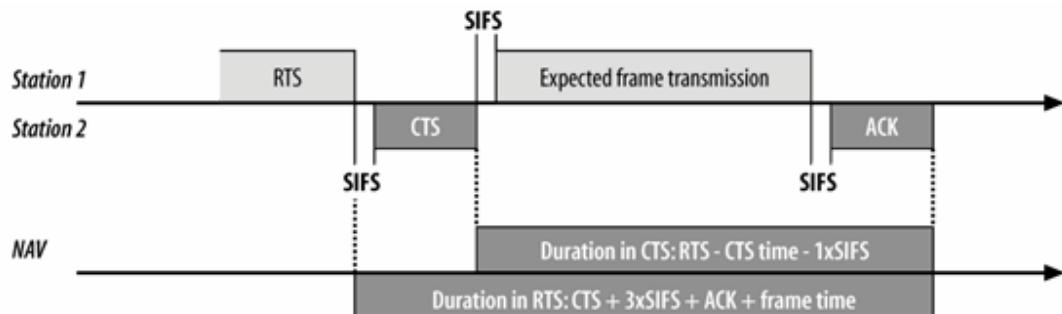


图 4-16 二 CTS 的持续时间

- Address 1 位: Receiver Address (接收端地址)

CTS 帧的接收端即为之前 RTS 帧的发送端，因此 MAC 会将 RTS 帧的发送端地址复制到 CTS 帧的接收端地址。802.118 防护作业所使用的 CTS 帧会被发送给发出 RTS 的工作站，而且只用来设定 NAV。

4.2.4 ACK (应答)

ACK 帧（图 4-17）就是 MAC 以及任何数据传输（包括一般传输 RTS/CTS 交换之前的帧、帧片段）所需要的正面应答（positive acknowledgment）。服务质量扩展功能放宽了个别数据帧必须各自得到应答的要求。欲评估应答机制对净传输量（net throughput）所造成的影响，详见第 25 章。

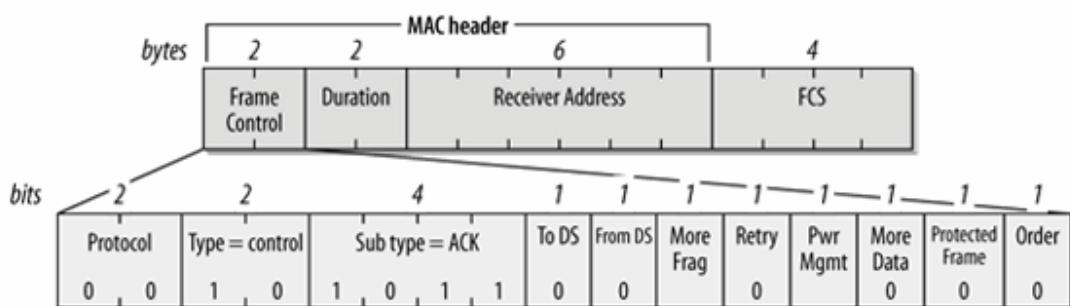


图 4-17: ACK 帧

ACK 帧的 MAC 标头由三个位构成：

- Frame Control (帧控制)
- 帧的 subtype (次类型) 位被设定为 1101，代表 ACK 帧。
- Duration (持续时间)

依照 ACK 信号在整个帧交换过程中位居何处，duration 的值可以有两种设定方式。在完整的数据帧及一连串帧片段的最后一个片段中，duration 会被设定为 0。数据发送端会将 Frame Control (帧控制) 位中的 More Fragments (尚有片段) bit 设定为 0，表示数据传输已经结束。如果 More Fragments bit 为 0，表示整个传输已经完成，没有必要再延长对无线信道的控制权，因此会将 duration 设定为 0。

如果 More Fragments bit 为 1，表示尚有帧片段仍在发送中。此时 Duration 位的用法和 CTS 帧中的 Duration 位相同。发送 ACK 以及短帧间隔所需要的时间，将由最近帧片段所记载的 duration 中减去。如果不是最后一个 ACK 帧，duration 的计算方式类似 CTS duration 的计算方式。事实上，802.11 的规格书将 ACK 帧中的 duration 设定称为虚拟 CTS。

- Address 1 位: Receiver Address (接收端地址)

接收端地址是由所要应答的发送端帧复制而来。技术上而言，它是由所要应答的 Address 2 位复制而来。应答主要是针对数据帧、管理帧以及 PS-Poll 帧。

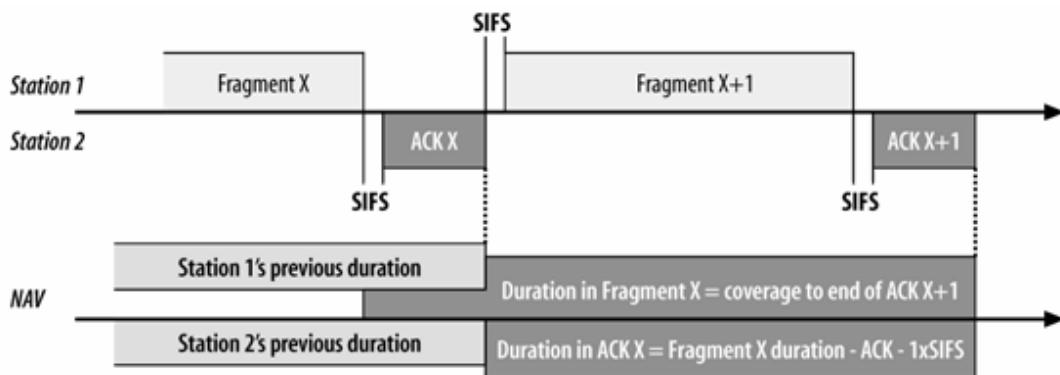


图 4-18: 非最终 ACK 帧的 Duration 位

4.2.5 PS-Poll (省电模式一轮询)

当一部移动工作站从省电模式中苏醒，便会发送一个 PS-Poll 帧给基站，以取得任何暂存帧。PS-Poll 帧的格式如图 4-19 所示。省电模式运作方式的进一步细节，详见第八章。

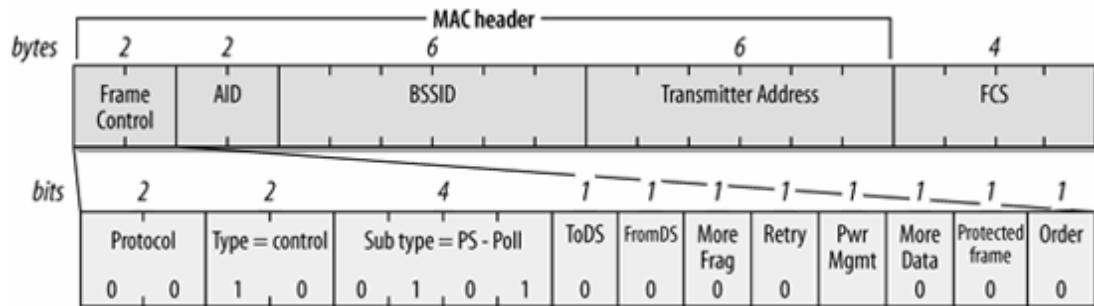


图 4-19: PS-Poll 帧

PS-Poll 帧的 MAC 标头由四个位构成：

- Frame Control (帧控制)

帧的 subtype (次类型) 位被设定为 1010，代表 PS-Poll 帧。

- AID (连接识别码)

PS-Poll 帧将会以 MAC 标头的第三与第四 bit 来代表连接识别码 (association ID)。连接识别码是基站所指定的一个数值，用以区别各个连接。将此识别码置入帧，可让基站找出为其 (移动工作站) 所暂存的帧。

- Address 1 位: BSSID

此位包含发送端目前所在 BSS 的 BSSID，此 BSS 建立自目前所连接的 AP。

- Address 2 位: Transmitter Address (发送端地址)

此为 PS-Poll 帧之发送端的 MAC 地址

在 PS-Poll 帧中并未包含 duration 信息，因此无法更新 NAV。不过，所有收到 Ps-Poll 帧的工作站，都会以短帧间隔加上发送 ACK 信号所需要的时间来更新 NAV。此一自动调整机制使得基站在发送 ACK 信号时，比较不会与移动基站发生碰撞。

【连接识别码（AID）在 PS-Poll 帧中，Duration/ID 位是连接识别码，而非虚拟载波侦测功能所使用的数值。当移动工作站与基站连接时，基站会从 1-2,007 范围内指派一个值来做为连接识别码（AID）。AID 的各种用法，见全书。】

4.3 管理帧

在 802.11 规格书中，管理所占据的篇幅最多。各式各样的管理帧，为的只是提供对有线网络而言相当简单的服务。对有线网络而言，识别一部工作站并非坏事，毕竟控制中心与工作站之间必须通过布线方能建立连接。有时候，集线器的插座面板可加速网络的构建，不过重点还是在于：建立新的连接时，可通过人员进行身份认证。

无线网络必须建立一些管理机制，方能提供类似的功能。802.11 将整个程序分解为三个步骤。寻求连接的移动工作站，首先必须找出可供访问的无线网络。在有线网络中，这个步骤相当于在墙上找出适当的插孔。其次，网络系统必须对移动工作站进行身份认证，才能决定是否让工作站与网络系统连接。在有线网络方面，身份认证是由网络系统本身提供。如果必须通过网线才能够取得信号，那么能够使用网线至少算得上是一种认证过程。最后，移动工作站必须与基站建立连接，这样才能访问有线网络，这相当于将网线插到有线网络系统。

4.3.1 管理帧的结构

802.11 管理帧的基本结构如图 4-20 所示。所有管理帧的 MAC 标头都一样，这与帧的次类型无关。管理帧会使用信息元素（带有数字标签的数据区块）来与其他系统交换数据。

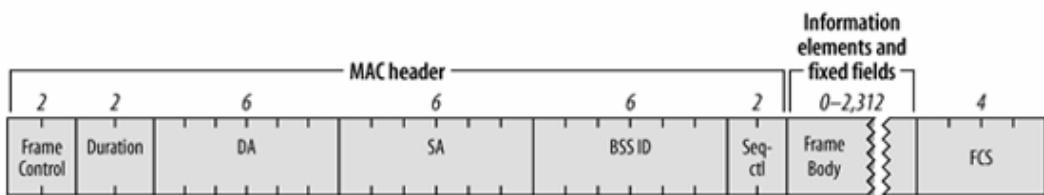


图 4-20：管理帧的基本结构

4.3.1.1 地址位

和其他帧一样，第一个地址位是给帧的目的地址使用的。有些管理帧主要用来维护个别 BSS 特有的属性。为了限制广播或组播管理帧所造成的副作用，收到管理帧之后，工作站必须加以验证，虽然不是所有实现均会进行这一 BSSID 过滤程序。只有在广播或组播帧来自工作站目前所连接的 BSSID，才会被送至 MAC 管理层。惟一的例外是 Beacon 帧，毕竟它是用来宣布 802.11 网络的存在。BSSID 是以大家所熟悉的方式来指定的。基站会以本身无线网络介面的 MAC 地址作为 BSSID。移动工作站会采纳目前所连接的基站的 BSSID。位于 IBSS 的工作站则会使用 BSS 建立之初随机产生的 BSSID。惟一的例外是：寻找特定网络的工作站，可以在所发出的帧中指定该特定网络的 BSSID，或者使用广播型 BSSID 来寻找邻近所有的网络。

4.3.1.2 计算持续时间

管理帧使用 Duration（持续时间）位的方式和其他帧没有两样：

1. 免竞争期间所发送的任何帧，均会将持续时间设为 32,768。
2. 竞争式访问期间，利用 DCF 所发送的帧会通过 Duration 位防止别人访问介质。确保基本帧交换程序得以完成。
 - a. 如果是广播或组播帧（目的地地址为群组地址），则持续时间会设定为 0。广播与组播帧无须得到应答，因此 NAV 无须防止别人访问介质。
 - b. 如果不是最终片段，则持续时间会设为三个 SIFS 期间加上下一个片段及其应答所需要的微秒数。
 - c. 最终帧片段的持续时间会设定为一个应答加上一个 SIFS 所需要的时间。

4.3.1.3 帧主体

管理帧十分具有弹性。帧主体中大部份的数据，如果使用长度固定的位，就称为固定式位；如果位长度不定，就称为信息元素（information element）。所谓信息元素，是指长度不定的数据区块。每个数据区块均会标注上类型编号与大小，各种信息元素的数据位都有特定的解释方式。新版的 802.11 规格书允许定义新的信息元素；根据旧版规格书所实现的产品可忽略这些新元素。实作上，硬件一般采取回溯相容（backward-compatible）原则，因此较旧的产品通常无法加入根据新标准所建立的网络。还好，新功能通常可以予以停用，以便兼容性。

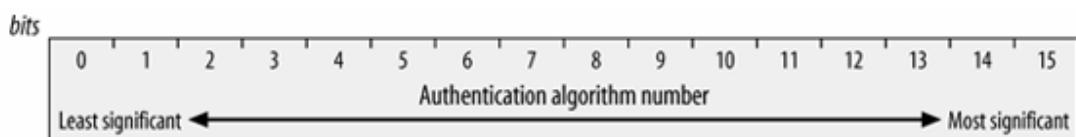
除了探讨这些作为基本元件的固定式与信息元素，本节还会说明这些基本元件如何构成管理帧。802.11 强制规定了这些信息元素的排列次序，不过并非所有元素均属于要。本书将以特定的顺序说明这些基本元件，论及各个次类型时，也会特别标明哪些元素比较少见，哪些元素彼此互不相容。

4.3.2 长度固定的管理帧元件

在管理帧中，可能出现的长度固定位有十种。长度固定的位一般简称为位，以便与长度不定的信息元素有所区别。位本身并无标头可与帧主体其他部份区别。因为长度与次序固定，因此不需要以位标头作为界定。

Authentication Algorithm Number 位

Authentication Algorithm Number（身份认证算法编号）位占用了两个字节，如图 4-21 所示。此位代表连接发生之前 802.11 层次（802.11-level）的最初认证程序所使用的认证类型（认证程序在第七章有更详尽的讨论）。此位值的允许范围列于表 4-3。目前只定义了两种值。其他值保留给未来版本使用。



4-21: Authentication Algorithm Number（身份认证演算法编号）位

表 4-3: Authentication Algorithm Number（身份认证算法编号）位的允许值

Value	Meaning
-------	---------

Value	Meaning
0	开放系统认证 Open System authentication (typically used with 802.1X authentication)
1	共享密钥认证 Shared Key authentication (deprecated by 802.11i)
2-65,535	保留 Reserved

Authentication Transaction Sequence Number 位

身份认证程序分为好几个步骤，其中包含由基站所发出的盘问口令（challenge），以及试图连接的移动工作站所做出的应答。如图 4-22 所示 Authentication Transaction Sequence Number（身份认证交易顺序编号）位是由两个字节所构成，用以追踪身份认证的进度。此位值介于 1 到 65,535 直接，其值不可为 0。这一位的用法将于第八章讨论。

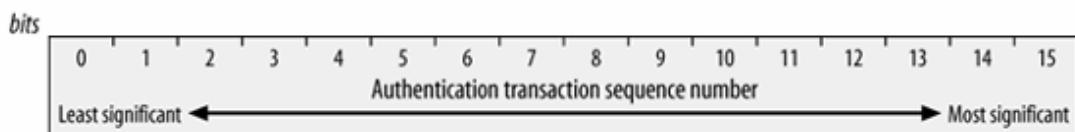


图 4-22: Authentication Transaction Sequence Number (身份认证交易顺序编号) 位

Beacon interval 位

每隔一段时间就会发出的 Beacon（信标）信号，用来宣布 802.11 网络的存在。Beacon 帧中除了包含 BSS 参数的信息，也包含基站暂存帧的信息，因此移动工作站必须仔细聆听 Beacons 信号。Beacon interval（信标间隔）位的长度有 16 个 bit，用来设定 Beacon 信号之间相隔多少时间单位。时间单位通常缩写为 TU，代表 1,024 微秒（microseconds），相当于一毫秒。有些文件中会以千一微秒（kilo-microseconds）〔注〕来表示时间单位。Beacon interval 位通常会被设定为 100 个时间单位，相当于每 100 毫秒或 0.1 秒发送一次 Beacon 信号。

〔注〕千一微秒（kilo-microseconds）是相当奇怪的组合，因为它以 2 的乘方来计算 Kilo，而以较为常见的 1/1000 来表示 micro。想必国际度量局可能会对这种用法提出抗议。

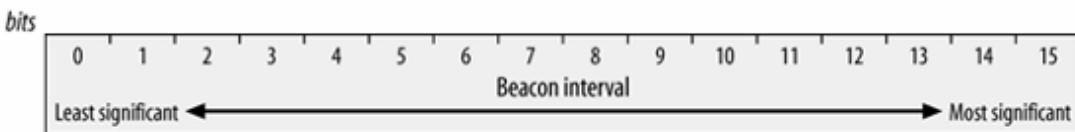


图 4-23: Beacon Interval (信标间隔) 寺闈位

Capability information 位

图 4-24 所示为长度 16 个 bit 的 Capability Information 性能信息位，发送 Beacon 信号的时候，它被用来通知各方，该网络具备哪种性能。Capability information 位也可以使用在 Probe Request 与 Probe Response 帧。在本位中，每个 bit 各自代表一个旗标，对应到网络所具备的某种特殊功能。工作站会使用这些公告数据来判断自己是否支持该 BSS 所有的功能。没有实现性能公告中所有功能的工作站，就无法加入该 BSS。

<i>bits</i>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	ESS	IBSS	CF-Pollable	CF-Poll request	Privacy	Short preamble (802.11b)	PBCC (802.11b)	Channel agility (802.11b)	Reserved	Short slot time	Reserved	Reserved	DSSS-OFDM	Reserved	Reserved	

图 4-24: Capability Information (性能信息) 位

- ESS/IBSS (扩展服务组合/独立型基本服务组合)

这两个 bit 旗标彼此互斥 (mutually exclusive)。基站会将 ESS 位设定为 1，而将 IBSS 位设定为 0，表示基站属于基础网络的一部分。IBSS 中的工作站则会将 ESS 位设定为 0，而将 IBSS 位设定为 1。

- Privacy (私响性)

将 Privacy bit 设定为 1，代表需要使用 WEP 以维持机密性。在基础网络中，发送端为基站。在 IBSS 里，Beacon 信号必须由 IBSS 当中某部工作站负责。

- short Preamble (短同步信号)

802.11b 规格新增此位的目的，是为了支持高速直接序列扩频物理层 (high-rate DSSS PHY)。将之设定为 1，代表此网络目前使用短同步信号 (short preamble)，对此第十章会有进一步的说明。0 代表不使用此选项，并且在该 BSS 中禁止使用短同步信号。802.11g 规定使用短同步信号，因此在依循 802.11g 标准所建置的网络中，此位必然设定为 1。

- PBCC (分组二进制卷积编码)

802.11b 规格新增此位的目的，是为了支持高速直接序列扩频物理层 (high-rate DSSS PHY)。将之设定为 1，代表此网络目前使用第十二章所描述的分组二进制卷积编码 (packet binary convolution coding) 调变机制，或是第十四章所描述的 802.11g PBCC 调变机制。0 代表不使用此选项，并且在该 BSS 中禁止使用分组二进制卷积编码。

- Channel Agility (机动信道转换)

这一位加入 802.11b 规格的目的，是为了支持高速直接序列扩频物理层 (high-rate DSSS PHY)。将之设定为 1，代表此网络使用机动信道转换 (Channel Agility) 选项，对此第十二章会有进一步的说明。0 代表不使用此选项，并且在该 BSS 中禁止使用机动信道转换。

- Short Slot Time (802.11g)

此 bit 若设定为 1，代表使用 802.11 所支持的较短的时槽，这将于第十四章讨论。

- DSSS-OFDM (802.11g)

此 bit 若设定为 1，代表使用 802.11g 的 DSSS-OFDM 帧构建 (frame construction) 选项。

- Contention-free polling (免竞争轮询) bit

工作站与基站使用这两个 bit(CF-Pollable 与 CF-Poll Request)当作标签。这些标签的意义如表 4-4 所示。

表 4-4: Capability Information (性能信息) 位中 polling bit 所代表的意义

CF-Pollable	CF-Poll Request	意义
工作站的用法		

0	0	工作站不支持轮询 (polling)
0	1	工作站支持轮询, 但并没有要求置于轮询表 (polling list)
1	0	工作站支持轮询, 且要求将之置于轮询表
1	1	工作站虽然支持轮询, 但要求不要对其轮询 (结果是该工作站会被视为不支持免竞争工作)
基站的用法		
0	0	基站并不支持中枢协调功能 (point coordination function)
0	1	基站使用 PCF 来传递, 但并不支持轮询
1	0	基站使用 PCF 来传递与轮询
1	1	保留, 未使用

Current AP Address 位

移动工作站可以使用图 4-25 所示的 Current AP Address (目前基站的地址) 位来表明目前所连接的基站的 MAC 地址。这个位的用途是便于连接 (association) 与重新连接 (reassociation) 的进行。工作站会借此发送上一次所连接的基站的地址。当工作站打算与不同的基站建立连接时, 此位可用来转换连接, 以及取回所有暂存的帧。

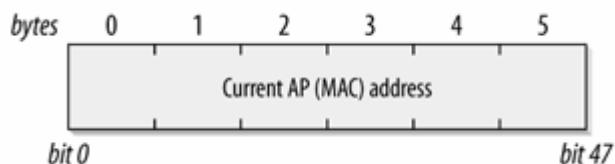
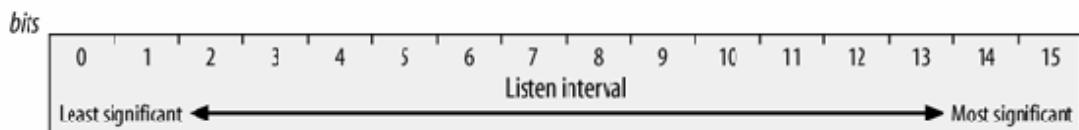


图 4-25: Current AP Address (目前基站的地址) 位

Listen interval 位

为了节省电池的电力, 工作站可以暂时关闭 802.11 网络介面的天线。当工作站处于休眠状态, 基站必须为之暂存帧。休眠中的工作站会定期醒来聆听往来信息, 以判断是否有帧暂存于基站。当工作站与基站连接时, 会将 Listen Interval (聆听间隔) 记录下来。所谓 Listen Interval, 其实就是以 Beacon interval (信标间隔) 为单位所计算出的休眠时间。图 4-26 所示的 Listen Interval, 让移动工作站得以要求基站必须为它暂存帧多久的时间。聆听间隔越久, 基站就必须使用更多记忆体来暂存帧。基站可以藉此项功能估计所需资源, 以决定是否拒绝资源密集 (resource-intensive) 的连接。第八章会进一步描述 Listen Interval。



4-26: Listen Interval (聆听间隔) 位

Association ID 位

图 4-27 所示为长度 16bit 的 Association ID (连接识别码) 位。当工作站与基站连接时, 就会被赋予一个连接识别码, 用以协助控制与管理功能。虽然连接识别码可用 bit 数为 14 个 bit,

不过只有 1-2007 可以使用。为了与 MAC 标头的 Duration/ID 位相容，最高效的两个 bit 均被设定为 1。

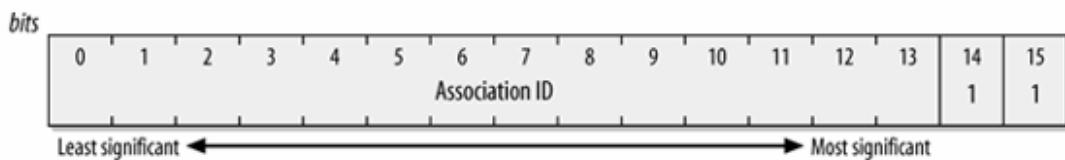


图 4-27: Association ID (连接识别码) 位

Timestamp 位

图 4-28 所显示的 Timestamp (时戳) 位，可用来同步 BSS 中的工作站 BSS 的主计时器会定期发送目前已作用的微秒数。当计数器到达最大值时，便会从头开始计数。(对一个长度 64bit、可计数超过 580,000 年的计数器而言，很难会遇到有从头开始计数的一天。)

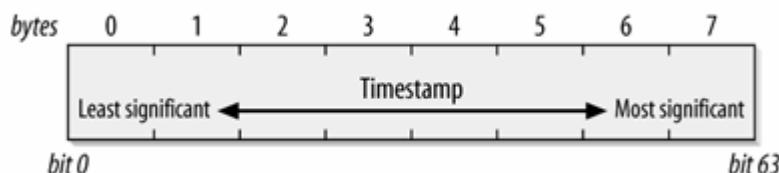


图 4-28: Timestamp (时戳) 位

Reason Code 位

当对方不适合加入网络时，工作站会送出 Disassociation (解除连接) 或 Deauthentication (解除身份认证) 帧作为应答。这些帧当中包含一个长度 16bit 的 Reason Code (原因代码) 位，表示对方的做法有误，如图 4-29 所示。表 4-5 列出了产生原因代码的理由。要完全了解原因代码的用法，必须对各种帧以及 802.11 工作站的状态有所了解。关于这一点，本节已有讨论。

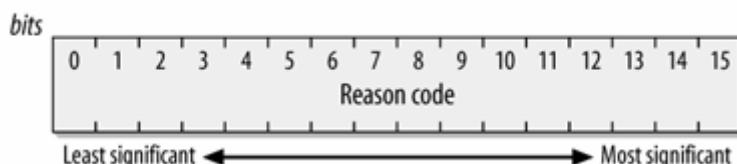


图 4-29: Reason Code (原因代码) 位

代码	含义
0	保留，未使用 (Reserved; unused)
1	未指定 (Unspecified)
2	之前的身份认证无效 (Prior authentication is not valid)
3	工作站已经离开基本服务区或扩展服务区，目前已经接触身份认证 (Station has left the basic service area or extended service area and is deauthenticated)
4	闲置计时器超时，且工作站已经解除连接 (Inactivity timer expired and station was disassociated)

代码	含义
5	基站资源不足，因此解除连接（Disassociated due to insufficient resources at the access point）
6	从尚未认证的工作站所收到的帧类型或次类型不正确（Incorrect frame type or subtype received from unauthenticated station）
7	从尚未连接的工作站所收到的帧类型或者次类型不正确（Incorrect frame type or subtype received from unassociated station）
8	工作站已经离开基本服务区或扩展服务区，目前已经解除连接（Station has left the basic service area or extended service area and is disassociated）
9	在身份认证完成之前要求连接或者重新连接（Association or reassociation requested before authentication is complete）
10 (802.11h)	无法接受 Power Capability 信息元素的设定值，因此解除连接 (Disassociated because of unacceptable values in Power Capability element)
11 (802.11h)	无法接受 Supported Channels 信息元素的设定值，因此解除连接 (Disassociated because of unacceptable values in Supported Channels element)
12	保留（Reserved）
13 (802.11i)	信息元素不正确(802.11i 所加入的原因代码, 因此应指 802.11i 的信息元素) Invalid information element (added with 802.11i, and likely one of the 802.11i information elements)
14 (802.11i)	数据完整性检验失败（Message integrity check failure）
15 (802.11i)	四道密钥磋商超时（4-way keying handshake timeout）
16 (802.11i)	群组密钥磋商超时（Group key handshake timeout）
17 (802.11i)	四道磋商信息元素的安全参数与原始参数组合不符（4-way handshake information element has different security parameters from initial parameter set）
18 (802.11i)	群组密码锁不正确（Invalid group cipher）
19 (802.11i)	成对密码锁不正确（Invalid pairwise cipher）
20 (802.11i)	身份认证与密钥管理协议不正确（Invalid Authentication and Key Management Protocol）
21 (802.11i)	未支持的固安网络信息元素版本（Unsupported Robust Security Network）

代码	含义
	Information Element (RSN IE) version)
22 (802.11i)	RSN IE 的性能项不正确 (Invalid capabilities in RSN information element)
23 (802.11i)	802.1X 身份认证失败 (802.1X authentication failure)
24 (802.11i)	所设定的使用政策拒绝所提议的密钥锁组 (Proposed cipher suite rejected due to configured policy)
25-65,535	保留, 未使用 (Reserved; unused)

Status Code 位

状态代码用来表示某项过程成功或失败。Status Code (状态代码) 位, 如图 4-30 所示。如果某项过程成功, 该位的值就会被设定为 0, 否则设为非零值。表 4-6 列出了标准的状态代码。

表 4-6: 状态代码

Code	Explanation
0	操作成功 (Operation completed successfully)
1	未指定失败原因 (Unspecified failure)
2-9	保留, 未使用 (Reserved; unused)
10	所要求的能力范围过广无法支持 (Requested capability set is too broad and cannot be supported)
11	拒绝重新连接; 之前的连接无法辨识与转移 (Reassociation denied; prior association cannot be identified and transferred)
12	拒绝重新连接, 原因不在 802.11 标准指定范围内 (Association denied for a reason not specified in the 802.11 standard)
13	不支持所使用的身份认证算法 (Requested authentication algorithm not supported)
14	超乎预期的身份认证序号 (Unexpected authentication sequence number)
15	身份认证被拒绝; 回应信息有误 (Authentication rejected; the response to the challenge failed)
16	身份认证被拒绝; 下一个帧并未出现在预定的期间 (Authentication rejected; the next frame in the sequence did not arrive in the expected window)
17	连接被拒绝; 基站资源有限 (Association denied; the access point is resource-constrained)
18	连接被拒绝; 工作站并未支持 BSS 要求的所有数据传输速率 (Association

Code	Explanation
	denied; the mobile station does not support all of the data rates required by the BSS)
19 (802.11b)	连接被拒绝; 工作站并未支持 Short Preamble 功能 (Association denied; the mobile station does not support the Short Preamble option)
20 (802.11b)	连接被拒绝; 工作站并未支持 PBCC 调制技术 (Association denied; the mobile station does not support the PBCC modulation option)
21 (802.11b)	连接被拒绝; 工作站并未支持 Channel Agility 功能 (Association denied; the mobile station does not support the Channel Agility option)
22 (802.11h)	连接被拒绝; 需要 Spectrum Management 功能 (Association denied; Spectrum Management is required)
23 (802.11h)	连接被拒绝; 不接受 Power Capability (Association denied; Power Capability value is not acceptable)
24 (802.11h)	连接被拒绝; 不接受 Supported Channels (Association denied; Supported Channels is not acceptable)
25 (802.11g)	连接被拒绝; 工作站并未支持 Short slot Time 功能 (Association denied; the mobile station does not support the Short Slot Time)
26 (802.11g)	连接被拒绝; 工作站并未支持 DSSS-OFDM 功能 (Association denied; the mobile station does not support DSSS-OFDM)
27-39	保留 (Reserved)
40 (802.11i)	信息元素不正确 (Information element not valid)
41 (802.11i)	群组 (广播/组播) 密码锁不正确 (Group (broadcast/multicast) cipher not valid)
42 (802.11i)	成对 (单点传播) 密码锁不正确 (Pairwise (unicast) cipher not valid)
43 (802.11i)	身份认证与密钥管理协议不正确 (Authentication and Key Management Protocol (AKMP) not valid)
44 (802.11i)	未支持的固安网络信息元素版本 (Robust Security Network information element (RSN IE) version is not supported)
45 (802.11i)	不支持 RSN IE 性能 (RSN IE capabilites are not supported)
46 (802.11i)	密码锁组被使用政策拒绝 (Cipher suite rejected due to policy)
47-65,535	保留给未来的标准使用 (Reserved for future standardization work)

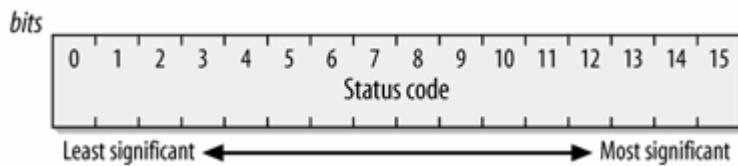


图 4-30: Status Code (状态代码) 位

4.3.3 管理帧的信息元素

信息元素 (information element) 是管理帧的组成元件，其长度不定。信息元素通常包含一个 Element ID (元素识别码) 位、一个 Length (长度) 位以及一个长度不定的位，如图 4-31 所示。Element ID 编号的标准值如表 4-7 所示。

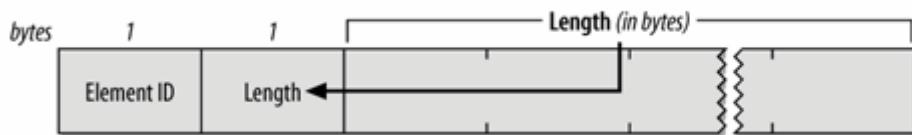


图 4-31: 一般管理帧的信息元素

表 4-7: 信息元素

Element ID	Name
0	服务集标识 (Service Set Identity (SSID))
1	所支持的速率 (Supported Rates)
2	跳频参数集合 (FH Parameter Set)
3	直接序列参数集合 (DS Parameter Set)
4	免竞争参数集合 (CF Parameter Set)
5	数据待传信息 (Traffic Indication Map (TIM))
6	IBSS 参数集合 (IBSS Parameter Set)
7 (802.11d)	国家 (Country)
8 (802.11d)	跳频模式参数 (Hopping Pattern Parameters)
9 (802.11d)	跳频模式表 (Hopping Pattern Table)
10 (802.11d)	请求 (Request)
11-15	保留; 未使用 (Reserved; unused)
16	盘查口令 (Challenge text)
17-31	保留【注 a】(在 802.11 共享密钥身份认证停用之前，保留给盘查口令未来扩充用) Reserved (formerly for challenge text extension, before 802.11 shared key authentication was discontinued)



Element ID	Name
32 (802.11h)	功率限制 (Power Constraint)
33 (802.11h)	功率性能 (Power Capability)
34 (802.11h)	发射功率控制请求 (Transmit Power Control (TPC) Request)
35 (802.11h)	发射功率控制报告 (TPC Report)
36 (802.11h)	所支持的信道 (Supported Channels)
37 (802.11h)	信道切换宣告 (Channel Switch Announcement)
38 (802.11h)	测量请求 (Measurement Request)
39 (802.11h)	测量报告 (Measurement Report)
40 (802.11h)	禁声 (Quiet)
41 (802.11h)	IBSS 动态选频 (IBSS DFS)
42 (802.11g)	ERP 信息 (ERP information)
43-49	保留 (Reserved)
48 (802.11i)	固安网络 (Robust Security Network)
50 (802.11g)	扩展支持速率 (Extended Supported Rates)
32-255	保留; 未使用 (Reserved; unused)
221 【注 b】	Wi-Fi 访问保护 (Wi-Fi Protected Access)

【注 a】 由于不再建议使用 802.11 共享密钥身份认证, 因此为了应该不会用到这个位 (802.11 shared key authentication is no longer recommended, so it is unlikely that these fields will ever be used.)

【注 b】 此为 WPA 所使用的信息元素, 并不属于 802.11 官方版本的内容。不过这项功能在实现上十分常见, 因此我将它列在此表。 (This is used by WPA, and is not an official part of 802.11. However, it is widely implemented, so I include it in the table.)

4.3.3.1 服务集标识 (Service Set Identity (SSID))

网络管理人员通常比较喜欢跟文字、数字或名称打交道，而不是 48 个 bit 的 MAC 地址。广义的 802.11 网络不是扩展式服务组合（extended service set），就是独立型基本服务组合（independent BSS）。如图 4-32 所示的 SSID，让网管人员为服务组合(service set)指定识别码。试图加入网络的工作站可以扫描目前区域所有网络，然后以特定的 SSID 加入。共同组成扩展式服务区域（extended service area）的所有基本服务区域（basic service areas）都会使用相同的 SSID。

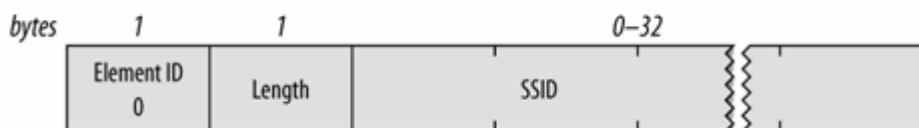


图 4-32: SSID (服务组合识别码) 信息元素

有些文件将 SSID 视为网络名称，因为网管人员通常以字串来指定 SSID。其实，SSID 不过是由字节所形成的字串，用来标示所属网络的 BSSID。有些产品要求此字串必须是以 null (即 0) 结尾的 ASCII 字串，虽然标准对此并无特别规范。

SSID 的长度介于 0 至 32 字节之间。如果完全不加指定，此种特例称为 broadcast SSID；broadcast SSID 只用于 Probe Request 帧，工作站可以藉此找出该区域中所有的 802.11 网络。

4.3.3.2 支持速率 (Supported Rates)

无线局域网络支持数种标准速率。802.11 网络可以使用 Supported Rates (所支持的速率) 信息元素指定其所支持的速率。当移动工作站试图加入网络，会先检视该网络所使用的数据速率。有些速率是强制性的，每部工作站都必须支持，有些则是选择性的。

Supported Rates 信息元素如图 4-33 所示。它是由一串字节所构成。每个字节会使用七个低效 bit 来代表数据速率；最高效 bit 则是用来表示该数据速率是否为强制性。如果是强制性速率，最高效 bit 为 1；非强制性速率则为 0。此信息元素最多可涵括八种速率。随着各种数据速率的增加，目前已将 Extended Supported Rates (扩展支持速率) 元素标准化，以便处理八种以上的速率。

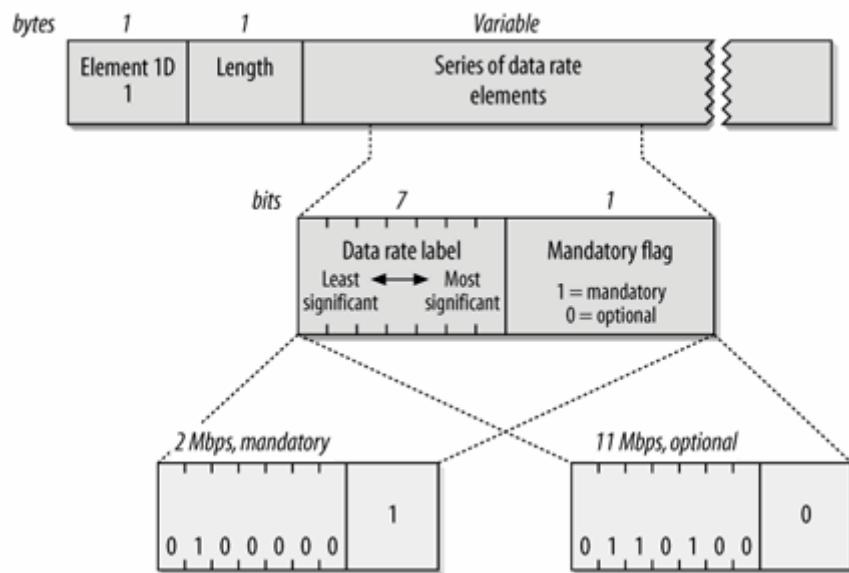


图 4-33: Supported Rates (所支持的速率) 信息元素

在 802.11 规格书最初的版本中，是以这七个 bit 对数据速率进行编码，而数据速率为 500 kbps 的倍数。新的技术，特别是 ETSI 的 HIPERLAN，必须以不同的方式来解读。当这七个 bit 用来编码数据速率时，每种编码均为 500 kbps 的倍数，那么可编码的最高数据速率为 63.5 Mbps。无线网络的进展，使得这个速率在不久的将来即可实现。因此，IEEE 在 802.11b 中改用简单的标记来代表所支持的速率。先前已经标准化的速率，则根据 500 kbps 倍数予以标记，不过未来的标准可能会有所更动。目前使用的标准值如表 4_8 所示。

表 4_8: 数据速率标记

二进制数值	响应的速率 (Corresponding rate (Mbps))
2	1 Mbps
4	2 Mbps
11 (802.11b)	5.5 Mbps
12 (802.11g)	6 Mbps
18 (802.11g)	9 Mbps
22 (802.11b)	11 Mbps
24 (802.11g)	12 Mbps
36 (802.11g)	18 Mbps
44 (802.11g)	22 Mbps (802.11g PBCC 选项 optional 802.11g PBCC)
48 (802.11g)	24 Mbps
66 (802.11g)	33 Mbps (802.11g PBCC 选项 optional 802.11g PBCC)
72 (802.11g)	36 Mbps
96 (802.11g)	48 Mbps

二进制数值**响应的速率 (Corresponding rate (Mbps))**

108 (802.11g) 54 Mbps

图 4-33 显示了如何同时编码两种数据速率。除了支持强制性的 2Mbps 服务，也支持选择性的 11Mbps 服务。

4.3.3.3 跳频参数组合 (PH Parameter Set)

跳频参数组合信息元素如图 4-34 所示，其中包含了加入 802.11 跳频 (frequency-hopping) 网络所需要的参数。

在 FH Parameter Set 中有四个特别针对 802.11 跳频式网络的位。对此第十二章会有更深入的描述。

<i>bytes</i>	1	1	2	1	1	1
	Element ID 2	Length 5	Dwell time	Hop Set	Hop Pattern	Hop Index

图 4-34: PH Parameter Set (跳频参数集合) 信息元素

Dwell Time (停留时间)

802.11 FH 网络会在信道与信道间跳跃。停留在每个信道上的时间为 dwell time (停留时间)。停留时间是以时间单位 (time units 简称 TUs) 来表示。

Hop Set (跳频组合)

802.11 跳频物理层定义了若干跳频模式 (hopping patterns)。此位的长度为一个字节，代表所使用的跳频模式组合。

Hop Pattern (调频模式)

工作站从跳频组合中挑出一种跳频模式。此位的长度亦为一个字节，代表所使用的跳频模式。

Hop Index (跳频索引)

每种跳频模式均包含一组跳频顺序。此位的长度为一个字节，代表目前位于跳频顺序的哪一点上。

4.3.3.4 直接序列参数集合 (DS Parameter Set)

802.11 直接序列 (Direct-sequence) 网络只有一个参数：网络所使用的信道数。高速直接序列网络使用相同的信道，因此可以使用相同的参数集合。信道数以一个字节进行编码，如图 4-35 所示。

<i>bytes</i>	1	1	1
	Element ID 3	Length 1	Current channel

图 4-35: DS Parameter Set (直接序列参数集合) 信息元素

4.3.3.5 数据待传信息 (Traffic Indication Map (TIM))

基站会为处于休眠状态的工作站暂存帧。每隔一段时间，基站就会尝试传递这些暂存帧给休眠中的工作站。如此安排的理由是，启动发送器比启动接收器所耗费的电力还要多。**802.11** 的设计者预见未来将会有以电池供电的移动工作站；定期发送暂存帧给工作站的这个决定，主要是为了延长设备的电池使用时间。将 **TIM**（数据待传指示信息）信息元素送到网络上，指示有哪些工作站需要接收待传数据，只是此过程的一部分。

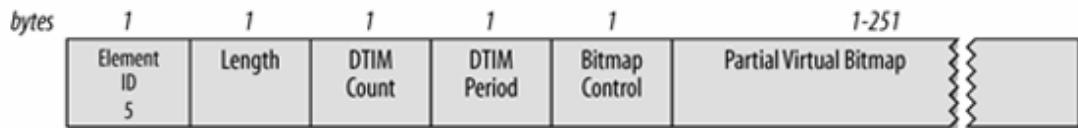


图 4-36: Traffic Indication Map (数据待传指示信息) 信息元素

TIM 的内容是虚拟 bit 对映 (virtual bitmap)，这是由 2,008 个 bit 所组成的逻辑结构。每个 bit 分别对映到一个连接识别码 (Association ID)。当某个识别码有数据暂存时，相应的 bit 就会设成 1，否则会设成 0。

DTIM Count (DTIM 计数)

此位的长度为一个字节，代表下一个 **DTIM** (数据待传指示传递信息) 帧发送前，即将发送的 **Beacon** 帧数。**DTIM** 帧用来表示所暂存的广播与组播帧即将被发送。并非所有 **Beacon** 帧均为 **DTIM** 帧。

DTIM Period (DTIM 期闲)

此位的长度为一个字节，代表两个 **DTIM** 帧之间的 **Beacon interval** 数。0 值目前保留未用。**DTIM** 会由此期间倒数至 0。

Bitmap Control (bit 对映控制) 与 Partial Virtual Bitmap (部分虚拟 bit 对映)

Bitmap Control (bit 对映控制) 位可进一步划分为两个次位。Bit 0 用来表示连接识别码 0 的待传状态，主要是保留给组播使用。其他七个 bit 则是保留给 **Bitmap Offset** (bit 对映偏移) 次位使用。

为了节省频宽，可以通过 **Bitmap Offset** 次位，只发送一部分的虚拟 bit 对映。**Bitmap Offset** 是相对于虚拟 bit 对映的开头处。利用 **Bitmap Offset** 次位及 **Length** 位，802.11 工作站可以推断虚拟 bit 对映有哪些部分包括在内。

4.3.3.6 免竞争参数集合 (CF Parameter Set)

CF Parameter Set (免竞争参数组合) 信息元素出现在支持免竞争基站所发送的 **Beacon** 帧中。免竞争服务并非必要，因此留待第九章讨论。

4.3.3.7 IBSS 参数集合 (IBSS Parameter Set)

IBSS 目前只有一个参数，即 **ATIM window** (数据待传指示通知信息间隔期间)，如图 4-37 所示。此位只用于 **IBSS Beacon** 帧，用来表示 **IBSS** 中 **ATIM** 帧之间相隔时间单位数量。

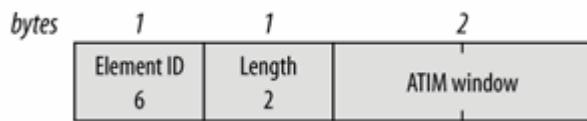


图 4-37: IBSS 参数集合信息元素

4.3.3.8 国家 (Country)

802.11 规格书原本是针对主要工业化国家现有的管制规定所设计。为了避免每新增一个国家就得重新修订规格，因此在规格书中加入新的规定，让网络能够提供管制规范给新加入的工作站。这一机制的核心，就是 Country 信息元素，如图 4-38 所示。

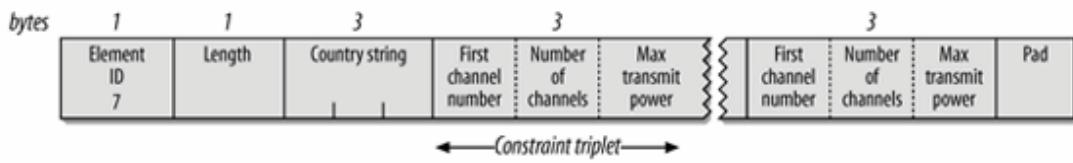


图 4-38: Country 信息元素

在 type/length 信息元素标头之后的是国家识别码（country identifier），之后是一系列由三个字节所构成的限制描述符（three-byte descriptor）。每组限制描述均注明特定频段，它们彼此不会重覆，因为每个特定频率只会有一个最大允许功率。

Country String (国家字串, 三个字节)

由三个字符所构成的 ASCII 字串，代表工作站的使用国家。前两个字符即 ISO 国码（例如 US 代表美国）。有些国家对室内与室外有不同的管制规定，第三个字符即是用来区别两者。如果室内外的管制规定相同，第三个字符则为空白。如果只想指定室内或室外管制规定，可以分别将第三个字符设为 I 或 O。

First Channel Number (第一信道编号, 一个字节)

第一信道编号即是符合功率限制的最低信道。每种 PHY 所指定的信道编号将于适当的章节讨论。

Number of Channels (信道数, 一个字节)

符合功率限制的频段大小，是由信道数来指定。信道大小随 PHY 而有所不同。

Maximum Transmit Power (最大传输功率, 一个字节)

最大传输功率，以 dBm 为单位。

Pad (补零码, 一个字节; 可有可无)

信息元素所使用的字节必须刚好是偶数。如果信息元素的长度恰为奇数，就必须用一个字节补零。

4.3.3.9 Hopping Pattern Parameters (跳频模式参数) 与 Hopping Pattern Table (跳频模式表)

第十一章所描述的 802.11 跳频规格，是根据设计当时的管制规定所制定。这两个元素可以用来制定新的跳频模式，以便符合其他国家的管制规定。如此一来，若要采用不同的跳频物理层，就不需要进一步修订规格书了。

4.3.3.10 请求 (Request)

在 Probe Request 帧中，Request 信息元素（图 4-39）用来向网络查询特定的信息元素。Request 信息元素本身具备 type/length 标头，以及一连串所要查询的信息元素编号。

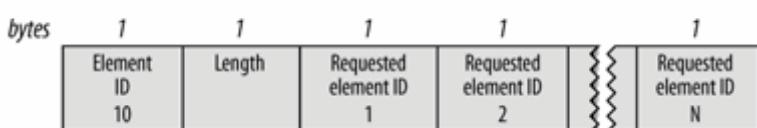


图 4-39: Request 信息元素

4.3.3.11 盘查口令 (Challenge Text)

802.11 所定义的共享密钥身份认证系统。会要求移动工作站必须成功解码一段加密过的盘问口令。这段盘问口令的发送系通过 Challenge Text (盘问口令) 信息元素，如图 4-40 所示。



图 4-40: Challenge Text (盘问口令) 信息元素

4.3.3.12 功率限制 (Power Constraint)

Power Constraint (功率限制) 信息元素让网络得以向工作站传达其所允许的最大传输功率。除了管制上的最大值，另外还有实际使用上的最大值。此信息元素只有一个位，长度为一个字节，其中所记录的整数值，乃是管制上的最大值减去实际使用上的最大值，以 dBm 为单位。例如，假设管制上允许的最大功率为 10 dBm，但是此信息元素值为 2，那么此工作站就会将本身的最大传输功率设为 8 dBm (图 4-41)。

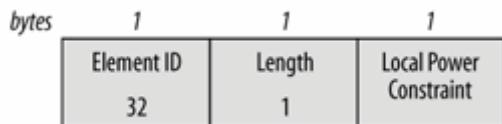


图 4-41: Power Constraint (功率限制) 信息元素

4.3.3.13 功率性能 (Power Capability)

802.11 工作站通常以电池供电，在无线电波的性能上无法与基站相提并论。另外部分原因是，移动工作站通常不需要像基站那样以高功率进行传输。Power Capability (功率性能) 信息元素让工作站得以报告本身最低与最高的传输功率，以 dBm 为单位 (图 4-42)。

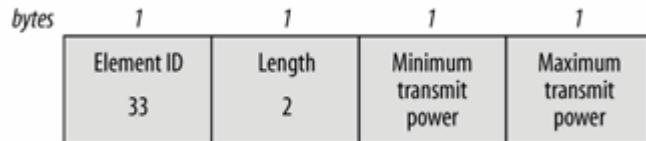


图 4-42: Power Capability (功率性能) 信息元素

4.3.3.14 发射功率控制要求 (TPC Request)

Transmit Power Control (发射功率控制，简称 TPC) Request 信息元素用来要求无线电波链路管理信息。此信息元素并无其他附属数据，因此长度位必然为 0 (图 4-43)。

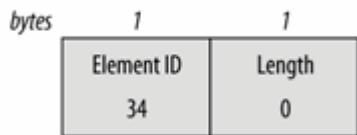


图 4-43: TPC Request 信息元素

4.3.3.15 发射功率控制报告 (TPC Report)

知道整个链路的衰减情况，可以帮助工作站了解该如何调整传输功率。TPC Report 信息元素散见于各种管理帧，由两个长度各为一字节的位所构成（图 4-44）。第一个位代表传输功率，亦即包含此信息元素帧的传输功率，以 dBm 为单位。第二个位代表链路边际(link margin)，亦即工作站所提出的安全边际值，同样以 dBm 为单位。工作站将会根据这两个值来调整本身的传输功率，就像第八章所说的那样。

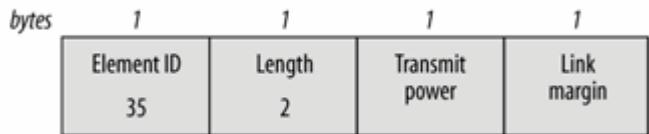


图 4-44: TPC Report 信息元素

4.3.3.16 所支持信道 (Supported Channels)

Supported Channels (所支持的信道) 信息元素与 **Country** 信息元素类似，用来记载所支持的子频段。在标头之后的是一系列子频段的描述符 (sub-band descriptor)。每组子频段描述符由第一信道编号，亦即所支持子频段中的最低信道，以及子频段的信道数所组成（图 4-45）。举例来说，如果装置只支持信道 40 至 52，那么第一信道编号即为 40，信道数则为 12。

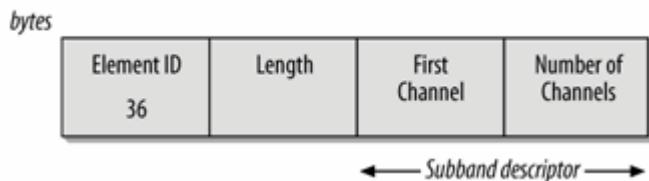


图 4-45: Supported Channels (所支持的信道) 信息元素

4.3.3.17 信道切换宣告 (Channel Switch Announcement)

802.11h 为网络加入了动态切换信道的能力。为了警告网络中的工作站即将变换信道，可以在管理帧中加入如图 4-46 所示的 **Channel Switch Announcement** (信道切换宣布) 信息元素。

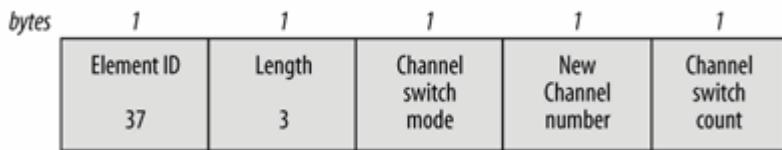


图 4-46: Channel Switch Announcement (信道切换宣布) 信息元素

Channel Switch Mode (信道切换模式)

当信道改变，通讯会突然中断。如果此位设定为 1，已连接的工作站就会停止发送帧，直到信道切换完成。如果设定为 0，则帧的发送就不受限制。

New Channel Number (新信道编号)

切换后的新信道编号。目前，此位的值尚不需要超过 255。

Channel Switch Count (信道切换计时)

信道切换可以预先排定时间。此位记载再过多少 Beacon 帧间隔后进行信道切换。信道切换会在发送 Beacon 帧之前进行。非 0 值代表等待多少个 Beacon 间隔；0 值代表信道切换可以立刻进行，无须多作警告。

4.3.3.18 Measurement Request (测量要求) 与 Measurement Report (测量报告) 信息元素

对于信道与功率设定的监控而言，定期进行信道测量十分重要。为了让工作站能够提出测量要求与接收测量报告，因此定义了这两种信息元素。测量报告属于 802.11h 的关键元件，将于 8.8 节（频谱管理）中详细探讨。

4.3.3.19 禁声 (Quiet)

开发动态选频的理由之一是为了避免与特定的军事雷达技术彼此干扰。要找出是否有雷达或其他干扰源存在，基站可以使用 Quite 信息元素，暂时关闭该信道，以改善测量的质量，如图 4-47 所示。

bytes	1	1	1	1	2	2
	Element ID	Length	Quiet count	Quiet period	Quiet duration	Quiet offset
	40	6				

图 4-47: Quiet 信息元素

在标头之后有四个位：

Quiet Count (禁声计时)

禁声期可以预先排定定时程。此位记载再过多少 Beacon 间隔后开始进入禁声期。它的运作方式类似 Channel Switch Count 位。

Quiet Period (禁声期)

禁声期也可以预先排定周期。如果此位值为 0，代表没有预先排定的禁声期。非 0 值代表每段禁声期间相距多少 Beacon 间隔。

Quiet Duration (禁声持续时间)

禁声期不见得要持续一整个 Beacon 间隔时间。此位用来指定禁声期打算持续多少个单位时间。

Quiet Offset (禁声偏移时间)

禁声期不见得始于某个 Beacon 间隔。此位用来指定 Beacon 间隔开始后经过多少单位时间后开始进入下一个禁声期。这个值必须小于 Beacon 间隔时间。

4.3.3.20 IBSS 动态选项 (IBSS DFS)

在基础型网络里，是由基站负责动态选频。至于独立型网络，则必须指定由谁进行动态选频 (dynamic frequency selection，简称 DFS) 算法。在 IBSS 中负责动态选频的工作站可以在管理帧中传递 IBSS DFS 信息元素，如图 4-48 所示。

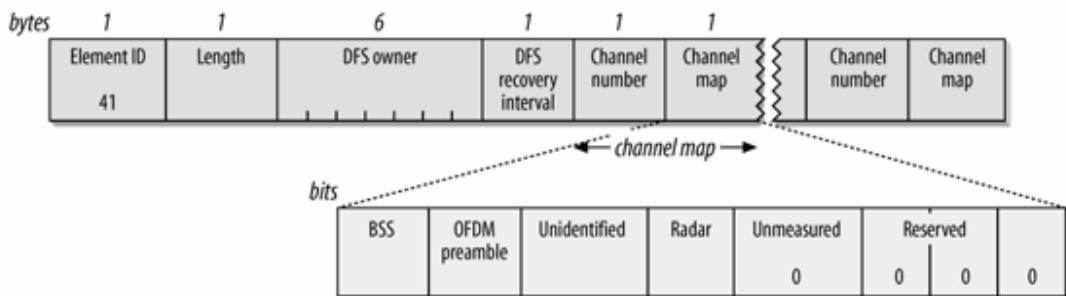


图 4-48: IBSS Dynamic Frequency Selection (DFS) 信息元素

紧跟在标头之后的是负责管理 DFS 信息之工作站的 MAC 地址，以及测量间隔。之后就是一系列的信道对映表，用来报告在每个信道监测到什么东西。信道对映表由一个信道编号，以及一个对映字节所构成，其中包含下列位：

BSS (一个 bit)

如果在测量期间侦测到来自其他网络的帧，则此 bit 会被设定。

OFDM Preamble (一个 bit)

如果侦测到 802.11a 的短调整序列(short training sequence)，但其余的帧并未追随其后，则此 bit 会被设定。HIPERLAN/2 网络采用的是一样的同步信号，但显然使用不同的帧结构。

unidentified Signal (一个 bit)

当所接收到的信号功率颇高，但无法分辨此信号究竟来自另一个 802.11 网络（因此要设定 BSS bit）、另外一个 OFDM 网络（因此要设定 OFDM Preamble bit）或是一个雷达信号（因此要设定 Radar bit），则此 bit 就会被设定。标准当中并没有明确规定功率必须高到何种程度，才可以设定本 bit。

Radar (一个 bit)

如果在测量期间监测到雷达信号，则此 bit 会被设定，必须监测哪些雷达系统，由管制当局定义，而非 802.11 任务小组。

Unmeasured (一个 bit)

如果未曾测量该信道，则此 bit 会被设定。如果未曾测量，当然也就监测不到任何东西，因此上述四个 bit 均会被设定为 0。

4.3.3.21 扩展物理层 (ERP)

802.11g 定义了扩展速率物理层 (extended rate PHY，简称 ERP)。为了兼容早期产品，另外定义了 ERP 信息元素，如图 4-49 所示。在最初的定义里，它相当于一个字节中的三个 bit 旗标。

Non-ERP present (无 ERP 信息)

当比较老旧、非 802.11g 的工作站与网络连接，就会设定此 bit。如果监测到相邻网络无法使用 802.11g，也会设定此 bit。

Use Protection (使用防护机制)

当网络中出现无法以 802.11g 数据速率运作的工作站，此防护 bit 就会被设定为 1。如此一来就可以兼容比较老旧的工作站，如第十四章所述。

Barker Preamble Mode (Barker 同步信号模式)

如果连接到网络的工作站没有能力使用第十二章所描述的短同步信号模式，则此 bit 就会被设定。

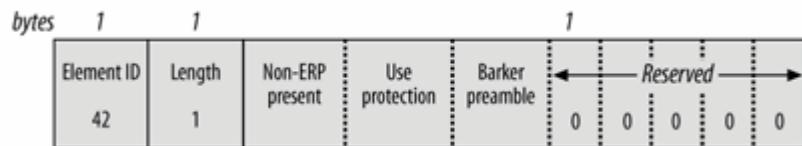


图 4-49: ERP 信息元素

4.3.3.22 固安网络 (Robust Security Network (RSN))

既然 802.11i 大幅改善了安全性，因此有必要开发一种方式，让工作站之间得以彼此交换安全性信息。用来达成此一目标的主要工具即是 Robust Security Network(固安网络，简称 RSN)信息元素，如图 4-50 所示。其中包含几种可能变动的成份，在某些情况下，就算不计标头，RSN 信息元素也有可能超出信息元素 255 个字节的限制。

Version (版本)

Version 属于必要位。802.11i 定义了版本 1。0 则保留未用，版本 2 以上则尚未定义。

Group cipher suite (群组密码锁集合)

紧跟版本编号之后的是 group cipher suite (群组密码锁节后) 描述符。基站必须从中选择一种相容于所有已连接工作站的群组密码锁，以便保护广播与组播帧。同时间只允许选择一种群组密码锁。

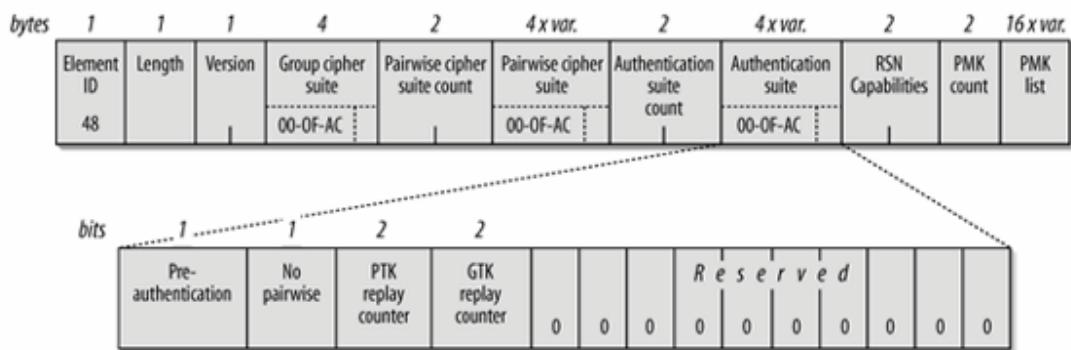


图 4-50: Robust Security Network (RSN) 信息元素

密码锁集合选项(cipher suite selector)的长度为四个字节，由厂商的 OUI 以及代表密码锁的编号所组成。标准化的密码锁集合如表 4-9 所示。(未出现在该表的值，代表保留未用。) 802.11i 所使用的 OUI 为 00-OF-AC，为 802.11 工作小组所拥有。

表 4-9: 密码锁集合

OUI	Suite Type	Definition
00-0F-AC (802.11)	0	使用群组密码锁集合 (只对成对密码锁有效) Use the group cipher suite (only valid for pairwise ciphers)
00-0F-AC	1	WEP-40
00-0F-AC	2	TKIP

OUI	Suite Type	Definition
00-0F-AC	3	保留 (Reserved)
00-0F-AC	4	CCMP
00-0F-AC	5	WEP-104
Vendor OUI	Any value	厂商自定义 (Defined by vendor)

Pairwise Cipher Suites (count+list) (成对密码锁集合 (计数+列表))

除了群组密码锁集合，必然要有一些用来保护单点传播帧的成对密码锁集合。它是由两个字节的计数，以及一系列其所支持的密码锁描述符所组成。密码锁集合选项(**cipher suite selector**)可以设定为 0，代表只支持群组密码锁集合。除了信息元素的大小之外，支持多少成对密码锁并无限制。

Authentication and Key Management (AKM) suites (count+list) (身份认证与密钥管理集合 (计数+列表))

和成对密码锁集合选项(**pairwise cipher suite selector**)一样，目前也存在好几种身份认证类型。它是由计数，以及一系列四个字节的识别码所构成。和密码锁集合一样，由四个字节所构成的识别码，包含了一个 OUI 以及一组类型编号。标准的身份认证类型，如表 4-10 所示。

表 4-10: 身份认证与密钥管理组合

OUI	集合 类型	身份认证	密钥管理
00-0F-AC	1	802.1X 或 PMK 快取(802.1X or PMK caching)	密钥衍生自预设共享主钥，如第七章所述 (Key derivation from preshared master key, as described in Chapter 7)
00-0F-AC	2	预设共享密钥 (Pre-shared key)	密钥衍生自预设共享密钥，如第七章所述 (Key derivation from pre-shared key, as described in Chapter 7)
Vendor OUI	Any	厂商自定义 (Vendor-specific)	厂商自定义 (Vendor-specific)

RSN Capabilities (RSN 性能)

此位的长度为两个字节，由四个旗标构成，用来描述发送端的能力，其后的 bit 保留未用，必须设定为 0。

Pre-authentication (事先身份认证)

基站可以设定此 bit，代表它可以和网络中其他基站进行事先身份认证，以便安全地转移连接事宜。否则，此 bit 会被设定为 0。事先身份认证将于第八章探讨。

No Pairwise (无成对密钥)

如果工作站除了较牢靠的单点传播密钥（unicast key），也支持手动设定的 WEP 密钥，以做为广播数据之用，则此 bit 就会被设定。虽然工作站支持但除非绝对必要，否则不会使用这种配置设定。

Pairwise Replay Counter（成对重演计数器）与 Group Replay Counter（群组重演计数器）

在逐渐浮出台面的服务质量扩展功能中，每个优先程度可以拥有好几个不同的重演计数器。这些 bit 用来描述工作站所支持的重演计数器数量。

PMK list (count+list) (PMK 列表 (计数+列表))

如果基站快取成对主钥（pairwise master key），就可以在基站间进行快速换手。工作站可以在进行连接时提供基站一串主钥，如此就可以免除费时的身份认证程序。PMK 快取在第八章中有更为详细的讨论。

4.3.3.23 扩展支持速率 (Extended Supported Rate)

Extended Supported Rates 信息元素的作用和图 4-33 的 Supported Rates 元素没有两样，不过它允许信息元素的内容超过 25 多个字节。

4.3.3.24 Wi-Fi Protected Access (Wi-Fi 访问保护，简称 WPAI)

Wi-Fi 访问保护从 802.11i 中抽出部分功能并稍做修改，目的是为了尽快将 TKIP 推到市场上。它相当于图 4-50 的 Robust Security Network 信息元素，不过做了以下变动：

- 元素识别码 (element ID) 为 221，而非 48。
- WPA 特有的 00:50:F2:01 标记被安插于版本位之前。
- 使用微软 (00:50:F2) 而非 802.11 工作小组的 OUI。
- 此信息元素只支持一种密码锁集合 (cipher suite) 以及一种身份认证组合 (authentication suite)。不过，有些 WAP 实作并未遵照此项限制。
- 使用 TKIP (而非 CCMP) 做为预设的密码锁。
- WPA 不支持事先身份认证，因此 preauthentication capabilities bit 必然设定为 0。

4.3.4 管理帧的类型

管理帧的主体所包含的固定位与信息元素是用来运送信息。管理帧有好几种分别负责链路层各种维护功能。

4.4.1.1 Beacon (信标) 帧

Beacon 帧是相当重要的维护机制，主要用来宣告某个网络的存在。定期发送的信标，可让移动工作站得知该网络的存在，从而调整加入该网络所必要的参数。在基础型网络里，基站必须负责发送 Beacon 帧。Beacon 帧所及范围即为基本服务区域。在基础型网络里，所有沟通都必须通过基站，因此工作站不能距离太远，否则便无法接收到信标。

图 4-51 依序显示了 Beacon 帧所使用的各个位。信标并不全然会用到所有位。选择性位只有在用到时才一会儿出现。只有在使用跳频(frequency hopping，简称 FH) 或直接序列

(direct-sequence, 简称 DS) 物理层技术时, 才会用到 FH 与 DS 参数组合。任何时候只能使用一种物理层, 因此 FH 与 DS 参数组合是彼此互斥的。

CF 参数组合只用于支持 PCF 的基站所产生的帧中, 至于是否支持 PCF 并非强制 PCF 的 TIM 只用于基站所产生的 Beacon 帧中, 因为只有基站才会暂存帧。如果有特定国家的跳频扩展元素, 则必然随附在 Country 信息元素之后。不过, 跳频网络至今已不常见, 为求简化, 因此我省略了跳频扩展元素。同样地, 若是出现 IBSS DFS 元素, 则其必然位于 Quiet 与 TPC Report 元素之间。

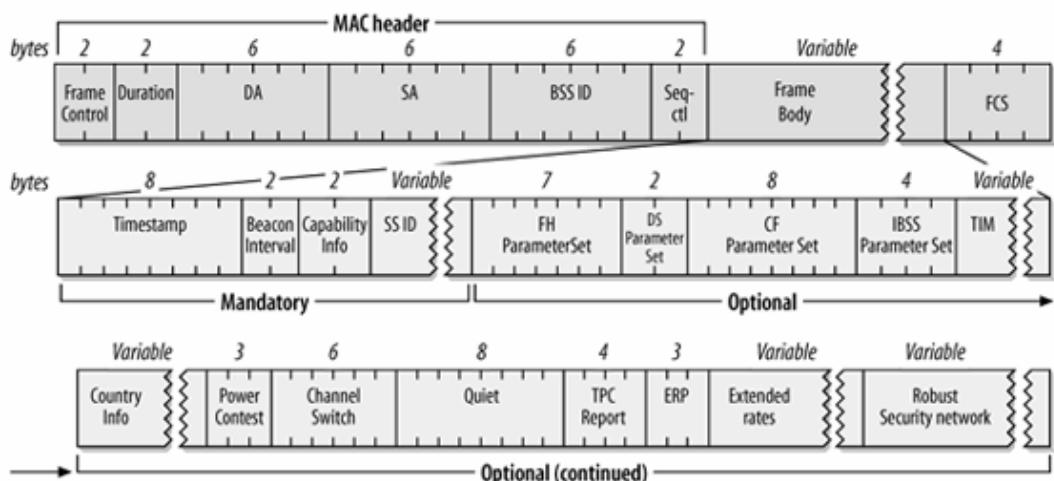


图 4-51: Beacon (信标) 帧

4.3.4.2 检测要求 (Probe Request)

移动工作站将会利用 Probe Request (检测要求) 帧, 扫描所在区域内目前有哪些 802.11 网络。Probe Request 帧的格式如图 4-52 所示。所有位均为必要。

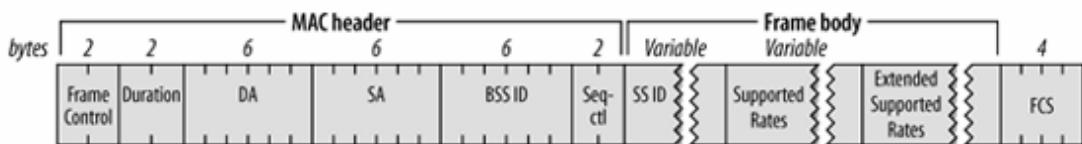


图 4-52: Probe Request (检测要求) 帧

Probe Request 帧包含两个位: SSID 以及 Supported Rates (移动工作站所支持的速率)。收到 Probe Request 帧的工作站会据此判定对方能否加入网络。为了相处愉快, 移动工作站必须支持网络所要求的所有数据速率, 并以 SSID 表明所欲加入的网络。SSID 可设定为特定网络的 SSID, 或设定为任何相容网络的 SSID。允许网卡加入任何网络的驱动程式, 将会在 Probe Requests 中使用 broadcast SSID (广播形式的服务集识别码)。

4.3.4.3 检测应答 (Probe Response)

如果 Probe Request 帧所探查的网络与之相容, 该网络就会以 Probe Response 帧应答。送出最后一个 Beacon 帧的工作站, 必须负责应答所收到的检测信息。在基础型网络里, 负责应答的工作站即为基站。在 IBSS 当中, 工作站会彼此轮流发送 Beacon 信号。发送 Beacon 信号的工作站必须负责发送 Probe Response 帧, 直到下一个 Beacon 被发送出来。Probe Response 帧的格式如图 4-53 所示。其中某些位彼此互斥; 此规则同样适用于 Probe Response 以及 Beacon 帧。

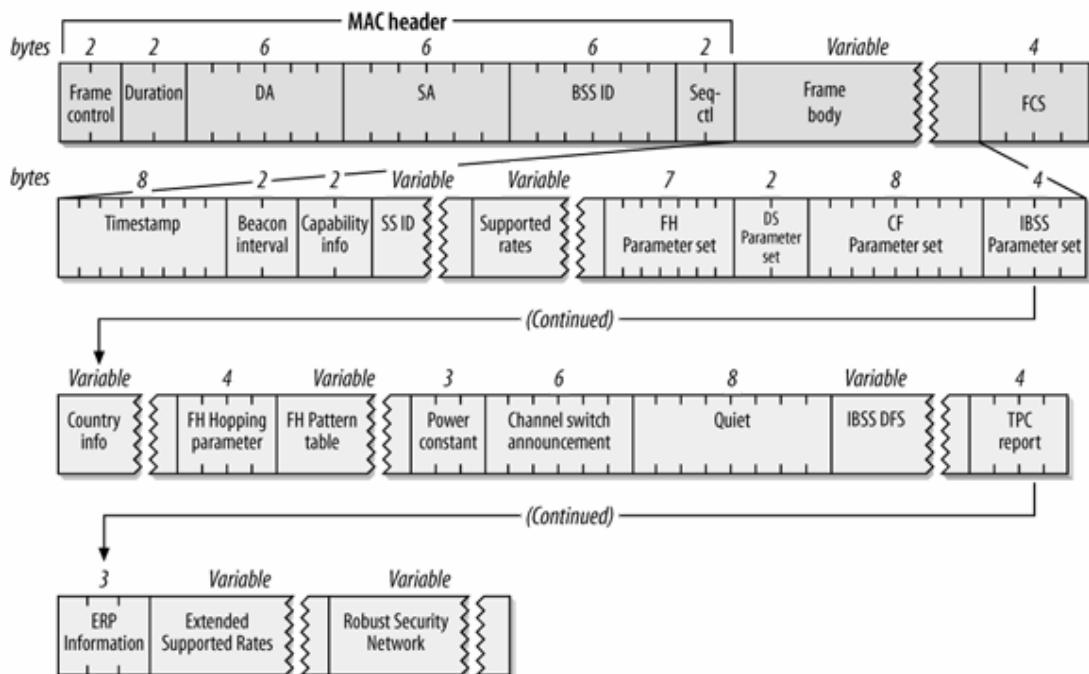


图 4-53: Probe Response (检测应答) 帧

Probe Response 帧中包含了 Beacon 帧的所有参数，移动工作站可据以调整切入网络所需要的参数。• Probe Response 帧可以剔除 TIM 元素，因为此时工作站尚未建立连接，因此不必知道哪些连接在基站中有暂存帧。

4.3.4.4 IBSS 的数据待传指示通知信息 (ATIM) 帧

HSS 中没有基站，因此无法仰赖基站暂存帧。IBSS 中的工作站如果为处于休眠状态的接收者暂存帧，就会在递送期间送出一个 ATIM 帧，通知对方有信息待阵，如图 4-54 所示。

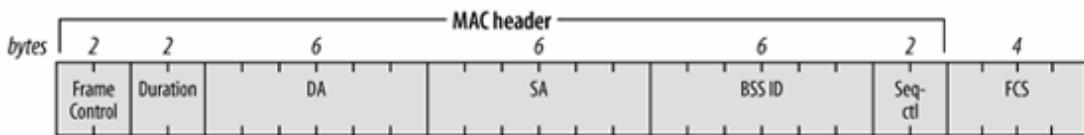


图 4-54: ATIM 帧

4.3.4.5 解除连接和解除认证 (Disassociation 与 Deauthentication)

Disassociation (解除连接) 帧用来终结一段连接关系，而 Deauthentication (解除认证) 帧则用来终结一段认证关系。两者均包含一固定位，Reason Code (原因代码)，如图 4-55 所示。当然，Frame Control 位彼此不同，因为不同类型的管理帧拥有不同的次类型。802.11 改版并不需要改变这一格式，但几次修订均加入了新的原因代码。

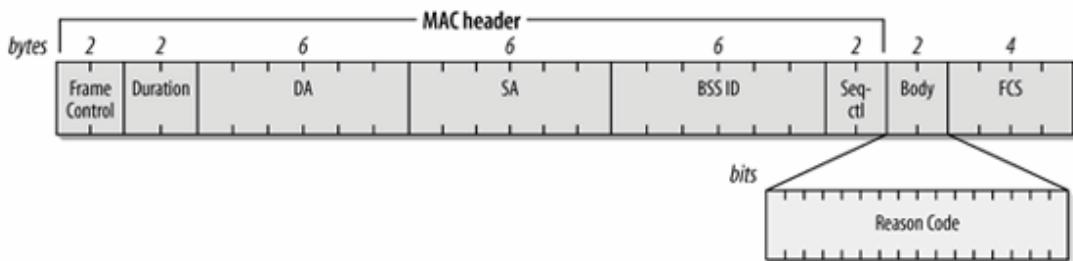


图 4-55: Disassociation (解除连接) 与 Deauthentication (解除认证) 帧

4.3.4.6 连接要求 (Association Request)

一旦移动工作站找到相容网络并且通过身份认证，便会发送 Association Request (连接要求) 帧，试图加入网络。Association Request 帧的格式如图 4—56 所示。

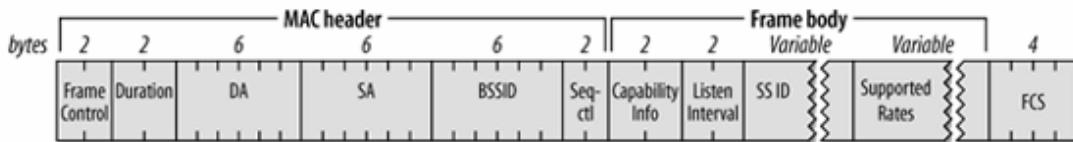


图 4-56: Association Request (连接要求) 帧

Capability Information (性能信息) 位用来指出移动工作站所欲加入的网络类型。在接受连接要求之前，基站会验证 Capability Information、SSID 以及 (Extended) Supported Rated 等位是否符合网络参数。此外，基站也会记录工作站所使用的 Listen Interval (聆听间隔；即移动工作站每隔多久聆听一次 Beacon 帧，以监视 TIM 信息)。支持频谱管理的工作站具备 power (功率) 与 channel (信道) 性能信息元素，支持安全防护的工作站则具备 RSN 信息元素。

4.3.4.7 重新连接 (Reassociation Request)

位于相同扩展服务区域，但在不同基本服务区域之间游走的移动工作站，若要再次使用传输系统，必须与网络重新连接。如果工作站暂时离开基站所涵盖的范围，之后要重新加入的时候，也必须重新连接。如图 4-57 所示。

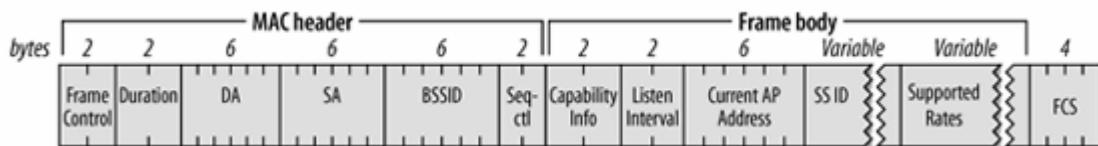


图 4-57: Reassociation Request (重新连接要求) 帧

association Request (连接要求) 与 Reassociation Request (重新连接要求) 之间的差别在于，后者包含移动工作站目前所连接之基站的地址。拥有这项信息可让新旧基站彼此联系，以及交接连接数据。交接项目包括先前连接之基站所暂存的帧。

4.3.4.8 连接应答与重新连接应答 (Association Response 与 Reassociation Response)

当移动工作站试图连接基站时，基站会回覆一个 Association Response (连接应答) 或 Reassociation Response (重新连接应答) 帧，如图小 58 所示。两者之间的差别，在于 Frame Control 位所记载的 subtype 位。所有位均属必要。在应答的过程中，基站会指定一个 Association ID (连接识别码)，至于指定的方式则因实作而异。

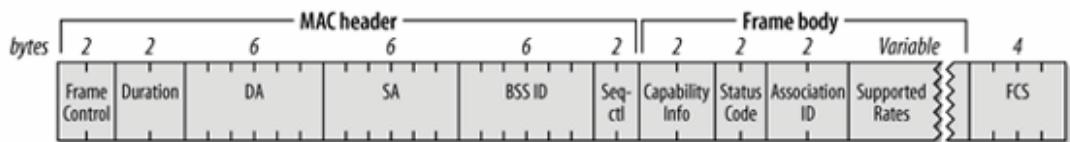


图 4-58: (Re)Association Response ((重新) 连接应答) 帧

4.3.4.9 认证 (Authentication)

802.11 网络发展初期，工作站是使用共享密钥以及图 4-59 所示的 Authentication 帧进行身份认证。到了 802.11i，共享密钥身份认证虽然仍保留在标准当中，但却无法与新的安全机制相容。如果工作站使用共享密钥身份认证，将不允许使用较为牢靠的安全性协议，如第八章所述。

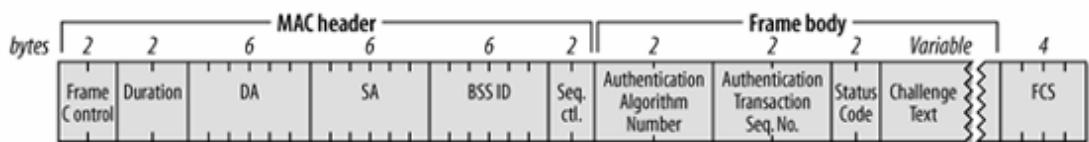


图 4-59: Authentication (身份认证) 帧

不同的身份认证算法可以同时存在。Authentication Algorithm Number (身份认证演算法编号) 位用于选择演算法。整个认证程序可能包含好几个步骤 (与所使用的算法有关)，因此认证的过程中每个帧都有其序号。Status Code 与 Challenge Text 的用法因算法而异，相关细节将于第八章讨论。

4.3.4.10 Action

802.11h 加入了 Action 帧的支持，用来触发测量动作。这些帧将于 8.8 节<频谱管理>详加描述。

4.4 帧发送以及连接与身份认证状态

所能发送的帧类型，依连接状态与身份认证状态而有所不同。工作站可能已经认证或未经认证，也可能已经连接或尚未连接。这两个变数的组合有三种可能状态，结果构成了 802.11 的网络发展层级：

1. 初始状态；未经认证且尚未连接
2. 已经认证但尚未连接
3. 已经认证且已经连接

每种状态分别对应到 802.11 连接的发展阶段。一开始，移动工作站处于状态 1，只有进入状态 3 才可以通过传输系统发送数据。（IBSS 不包含基站，也无须进行连接，因此只会停留在状态 2。）802.11 帧传输的整体状态图，如图 4-60 所示。

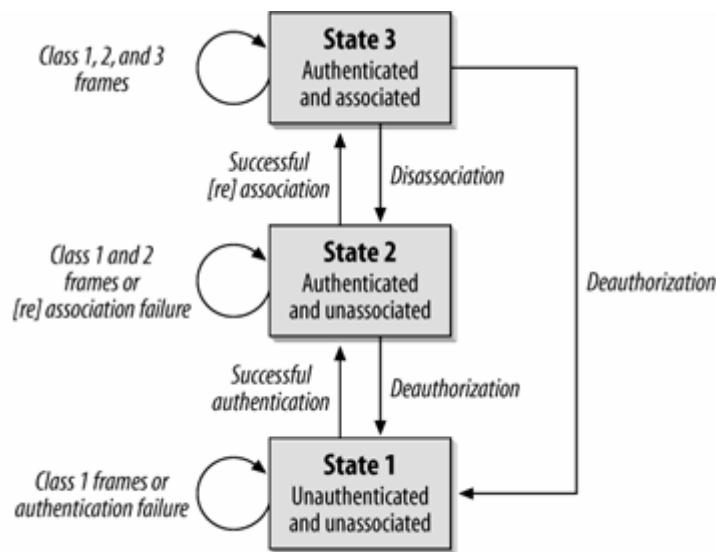


图 4-60: 802.11 整体状态图

4.4.1 帧等级

帧可以被划分为三种等级。在状态 1 可以传递第 1 级帧；在状态 2 可以发送第 1 与 2 级帧；在状态 3 则可以传递第 1、2 与多级帧。

第 1 级帧

第 1 级帧可以在任何状态中传递，它让 802.11 的工作站得以进行基本作业。在 IBSS 当中，控制帧主要用来依循 CSMA/CA 规则，以及发送帧。工作站也会使用第 1 级帧来找寻基础型网络，并与之进行身份认证。表 4-11 列出了属于第 1 级的各种帧。

表 4-11：第 1 级帧

控制帧	管理帧	数据帧
Request to Send (RTS)	Probe Request	Any frame with ToDS and FromDS false (0)
Clear to Send (CTS)	Probe Response	
Acknowledgment (ACK)	Beacon	
CF-End	Authentication	
CF-End+CF-Ack	Deauthentication	
	Announcement Traffic Indication Message (ATIM)	

第 2 级帧

工作站只有在经过身份认证之后，方能够发送第 2 级帧，而且第 2 级帧只能使用于状态 2 与状态 3。2 级帧主要用来管理连接。线或重新连接成功后，工作站就会进入状态 3；如果连接

失败，则工作站依然处于状态 2。工作站收到未经认证的作站所传来的第 2 级帧时，就会应答一个 Deauthentication（解除认证）帧，将对方推回状态 1。表 4-12 列出了所有的第 2 级帧。

表 4-12：第 2 级帧

控制帧	管理帧	数据帧
None	Association Request/Response	None
	Reassociation Request/Response	
	Disassociation	

第 3 级帧

第 3 级帧的使用时机，是在工作站认证成功并与基站连接之后“一旦工作站进入状态 3，就可以使用传输系统服务，也可以和基站范围以外的对象进行通讯。在状态 3，工作站还可以利用 PS-Poll 帧享受基站所提供的省电服务。表手 1 予列出了不同类型的第 3 级帧。

表 4-13：第多级帧

控制帧	管理帧	数据帧
PS-Poll	Deauthentication	任何帧，包含 ToDS 或 FromDs bit 都设为 1 的所有帧 (Any frames, including those with either the ToDS or FromDS bits set)

如果所收到的帧，来自一部已经验证但尚未连接的工作站，基站就会应答一个 Disassociation（解除连接）帧，迫使工作站回到状态 2。如果发出帧的工作站尚未经过验证，则基站会应答一个 Deauthentication（解除认证）帧，迫使工作站回到状态 1。

第5 章 有线等级隐私 (WEP)

不曾为之震撼的人，
哪里懂得量子理论。

- Niels Bohr

在无线网络领域中，广播（broadcast）一词具有崭新的意义。无线网络使用开放性介质，如果传输链路没有采取适当的加密保护，使用上的风险就会大幅增加。既然是开放性的网络介质，只要拥有适当的设备，任何人都可以偷窥未经保护的数据。以无线局域网络而言，所谓“适当的设备”是指能够接收和解读 802.11 的界面，然而这种设备并不算昂贵。如果需要更高档的设备，可以考虑使用具高增益的外置天线。既然天线已经相当便宜，各位最好假定有意攻击的黑客早就人手一支。

防范数据遭到拦截属于加密协议的范畴。当帧在空气中传播，必须加以保护方能免遭毒手。保护有好几种形式，不过最常被引用的两种非正式目的，就是维护网络数据的私密性以及确保数据未被篡改。起初，有线等级隐私 (WEP) 标准被视为无线安全的解决方案。不过在 802.11 问世的前四年，研究人员发现 WEP 并不安全。

倘若 WEP 真是如此差劲，为何还要为它浪费时间呢？因为有些时候，某些特殊设备只支持 WEP。况且 WEP 的设计相当容易实现。虽然它不如后续出现的加密协议复杂，也不要求多么强大的计算能力。一些老旧设备，特别是手持应用方面的设备，也许缺乏足够的处理能力而无法运行得更为顺畅，因此 WEP 已经算是最佳的选择了。此外，较新的技术如 TKIP 仍旧会用到 WEP 的帧处理过程，因此了解 WEP 也就十分重要了。

5.1 WEP 的密码学背景

探讨 WEP 的设计之前，有必要先了解一些基本的密码学概念。我并不是密码学者，本书也不适合深究密码学，因此本章只能轻描淡写。

WEP 用来保护数据的 RC4 密码锁属于对称性密钥串流密码锁(stream cipher)。RC4 具备所有串流密码锁的共同特性。一般而言，串流密码锁会用到称为密钥串流 (keystream) 的 bit 串流。密钥串流随后会与讯息结合，产生密文(ciphertext)。为了还原原始讯息，接收端会以相同的密钥串流处理密文。RC 缠会利用异或 (exclusive OR, 简称 XOR) 运算结合密钥串流与密文。图 5-1 说明了整个过程。

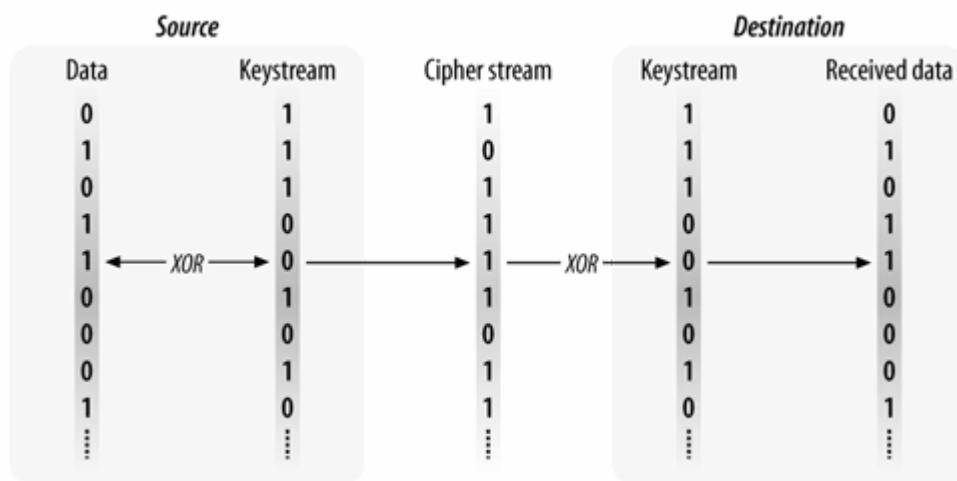


图 5-1：串流密码锁的一般运作程序

串流密码锁的运作方式，通常会先选用一把较短的密钥，然后将之展开为与讯息等长的伪随机数密钥串。整个过程如图 5-2 所示：伪随机数产生器（*pseudorandom number generator*，简称 **PRNG**）是一组用来将密钥展开为密钥串的规则。为了还原数据，双方必须拥有相同的密钥，并且使用相同的算法，将密钥展开为伪随机数序列。

既然串流密码锁的安全性完全取决于密钥串的随机程度，因此密钥如何展开为密钥串在设计上就极为重要。当 802.11 工作小组决定采用它时，RC4 看似十分安全。不过当 RC4 被选为 WEP 的加密引擎后，其所带动的一连串相关研究发现 RC4 密码锁本身存在极大的瑕疵，我们将于稍后提及。

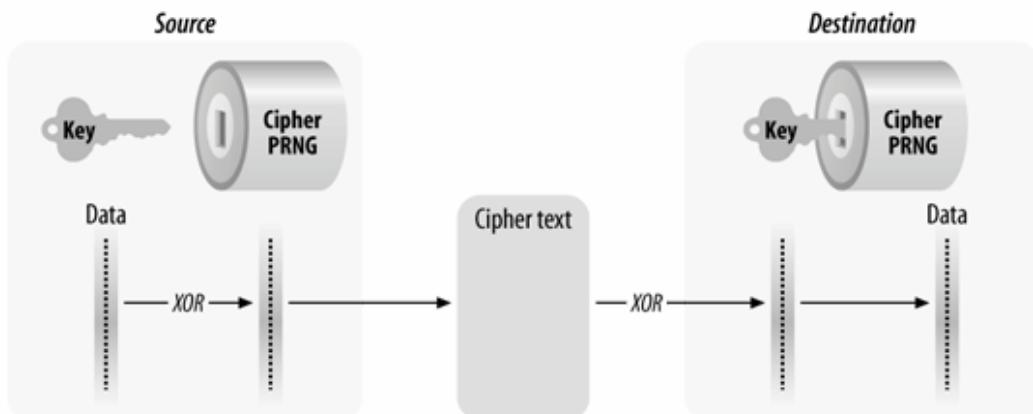


图 5-2：密钥式串流密码锁的运作过程

5.1.1 串流密码锁的安全性

一个完全随机的密钥串通常称为单次密码簿，它是经过数学证明，目前已知惟一可以防范任何攻击的加密方式。单次密码簿很少使用，因为除了密钥串必须完全随机，并与受保护的数据等长，而且还不得重复使用。

可能遭受攻击的对象，不只底层使用的密码。加密是统中任何的薄弱点都可能让攻击者趁虚而入。在以 VENONA（薇诺娜）为代号的着名任务中，西方国家之所以能够破解苏联的讯息，

是因为对方重复使用单次密码簿进行加密。想要重复使用单次密码簿的冲动不难理解。就算只是保护一丁点数据，也要用到大量的加密素材，何况这些密码簿还得安全地送到接收者手上。光这一点，实际上就是非常大的挑战。每个数据单元都必须用到相应的单次密码簿单元。**54 Mbps** 的网络可以传送大约 **25 Mbps** 的使用者数据。就算网络只用掉 **10%** 的频宽，以一个工作天八小时的数据传输而言，总计也要傳送 **9 gigabytes** 左右的数据。要将好几个 **gigabytes** 的密钥素材传给每部基站，根本就不切实际。

串流密码锁是安全与实际应用下的折衷产物。单次密码簿所具备的完全随机性（以及绝对安全性）虽然吸引人，但考虑到实际的困难以及产生与传递解密文件的成本，除非要求绝对安全的信息，实际上并不值得采用。串流密码锁所使用的密钥串的随机程度虽然较低，但已足够应付绝大多数的应用。

5.1.2 密码政治学

密码学的讨论，如果不能交待围绕其应用的种种法律与管制上的考虑，就不能称得上完整。**WEP** 的应用有三项主要议题，虽然这些议题的效应将会随着时间而递减。

WEP 需要通过 **RC4** 密码锁来加密数据帧。撰写本书第一版时，**WEP** 只是一种可有可无的选项，并未内置到所有产品当中。经过授权的软件可以使用 **RC4** 程序码，不过开放源码专案对此则有所顾虑，因为可能会侵犯 **RSA Security** 公司的智慧产权。本书第一版问世后，这项顾虑才逐渐消除。所有主要的芯片厂商均已获得 **RC4** 加密授权，并且将它整合到 **802.11** 芯片。设备驱动程序只需负责将 **WEP** 密钥交给硬件处理即可。让网卡硬件处理加密事宜，意味着软件无须考虑是否会侵犯到 **RSA** 的智慧产权。

起初，**WEP** 在设计上之所以采用短密钥。是为了符合美国对加密产品的出口管制。一开始，标准要求采用 **40bit** 的短密钥，不过现在几乎所有市面上的产品都至少支持 **104bit** 的密钥。短期而言，长密钥似乎是标准的重要延伸，不过其所能够提供的额外安全性，已经证明纯属虚幻。

最后，有些政府严格管制任何加密系统的使用，包括 **WEP** 在内。除了美国的出口管制，有些国家尚有进口管制，限制加密设备的进口。其他的政府也有权提出一些额外的加密限制。中国自己开发了一种替代方案，称为无线局域网络鉴别与私密基础结构(**WLAN Authentication and Privacy Infrastructure**，简称 **WAPI**)的安全系统，将之列为中国无线局域网络设备的选项。

5.2 WEP 的加密机制

通信安全主要有三种目的。当数据通过网络，数据保护协议必须能够协助网管人员达成这些目的。机密性(**confidentiality**)是为了防范数据不受未经授权的第三者拦截。完整性(**Integrity**)则是确定数据没有遭到篡改。而认证(**authentication**)是所有安全策略的基础，因为数据的可信度，部分取决于数据来源的可靠性。使用者必须确认数据的来源的正确性。系统必须利用认证来保护数据。授权(**authorization**)与访问控制两者均基于真实性之上。在允许访问任何数据之前，系统必须确认使用者的身份(真实性)，以及是否允许该使用者访问数据。

为了达到上述目的，**WEP** 本身提供了一些机制，虽然这些机制在遭受严重攻击时可能失效。帧主体加密机制(**frame body encryption**)主要用来提供机密性。完整性检验机制(**integrity check sequence**)在传送过程中用来保护数据，让接收者得以验证所收到的数据，在传送过程中未被改动过。实际上，**WEP** 在这些领域并非有力机制，需要用到一些额外的加强措施，这些将留在后两章探讨。

5.2.1 WEP 的数据处理

机密性与完整性的作业同时进行，如图 5-3 所示。加密之前，帧会通过完整性检验算法，产生一个称为完整性检验值（integrity check value，简称 ICV）的杂乱信号。ICV 可确保帧在传输过程中没有被篡改。帧本身与 ICV 两者均经过加密，因此 ICV 不会被攻击者任意宰割。

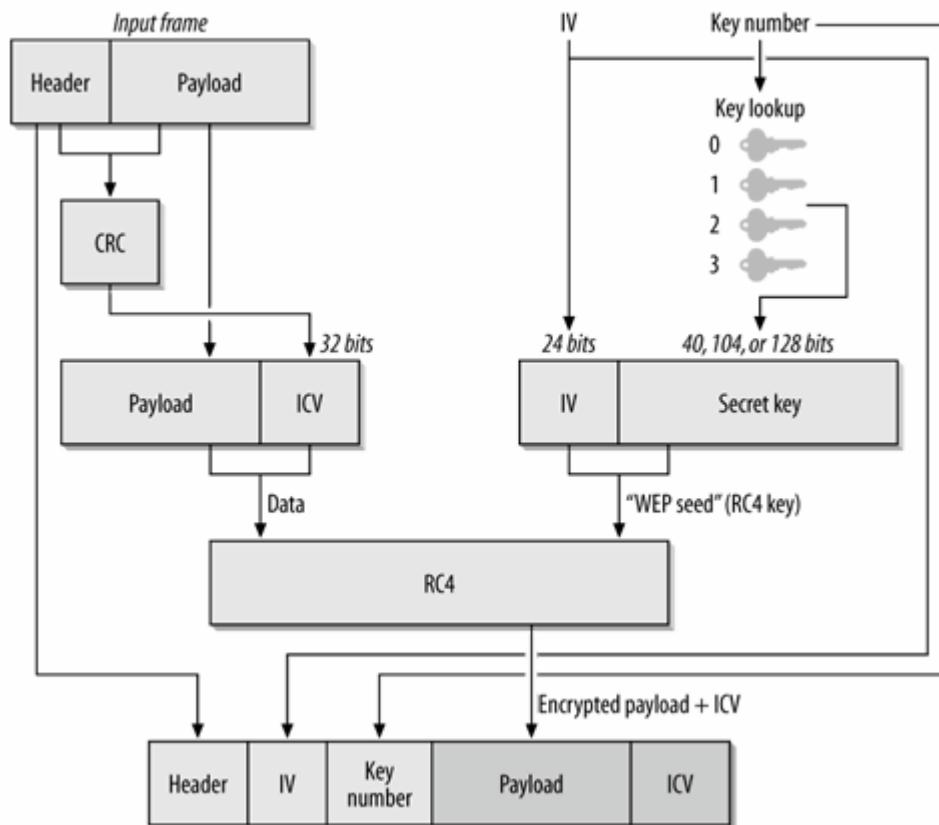


图 5-3: WEP 的运作方式

WEP 需要以下三种输入项：

- 需要保护的原始数据（Payload），来自上层协议栈（protocol stack）。
- 密钥(Secret Key)，用来加密帧。依实现方式的不同，可以用 bit 串(string of key bits) 或者数字（key number）来指定密钥，WEP 允许同时储存四把密钥。
- 初始向量(IV)搭配密钥在传送帧时使用。

经过处理后，WEP 会产生一输出项：

- 加密过的帧，可以通过不安全的网络加以传输，其中包含足够的数据，使对方能够正确解密。

5.2.1.1 WEP 的数据传输

驱动程序以及界面硬件负责处理数据，然后送出加密过的封包，顺序如下：

1. 802.11 帧被置于序列待传。帧由标头与所承载的数据组成。WEP 只保护 802.11 MAC 所承载的数据，至于 802.11 帧标头以及其他底层协议标头则丝毫无予改动。
2. 根据 802.11 MAC 帧所承载的数据计算出完整性检验值。由于此检验值是针对帧所承载的数据，因此计算所涵盖的范围始于 SNAP 标头的第一个 bit，直到帧本体的最后一个数据 bit。此时，802.11 帧检验值尚未计算出来，因此并未包含在 ICV 的计算当中。WEP 所使用的 ICV 属于循环冗余检验码(Cyclic Redundancy Check，简称 CRC)，稍后有更进一步的说明。
3. 帧加密密钥（或称 WEP 种子）随后组装完成。WEP 密钥分为两部分：密钥以及初始向量（IV）。如果使用同一把密钥，串流密码锁会产生相同密钥串流，因此另以初始向量为个别帧产生不同的串流密码锁。为了避免出现使用相同密钥串流进行加密的情况，传送帧的工作站会将 IV 附加在密钥之前。802.11 并未限制选取 IV 非得使用何种算法；有些产品使用流水号做为 IV 值，有些则会使用伪随机杂散算法。如何选择 IV 具有重要的安全性意义，选得不好，就可能危及密钥。
4. 帧加密密钥被当成 RC4 密钥，用以加密来自步骤一的 802.11 MAC 承载数据，以及来自步骤二的 ICV。整个加密程序，通常通过网卡上之 RC4 专用电路的协助完成。
5. 将承载数据加密之后，工作站就会开始组装待传输的帧。802.11 标头本身维持不变。802.11 MAC 标头与加密过的承载数据之间，则插入了 WEP 标头。除了 IV，WEP 标头中还包含密钥编号。WEP 最多允许定义四把密钥，因此传送端必须分辨目前使用的是哪一把密钥。一旦附加上最后的标头，就可以针对整个 MAC 帧，亦即从标头起算，直到加密过的 ICV 结尾，计算出 802.11 帧检验码（FCS）。

解密程序刚好相反。与任何的无线网络传输过程相同，首先是验证 FCS，确保所接收到的帧未在传送过程中损毁。解读帧受保护的部分时，接收端会使用密钥，加上 IV，然后产生密钥串。得到解密过的数据后，接下来则是验证 ICV。如果 ICV 验证无误，就根据 SNAP 标头所记载的内容，将封包数据交给适当的上层协议。

5.2.1.2 WEP 密钥的长度

理论上，WEP 可以搭配任意长度的密钥，因为 RC4 并未要求非得使用特定长度的密钥。不过，大多数产品均支持一或两种长度的密钥。惟一出现在标准中的密钥长度是 64bit 的 WEP 种子，其中 40 个 bit 是两部工作站进行传输时所共享的密码。不同厂商会以各种不同的名称来称呼标准的 WEP 模式：**standard WEP**、**802.11-Compliant WEP**、**40-bit WEP**、**40+24-bit WEP**，甚至是 **64-bit WEP**。我个人认为最后一种说法纯粹是误导，这是以共享密钥而非以共享密码的长度来蒙骗消费者。不过，这似乎已经成为业界的某种标准了。

另外比较常见的做法，就是采用较长的密钥，通常使用 128-bit 的 WEP 种子，其中 104 个 bit 密而不宣。有些文件称之为 **WEP-104**，虽然文件上通常称之为 128-bit WEP。虽然比较少见，但使用长度 128bit 的密钥，并非闻所未闻，结果 WEP 种子的长度就变成了 152 个 bit。容易令人混淆的是，这种少见的做法通常也称为 128-bit WEP，虽然因为密钥长度的不同，使得它与 WEP-104 互不相容。有家厂商甚至提供 256bit 的密钥，但这种做法是否提升安全性还令人怀疑。

在设计完善的密码系统中，使用较长的密钥可以获得较高的安全性。每增加一个 bit，就会让可能产生的密钥数量加倍。因此，理论上要破解系统的时间也随之加倍。然而，WEP 并非设

计完善的密码系统，况且在密钥中多加几个 bit 并不能带来多少好处，已经揭露的最佳攻击手法，可以在短短几秒钟内破解 WEP 取得密钥，不论密钥长度如何。

5.2.1.3 WEP 密钥的类型

可以使用两种不同类型的密钥。配套密钥（**mapped key**）用来保护流动于特定来源与接收端之间的数据。配套密钥有时也称为单点传播密钥(**unicast key**)或工作站密钥（**station key**），因为它们适合用来保护单点传播数据。在基础(**infrastructure**) 网络里，数据是在工作站与基站间流动。**802.11** 帧中同时包含了接收端与目的端地址。单点传播数据可以有许多不同的目的地，不过流动于基础网络里的单点传播帧均会以基站的 **MAC** 地址做为接收端地址。所有来自或传至工作站的单点传播帧，均可以使用单一配套密钥进行加密。如果两部 **802.11** 工作站之间并不存在配套关是，就必须改用预设密钥(**default key**)，有时也称为广播密钥(**broadcast key**)。预设密钥天生就适合用于广播与组播帧，因为群组地址代表多部工作站，因此无法支持配套密钥关是。

5.2.1.4 人工（静态）与自动（动态）的 WEP

802.11 并没有规范 WEP 必须使用特定的密钥传递机制。对 WEP 而言，反正密钥就是会神奇出现。早期的 WEP 实现必须靠人工传递密钥。网管人员必须负责将一把预设密钥传递给网络中所有工作站，这个程序通常是靠手动完成的。密钥的更新也是通过手动方式。实际上，大部分的网络都会被部署成长时间使用同一把密钥，因为更新密钥对网管而言其实是非常大的负担。因此，不具密钥传递机制的 WEP 通常称为人工 WEP 或静态 WEP。

人工密钥是个糟透了的概念。要管理整个网络这么多基站的密钥传递是相当困难的事。密钥是用来保护数据，如果组织中有知道密钥的人离职，就应该予以更换。理论上，设计完善的加密是统在使用密钥时，会尽可能将它们局限在某些特定的目的上，以防止密钥遭到破解。静态的 WEP 在每部工作站所传送的各个帧中均使用同一把密钥，万一密钥遭到破解，后果将不堪设想。

如果没有明确的理由，就不该采用静态 WEP。除了聊胜于无，静态 WEP 其实乏善可陈，它可以有效地制止散弹式的攻击 (**casual attacks**)，但无法防御集中火力型的侵略 (**determined assault**)。许多低功率设备，例如 **802.11** 电话、手持条码扫描器甚至是 PDA，无法提供优于 WEP 的解决方案。除非这些设备被完全被淘汰换掉，否则在这种情况下，静态 WEP 仍旧是保护链路层安全性的惟一选择。

比较好的解决方案是建立在动态 WEP 之上。在动态 WEP 中，每部工作站会使用两把密钥，而不是所有工作站共享一把密钥。其中一把是经过配套的密钥，为工作站与基站所共用，用来保护单点传播帧。另外一把是预设密钥，为同一服务组合中所有工作站共用，用来保护广播与组播帧。工作站所使用的加密密钥，是通过「密钥加密密钥」(**key encryption keys**) 来传递，至于用来衍生「密钥加密密钥」的认证协议，则留待下一章探讨。动态 WEP 具备许多静态 WEP 所不及的显著优势。从最抽象的层次而言，个别密钥均有范畴上的限制。由于密钥的使用次数不再如此频繁，相对可以降低密钥遭到破解的机会。有心人士当然可以集中火力攻击这些密钥，不过可供搜集的个别密钥数据一旦变少，攻击就变得更加费时。同等重要的是，动态密钥正如其名，本身会随着时间而改变。基站可以每隔一段时间就更换密钥，如此一来，攻击者就不得不放弃已经搜集到的数据，只能另起炉灶，重新对其他密钥发动攻击。只要更新密钥的间隔够短，就可以大幅减少密钥所遭受的攻击。动态 WEP 的解决方案将于本章稍后讨论。

5.2.1.5 WEP 密钥的编号与储存

WEP 密钥有其相对应的编号，802.11 工作站最多可以指定四把密钥。起初，WEP 密钥编号是为了协助更换网络密钥，指定好新的密钥后，工作站可以逐步切换，不必所在工作站同时切换。举例而言，假定组织原本使编号为 0 的密钥，如要更换，可以指定使用编号为 1 的密钥。如此一来，工作站至少有一段缓冲时间，逐渐改用编号为 1 的密钥，而不是在同一时间全面更新。等到过渡期结束，编号为 0 的密钥就可以停用。

在动态 WEP 解决方案里，密钥编号扮演不太一样的角色。每部工作站均会自基站处接收到两把密钥：一把配套密钥，通常储存为 0 号密钥，以及一把预设密钥，通常储存为 1 号密钥。工作站以 0 号密钥保护单点传播数据，以 1 号密钥保护广播数据。当帧被置于待传序列，驱动程序将会以 0 号密钥加密单点传播帧，以 1 号密钥加密广播帧。

802.11 刚问世时，有些网卡并不支持 WEP，或只能借助于主机的 CPU 进行 RC4 加密运算，因此效率大打折扣。以硬件实现 RC4 其实相当容易，1999 年以后，几乎所有市面上的无线局域接口均已内建 RC4 硬件加密的功能，免得软件加密拖垮整体效率，（包含大多数较晚推出的 802.11b 网卡）。有些较旧的网卡还通过软件限制只能使用长度为 40 而非 104bit 的密钥，如 Orinoco 所推出的银卡与金卡。后续发行的软件已经不再限制可使用的密钥长度。

为了让帧的加密更有效率，许多 802.11 芯片内含一种称为密钥快取 (key cache) 的数据结构。密钥快取组成自目的地地址、密钥识别编号、密钥本身各个 bit 的对映关系。大多数工作站网卡的芯片具备四个密钥槽。静态 WEP 使用其中一个密钥槽，动态 WEP 使用两个。当帧置于待传序列，首先会在密钥快取中查询目的地地址，所查到的密钥就用来加密帧。动态密钥在功能上和静态 WEP 一样，不过密钥获取的内容可能会被密钥管理软件所取代。

适用于网卡与适用于基站的芯片，不同之处在于后者具备较大的密钥快取，通常可以容纳 256 或更多的密钥项目。就算每部工作站需要用到两把密钥（一把配套密钥与一把预设密钥），这样的数据结构就可以处理 100 台以上的工作站密钥。既然大多数的无线链路技术所消耗的频宽有限，这样的数据结构应该绰绰有余。不过，有些早期支持动态产生密钥的基站，并无法维护过大的密钥数据结构，必须让好几部工作站共用密钥。为了节省成本，有些厂商甚至在基站里使用网卡的芯片。如此一来，这些基站就只有四个密钥槽，所有与该基站连接的工作站，就得共用同一把单点传播密钥。

5.2.2 WEP 的帧格式

一旦使用 WEP 进行加密，帧主体就会增加 8 个 bit 组。其中 4 个 bit 组作为帧主体的 IV 标头，另外 4 个 bit 组则作为 ICV 标尾。如图 5-4 所示。

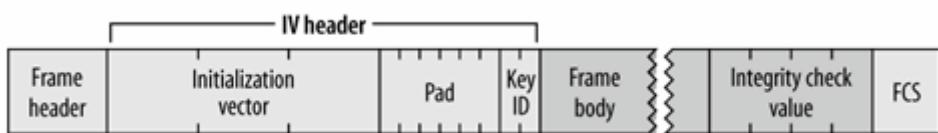


图 5-4: WEP 帧的延伸

IV 标头使用 3 个 bit 组来容纳长度 24 个 bit 的 IV，而第四个 bit 组则包含填空 bits(padding bits) 以及密钥识别码。使用预设密钥时，KEY ID 位可用来辨识加密帧的预设密钥。如果选择

使用密钥映射关系（key mapping relationship），则 Key ID 次栏位的值为 0。最后一个 bit 组中有 6 个填空 bit 必须为 0。数据帧的 32bit 校验码（CRC）提供了完整性的检查，附加于帧主体之后，同时为 RC4 所保护。帧检验序列（Name check sequence，简称 FCS）则是用来保护加密过的数据。

5.3 关于 WEP 的各种问题

密码学者在 WEP 当中发现了许多瑕疵。WEP 的设计者规定采用 RC4，而 RC4 向来被认为是一种可靠的密码锁（strong cryptographic cipher）。然而，攻击者并非只能对加密算法采取正面攻击，整个密码系统中的任何弱点都可以是侧面包抄的对象。摧毁 WEP 的方式来自各种不问角度。比较值得注意的一个案例是，有家厂商所生产的无线 AP 无意间暴露了 WEP 密钥，攻击者可以通过 SNMP 取得。不过，大部分的文件均将矛头指向实现之外，亦即设计上的瑕疵，要改正这一缺点可就困难多了。

5.3.1 RC4 在密码学上的性质

重复使用密钥串是所有串流密码锁（stream cipher）系统的主要弱点。以同样的 RC4 密钥串加密帧时，对两个加密过的封包做 XOR 运算的结果是相同的。只要对帧主体的结构分析两个相邻的串，攻击者即可得知明文帧的内容。为了避免重复使用密钥串，WEP 利用 IV 对不同的封包以不同的 RC4 密钥进行加密。不过，IV 属于封包标头的一部分，而且本身并未加密，因此窃听者仍能够从相同的 RC4 密钥所加密的封包中找出线索。

实际上种种问题的推波助澜，更进一步削弱了系统的安全性。802.11 认识到，使用相同的 IV 对大量帧进行加密并不安全，必须加以避免。所以 802.11 标准允许每个帧各自使用不同的 IV，但并未强制要求。

WEP 包含了完整性检查，不过其所使用的算法为循环冗余码（cyclic redundancy check，简称为 CRC）。个别 bit 若遭到篡改，十之八九均可通过 CRC 检测得知，然而它并不具备密码学上的安全性。密码学上，安全的完整性检查码（secure integrity check）是以杂散函数为基础，因为杂散函数无法预测。只要使用不可预测的函数，即使攻击者仅改变帧中的一个 bit，完整性检查码也会以不可预测的方式而有所改变。如此一来，就算攻击者想利用相同的完整性检查码找出更改的帧，其机会不仅微乎其微，也不可能马上完成。从密码学的角度来看，CRC 检验码并不安全。CRC 是相当直接的数学运算，而且要预测改变一个 bit 如何影响 CRC 的结算结果，其实是十分容易的。（这个属性通常会被压缩过的数据拿来修复文档！如果只有一些 bit 受损，有时候可以从 CRC 值发现并加以更正。）

5.3.2 WEP 统设计上的瑕疵

知道加州柏克莱大学的「网际网络安全、应用、认证与加密」（Internet Security, Applications, Authentication and Cryptography，简称 ISAAC）小组针对 WEP 标准所作的初步分析报告出炉后，WEP 设计上的瑕疵才被突显出来。研究人员在 WEP 中所发现的问题，没有一个是和 RC4 的破解有关。以下是已知问题的总结，有些问题前面已经提过：

1. 人工管理密钥是问题的症结之一。抛开发送相同密码给所有使用成员的庞大工程不说，安全上的顾虑就足以让人恶梦连连。新的密钥必须在某个特定时刻发送给所有系统，而只要有任何使用 WEP 的成员离开公司，基于安全上的考虑，实际的做法必然倾向于重新发送密钥。广为人知的秘密通常不算秘密。只要取得 WEP 密钥就能够进行被动式窃听攻击

(passive sniffing attack)，而密钥通常不会经常更改。一旦取得 WEP 密钥，窃听攻击就变得十分容易，特别是在 802.11 分析软件纳入解密功能之后。

2. 标准的静态 WEP 只提供长度 40 个 bit 的密钥。长久以来安全专家一直质疑长度 40 个 bit 密钥的适当性，有些专家建议至少以长度 128 个 bit 的密钥来保护重要数据。自从 WEP 的瑕庇被披露以来，业界标准所提供的密钥长度，最多只到 104bit。
3. 一旦重复使用密钥串，串流密码锁就容易被识破。WEP 采用 IV 的方式，让攻击者得以在密钥串的重复使用中找出蛛丝马迹。更糟的是，拙劣的产品如果没有采用随机 IV，就会使问题更形严重。Berkeley 小组发现，市面上居然有一张网络卡将 IV 由 0 开始起算，而后每个帧的 IV 值逐一递增。此外，可供运用的 IV 值 (IV 空间) 并不大 (小于一千七百万)，因此在忙碌的网络上必然会产生重复的现象。
4. 如果不经常更换密钥，攻击者就可以采集柏克莱小组所谓的解密字典 (decryption dictionary)，亦即累积以相同密钥串流加密的大量帧。一旦采用相同 IV 的帧累积到一定程度，就算密钥没被发现，也可以从未加密的帧中推敲出更多的数据。不过系统与网络管理人员通常十分忙碌，偶尔更换一次密钥根本就是经常性的情况。
5. WEP 使用 CRC 进行完整性检查。虽然完整性检验值本身经过 RC4 密钥串加密，但是 CRC 并不具密码学上的安全性。完整性检查如果不够完备，就无法防范有心人士在神不知鬼不觉的情况下更改帧。
6. AP (access point) 具有解读帧的特权。理论上，攻击者可以诱骗 AP 重新发送经 WEP 加密过的帧，针对此特殊功能发动攻势。基站所收到的帧将会在解密后被重新传送到攻击者的工作站。如果攻击者使用 WEP，AP 还会以攻击者的密钥为之加密，反而为之助功。

5.3.3 针对 WEP 密钥的还原攻击

2001 年 8 月，Scott Fluhrer、Itsik Mantin 以及 Adi Shamir 联合发表了一篇名为《Weaknesses in the Key Scheduling Algorithm of RC4》(RC4 密钥排程算法弱点) 的论文。在该篇论文末尾，三位作者描述理论上如何攻击 WEP。攻击的重点在于 RC4 将密钥展开为密钥串的方式 (此一过程称为密钥排程算法) 所露出的破绽。

Fluhrer-Mantin-Shamir 攻击 (或简称为 FMS 攻击) 假定：已加密的承载数据 (encrypted payload)，它的第一个 bit 组是可还原的。对一些加密系统而言，这是相当大胆的假设。不过，由于 802.11 采用 WEP 来保护帧，而 802.11 帧本体却是以 SNAP 标头为首。因此，第一个 bit 组的明文 (cleartext) 恰为众所皆知的 0xAA (SNAP 标头的第一个 bit 组)。既然知道第一个 bit 组的明文，若与第一个已加密的 bit 组进行 XOR 运算，便可轻易推论出密钥串的第一个 bit 组。

该篇论文将攻击的焦点锁定在以 (B+3):FF:N 为格式的弱点密钥 (weak key)。每个弱点 IV (weak IV) 用来攻击该 RC4 密钥的某个特殊 bit 组。密钥 bit 组由零起算。因此，对应到密钥第零 bit 组的弱点 IV 格式即为 3:FF:N。第二个 bit 组必然是 0xFF；此外，虽然必须知道该密钥的第三个 bit 组，但其值不确定。

标准的 WEP 密钥内含 40 个秘密 bit，或可以视为编号由 0 至 4 的 5 个 bit 组。在以标准 WEP 做为防护的网络中，弱点 IV 的第一个 bit 组必然不出由 3 (B=0) 到 7 (B=4) 的范围，而第二个 bit 组的值必定为 255。虽然必须特别标记第三个 bit 组，不过其值不确定。在静态 WEP 网络中，存在 $5 \times 1 \times 256 = 1280$ 个弱点 IV。这篇论文出版之后，陆陆续续被发现许多不同的弱点

IV，使得弱点 IV 的总数攀升至 9,000 个左右，相当于 IV 总数的 5%。这些新发现的弱点主要取决于 IVbit 组之间的关系，感兴趣的读者可以参考 WEP 破解工具的源码。

每个弱点 IV 所泄露的信息，和密钥的某个特定 bit 组有关。应用概率论，Fluhrer、Mantin 以及 Shamir 预测：要确定一个密钥 bit 组大概需要解析 60 个案例。最糟糕的是，一旦破解愈多 bit 组，攻击的速度就会愈快。破解第一个密钥 bit 组有助于破解第二个，依此类推。积小胜多，总体而言，攻击是以线性时间进行。将密钥长度加倍，攻克的时间也只是以等比例的方式增加。

既然理论如此诱人，对实际系统发动攻击不过是时间早晚的问题。2001 年 8 月初，Adam Stubblefield、John Ioannidis 以及 Avi Rubin 应用 FMS 理论，对一套试验性质的实际网络进行攻击，结果相当令人震惊。在他们的测试中，确定一个密钥的 bit 组通常需要解析 60 个案例，而完全破解密钥也大概只需要 256 个案例。从订购无线网卡到找出完整的密钥，实际攻克的时间不超过一个星期。编写攻击程序只需要几个小时。破解密钥大概需要五六百万个封包，这对不算忙碌的网络而言也不过是个小数目。

不过，和公开的破解程序码起来，破解报告可说是微不足道。Fluhrer/Mantin/Shamir 提出的攻击方式在事项上并不困难，棘手之处在于如何找出 RC4 的弱点，2001 年 8 月底，一套可以还原 WEP 密钥的开放源码程序 AirSnort 问世，随后也陆续出现许多类似工具。

分层式安全协议

写作本书第一版时 WEP 被视为一种不安全的安全系统。古老而又需要人工传递、使用静态密钥的 WEP 基本上已遭破解。当大家逐渐了解 WEP 所能提供的防护相对有限，且不足以保护大多数网络环境之际，有个任务小组就此成立，负责加强 MAC 的安全性。该工作小组的工作成果最后在 2004 年 6 月成为 802.11i 标准。

在研究证实 WEP 存在瑕疵与开发出较安全的技术以便防堵之前。网管人员只能转而采用已经证明，位于较上层的安全协议，比如 IPSec（第三层）、SSL（第四层）以及 SSH（第七层）。既然静态 WEP 只能提供最低限度的安全性，较上层技术在加密上所提供的额外保护便有其价值。

随着较牢靠的链路层技术的发展，分层式安全协议不再像以前那样具有魔弹（magic bullet）的效果。要使用 IPSec，必须先安装、设置用户端软件。采用 SSL 的 VPN 在设置上比较简单，不过在非网页应用上则有其缺点。SSH 较为人所知，而且可以任意产生 TCP 传输通道（TCP tunnel）。不过通常需要大幅修改应用程序。（当各位阅读本书时，可能已经习惯使用 ssh；不过，或许各位并不希望让使用者深陷苦海。）

随着本章与下两章所探讨的链路层安全技术的发展，现在我们终于能够在链路层打造安全的网络环境。一种日渐普及、用来建构安全无线网络的做法是，首先考虑这些新技术的特点，然后再决定需要在上层协议中加入那一种额外防护。如何在这些取舍间找出平衡点，乃是本书与部署相关章节的主要课题。

5.3.4 防范密钥还原攻击

较长的密钥并无助于防范密钥还原攻击。还原密钥所需要的时间，可以分为搜集攻击所需足够帧的搜集时间，以及执行程序得出密钥所需的计算时间。计算时间花不到几秒钟，搜集时间才是主导攻击的因素。较长的密钥需要稍微多一点计算时间，但搜集时间仍然维持不变。当密钥长度增加，就可以捕获更多弱点 IV。

有些厂商采用了一种防范机制，即避免使用弱点 IV。大多数厂商已经修改自家产品，在使用 IV 之前先行比对，若是属于弱点 IV 则以非弱点 IV 替换。遗憾的是，限制 IV 空间的结果，将导致 IV 重复使用的情况更容易发生。

网管人员可以使用比较牢靠的协议，比如第七章所探讨的 802.11i，来应付密钥还原攻击。对某些组织而言，这是一种解决方案。不过，新的协议不见得像动态 WEP 一样与既有设备相容。为了减少使用 WEP，如果更换密钥对网络造成的负担在可接受范围，大多数网管人员都会将之设置为 5 至 15 分钟。

5.4 动态 WEP

随着注目的焦点开始转向安全性，业界随即着手开发能够显著改善安全性的无线局域网络技术。第一步是通过动态密钥更新以弥补 WEP 不足。动态 WEP 使用的是一组不同的密钥，而不是让网络上所有工作站共用一把静态密钥来加密所有帧。实际的做法是，网络上所有工作站使用一把密钥来加密广播帧，但个别工作站使用自己的配套密钥来加密单点传播帧。

WEP 并未制定出一套密钥管理架构。密钥的产生与传递，是通过一组 802.11 未曾明文规定的系统。最早也是最简单的密钥管理架构，就是通过人工的方式。网管人员必须指定一串 bit 做为密钥，然后将之传递给位于相同 802.11 服务组合的所有工作站，要设置密钥，网管人员必须亲自搞定需要设置的机器。

动态 WEP 使用经过改良的密钥管理架构。它使用较坚固的加密协议来产生密钥，同时通过加密以便在不安全的网络上传递密钥，不再凡事依赖网管人员手动完成。WEP 密钥的产生，通常会运用到下一章所探讨的加密认证协议。

动态 WEP 处理帧时，和静态 WEP 采取的方式相同。唯一的差别在于，前者使用经过改良的机制，每隔一段时间就会产生并传递新的密钥。动态 WEP 所采用的自动密钥管理机制，相对于静态 WEP，能够提供更好的安全性，因为它动态地缩短了每把密钥的使用时间。更新密钥后仍可使用原本本地帧初始向量，因为两者对应到不同地 WEP 种子。如此一来，通过 Fluhrer/Mantin/Shamir 所进行地密钥还原攻击，就必须在同一把密钥的使用期间完成。动态 WEP 并不完美，不过比起静态 WEP 已有显著地改善。几乎所有网卡驱动程序均已支持动态 WEP。

第6 章 802.1X 使用者身份认证

你叫什么名字？

你在寻找什么？

你最喜欢的颜色是？

一守桥者 (Bridgekeeper)

圣杯传奇 (Monty Python and the Holy Grail)

过去几年，安全性一直是无线局域网络相关报导的主题。一些民调显示，网络管理人员认为，安全性乃是无线局域网络能否广为接受的最大障碍。许多安全问题，其实可以追溯到 WEP 设计上的瑕疵。

静态 WEP 企图同时解决好几个问题。它既打算提供身份认证 (**authentication**)，限定拥有特定密钥方能进行网络访问，也想要提供私密性 (**confidentiality**)，当数据行经无线链路时予以加密。最后分析发现，它在两方面的表现都不是特别好。身份认证与私密性都是无线局域网络的重要议题，也是本书第一版问世后许多技术发展的重点。

本章主要探讨身份认证，它是 802.1X 在链路层所提供的机制。^{【注 1】}本书第一版问世以来，802.1X 已经成熟许多，并且逐渐成为无线局域网络上身份认证协议的首选。

^{【注 2】}静态 WEP 只是对拥有加密密钥的机器进行身份认证。802.1X 则允许网管人员对使用者而非机器进行身份认证，同时可以确保使用者连接至合法、经过授权而非窃取个人数据的冒牌网络。

辨识使用者（而非机器）的身份，可以让网络架构更有效率。如此一来，就没有必要以功能别来区分使用者，或者对实体位置上的实体连接埠实施安全管制。相反地，使用者身份与访问权限均可整合到网络的交换结构当中，并且一路伴随使用者。无线局域网络通常会首先强制采用身份识别政策。公司行号通常是在使用一阵子后发现无线网络的好处，然后希望将它整合到有线网络。不论使用者置身何处，或者使用何种方式连上网络，身份识别政策均可如影随形。

802.1X 复杂之处，在于它本身只是一套架构。它是 IEEE 采用 IETF 的可延伸身份认证协议 (Extensible Authentication Protocol，简称 EAP) 制定而成。EAP 属于一种架构协议，最初规范于 RFC 2284，后来经由 RFC 3748 的更新。EAP 本身并未规范如何辨识使用者，但允许协议设计人员打造自己的 EAP 认证方式 (EAP method)，亦即用来进行交换过程的子协议。EAP 认证方式可以有不同目的，因此通常根据特殊情况的需求，采用不同的方式来辨识使用者的身份。不过在详细探讨不同认证方式之前，必须先了解 EAP 的运作方式。

【注 1】802.1X 由的 X 以大写表示。在 IEEE 的命名原则里，小写字母（比如 802.11a 和 802.11b）保留给修订既有标准的附加规格使用。大写字母则用加独立的规格。既然 802.1X 本身是个完整独立的协议规格，因此以大写字母来表示。

【注 2】我个人用来判断一项规格是否成熟的标准，就是有没有开放源码实现。开放源码软件通常扮演相当具有价值的角色，除了使专属实现产品不敢任意妄为 (*keeping proprietary implementations honest*) 以外，为使用者提供低成本的事实检验。在 802.1X 世界里，*xsupplicant* 和 *wpa_supplicant* 专案就属此类。

6.1 可延伸身份认证协议 (EAP)

802.1X 的基础是 EAP。由于近来无线网络的发展，原本的 EAP 标准已经不再使用，更新后的版本见于 RFC 3748。当 PPP 在 1990 年代初期问世时，有两种协议可用来辨识使用者的身份，两者都会用到 PPP 协议编号。身份认证不可能「一体适用」(one size fits all)，当时算是相当活络的研究领域。IETF 并未扬弃可能就此无用的 PPP 协议编号，而是制定了 EAP 标准。EAP 是一种简单的封装方式，可以执行于任何的链路层，不过它在 PPP 链路上并未广泛使用。EAP 的基本架构如图 6-1 所示，在设计上是为了能够执行于任何的链路层，以及使用各种的身份认证方式。

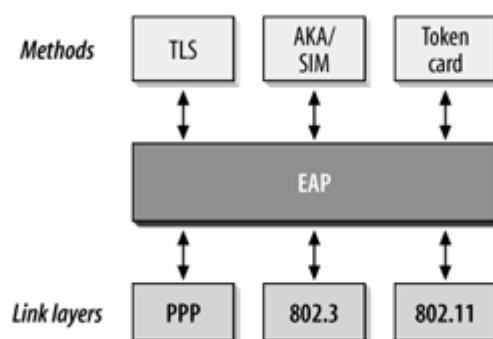


图 6-1: EAP 的架构

6.1.1 EAP 的封包格式

EAP 的封包格式如图 6-2 所示。搭配 PPP 链路使用时，EAP 是由 PPP 帧所承载，协议编号为 0xC227。EAP 并不是非得执行在 PPP 之上，图 6-2 的封包可以通过任何一种帧来承载。EAP 封包包含下列字段：

- **Code** (类型代码)

封包的第一个字段是 **Code** (类型代码) 字段，其长度为一个位元，代表 EAP 封包的类型。封包的 **Data** (数据) 字段必须通过此字段来诠释。

- **Identifier** (识别码)

Identifier (识别码) 字段长度为一个位元。其内容为一个无符号整数，用来对映要求与回复。重传时会使用相同的 **identifier number** (识别码编号)，新的传送则使用新的 **identifier number**。

- **Length** (长度)

Length (长度) 字段本身占有两个位元。它记载了整个封包的总位元数，包括 **Code**、**Identifier**、**Length** 以及 **Data** 等四个字段。在某些链路层协议中，有时可能必须填空补零 (padding)。EAP 会假定所有超过 **Length** 字段所记载之长度的数据，均是链路层额外添加的，因此可以忽略不计。

- **Data** (数据)

最后一个也是 **Data** (数据) 字段。其长度不定，取决于封包类型，**Data** 字段也可能不占任何位元。**Data** 字段如何诠释，完全取决于 **Code** 字段的值。

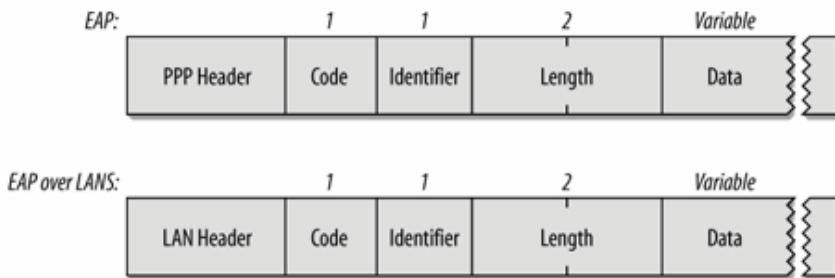


图 6-2: EAP 的封包格式

6.1.2 EAP 的要求与回复

EAP 的交换过程系由要求 (request) 与回复 (response) 所构成。认证者 (authenticator) 会送出要求给想要进行访问的系统，并根据所得到的回复，决定是否允许对方进行访问。如果认证者已经送出要求，用户端系统只能以回应封包答复，不允许发送多余的封包来要求身份认证。要求与回复的封包格式如图 6-3 所示。

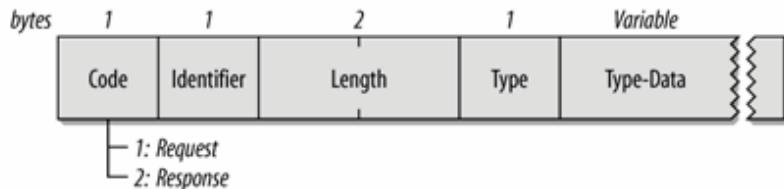


图 6-3: EAP 的要求与回复封包

Code 字段的值为 1 代表「要求」，2 代表「回复」。**Identifier** 与 **Length** 字段的用法，如上一节的基本格式所述。**Data** 字段用来携带「要求」与「回复」所使用的数据。每个 **Data** 字段将会携带一种数据，可再细分为 **type identifier code** (类型识别码) 以及 **associated data** (相关数据)：

- **Type** (类型)

Type (类型) 字段的长度为一个位元，代表「要求」或「回复」类型。每个封包只能使用一种类型。惟一的例外是，「回复」的 **Type** 字段与其「要求」须一致。亦即，当无法接受某个「要求」时，对方可以送出一个 **NAK**，提议使用不同的类型。大于或等于 4 的 **Type** 字段值，代表身份认证方式。

- **Type-Data** (类型一数据)

Type-Data (类型一数据) 字段长度不定，必须根据每种类型的规则加以诠释。

6.1.2.1 类型代码 1: identity (身份证明)

认证者通常会以 Identity (身份证明) 类型作为最初的要求，通常以 EAP-Request/Identity 来表示，或者简写为 Request/Identity，代表认证者试图建立某种使用者名称以便进行身份认证。通常 EAP Identity 即为使用者身份，或许附带一些路由信息。有些技术的运作方式是送出机器的 EAP 身份证明。在一开始的 Request/Identity 中，如果有任何信息出现在 Type-Data 字

段，就会被用来提示使用者，虽然这比较不常见。如果 Type-Data 字段存在并且包含提示字串，此字串长度可以从 EAP 封包的长度推论得知，不必另外使用界定符 (delimiter)。

有些 EAP 实现可以提示使用者（指人）输入必要的信息以判断其身份，虽然这并非必要。为了更便于使用，大多数 EAP 实现也允许静态设置身份。一旦知道使用者名称，EAP 用户端程序就会回复一个 Response/Identity 封包。Response/Identity 封包的 Type-Data 字段包含了使用者名称。它可以是「纯粹」的使用者名称，例如 mgast，或者附带 Internet 风格的域名名称 (mgastgdomain. com)，或者 Windows 风格的域名名称 (DOMAIN\mgast)。

有些 EAP 实现可能会在送出认证挑战 (authentication challenge) 信息之前，试图找出使用者的身份。如果使用者不存在，整个认证程序就算失败，不会再做进一步的处理。大部分的实现会再次送出身份数证明要求，以防使用者打字错误。

6.1.2.2 类型代码 2: Notification (通知)

认证者可以使用 Notification (通知) 类型传送信息给使用者。使用者的系统随后可用 Request/Notification 中的信息显示给使用者看。Notification 信息的用处，是由认证系统提供信息给使用者，例如密码即将过期，或者帐号遭锁定的理由。Notification 信息在 802.1X 中并不常用。Notification 要求必须得到回复，不过 Request/Notification 属于简单的回复，Type-Data 字段的长度为 0。

6.1.2.3 类型代码 3: NAK (负面回应)

Null acknowledgment (负面回应，简称 NAK) 用来提议，使用新的身份认证方式，认证者会在所送出的挑战 (challenge) 信息中，指定身份认证所使用的类型代码 (Type code)。身份认证类型的代码为 4 以上。如果使用者的系统不支持挑战所使用的身认证类型，可以回复 NAK 信息。NAK 信息的 Type-Data 字段，包含其所建议使用的认证类型。大多数 802.1X 实现并不会主动协商，如果用户端尝试使用不支持的类型，只会记录一个错误信息。

6.1.3 EAP 身份认证方式

除了流量控制与协商信息，EAP 也会为身份认证的方式指定类型代码。EAP 会把证明使用者身份的过程，授权给一个称为 EAP method 的附属协议，EAP method 乃是一组验证使用者身份的规则。

使用 EAP method 的优点是，EAP 从此可以不用去管验证使用者的细节。如果需求改变，这是无线网络普及之后常有的状况，就可以开发新的 EAP method 来满足这个需求。表 6-1 列出了一些 EAP method 以及它们的类型代码。无线局域网络常用的 EAP method 将于本章稍后详细说明。

表 6-1: 802.1X 身份认证常用的 EAP 认证方式 (EAP method)

类型代码	身份认证协议	说明
4	MD5 challenge	EAP 中类似 CHAP 的认证方式
6	GTC	原本打算搭配 RSA SecurID5 之类的标记卡 (token card) 一起使用
13	EAP-TLS	以数位凭证 (digital certificate) 相互认证
21	TTLS	管道式 TLS；以 TLS 加密保护较脆弱的身份认证方式
25	PEAP	防护型 EAP；以 TLS 加密保护较脆弱的 EAP 认证方式

18	EAP-SIM	使用移动电话的用户身份模组 (Subscriber Identity Module 简称 SIM) 卡进行身份认证
29	MS-CHAP-V2	Microsoft 之经加密的密码身份认证；相容于 Windows 网络

6.1.4 EAP 认证的成功或失败

在 EAP 交换程序结束之后，使用者不是认证成功，就是认证失败。一旦认证者判定整个交换过程已经完成，就会发出一个 EAP-Success (代码 3) 或 EAP-Failure (代码 4) 帧，以结束整个 EAP 交换程序。实现上，在送出认证失败信息之前，允许使用者送出多个要求信息，好让使用者有机会获得正确的认证数据。

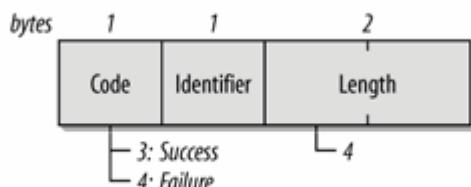


图 6-4: EAP 认证成功或认证失败的帧

无论是成功或失败帧都不会再经过任何形式的验证。在拨接的世界里，电话网络提供了某种程度的安全性，可以确保传送者必然位于线路的另外一端。在无线局域网络中，若要解决未能进一步验证 Success 与 Failure 帧的情况，可能需要额外的设计。

6.1.5 EAP 交换程序范例

EAP 交换程序范例如图 6-5 所示，这并不是无线网络上“实际”可见的交换程序，因为其中用到了一些未曾广泛部署的协议。举这个例子只是为了让读者对 EAP 协议的运作方式有个基本的概念。EAP 交换程序是一系列的步骤，以认证要求信息开始，以成功或失败信息结束。附带说明，在 EAP 认证方式交换过程中，由认证者所发送的封包是以 Request/Method 表示，如果是用户端所答复的回应则以 Response/Method 表示。

1 认证者 (authenticator) 发出一个 Request/Identity (要求/身份证明) 封包以辨识使用者身份。Request/Identity 有两个目的。除了启动交换程序外，也用来告诉用户端，在身份认证完成之前将会丢弃任何传输数据。

2 用户端要求使用者输入识别码，随后将所搜集到的使用者识别码以 Response/Identify(回复/身份证明) 信息送出。

3 一旦认出该使用者，认证者随即会送出认证查验。在本图第三个步骤中，认证者以一个 Request/MD-5 Challenge (要求/MD-5 挑战) 封包送出 MD-5 Challenge (MD-5 挑战) 给使用者。

4 用户端在设置上是以 token card (标记卡) 进行身份认证，因此它会送出一个 Response/NAK (回复/负面回应) 信息，提议以 Generic Token Card (一般标记卡) 作为认证机制。

5 认证者会送出一个 Request/Generic Token Card (要求/一般标记卡) 的挑战，要求取得卡号 (numerical sequence on the card)。

6. 使用者键入卡号，通过 Response/Generic Token Card (回复/一般标记卡) 送回。

7 使用者的回复并不正确，因此认证失败。不过，这个认证者在 EAP 的实现允许多次认证机会，因此会送出第二个 Request/Generic Token Card（要求/一般标记卡）的挑战。

8 使用者再度回复，依然通过 Response/Generic Token Card（回复/一般标记卡）传递。

9 此次的回复正确因此认证者发出一个 Success（成功）信息。

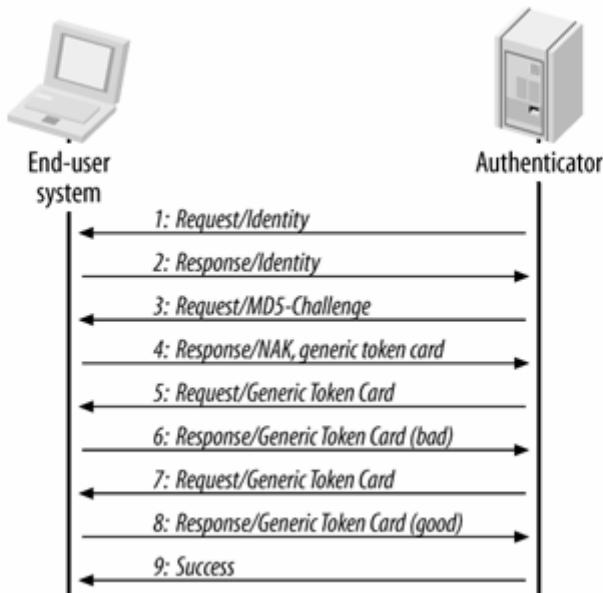


图 6-5：EAP 交换程序范例

6.2 EAP 认证方式 (EAP Method)

可延伸性 (EAP 当中的 E) 既是 EAP 最大的优点也是最大的缺点。可延伸性让协议得以在新的需求浮现时开发新的功能。正因为本身的可延伸性，EAP 已经从保留 PPP 协议编号的方式，转变为无线局域网络的安全防护基础。不过，要正确部署 EAP 可能不容易，因为要选择正确的协议选项之前必须先理清一大堆问题。EAP 之所以具有弹性，关键在于它本身只是一个架构。当新的需求浮现，就可以设计出新的认证方式，就算要用于无线局域网络也不成问题。

无线局域网络之安全防护协议这个议题十分广泛，本章试图一点一滴 (bit-by-bit) 勾勒出协议运作机制的细节。很多复杂的细节只会以文字来描述，不会用详细的封包格式图来说明。

6.2.1 加密的方式

EAP method 的选择通常取决于后端所使用的身份认证系统。早期的 EAP method 主要将焦点摆在如何提供与认证服务器间的传输管道。针对无线网络所设计的新型认证方式，除了可以跟认证服务器进行沟通，也符合无线局域网络特有的三项要求：

为使用者的数据提供坚固的加密防护

定义上，无线局域网络应该被视为一种开放介质。若要确保安全，任何通过无线网络传送的数据均须加以保护。大多数针对无线局域网络所设计的 EAP method 均采用 TLS 来提供私密数据的加密防护。

相互认证

早期无线局域网络协议的设计，将身分认证视为基站对使用者提出的要求。随着基站价格的滑落，如今攻击者已经能够部署「伪装」（rogue）的基站，用来窃取用户的私密数据。依常理判断，除了使用者的身份认证，用户端设备还必须验证它们所连接的网络是否正确无误。

衍生密钥

使用事先约定密钥的 WEP 机制，无法为电波链路上的帧提供多少保护。较坚固的安全防护协议必须使用由乱数集区（entropy pool）衍生而成的动态密钥。提供坚固之加密防护的副作用是，此类协议还会产生一份共享的加密串流，可用来传递密钥给链路层安全防护协议。

6.2.1.1 LEAP

Cisco 专属的 Lightweight LAP（轻量级 EAP，简称 LEAP）^{【注】}是最早广泛使用的无线网络身份认证方式。相对于通过手动方式设置密钥的 WEP，LEAP 可说是往前迈进了一大步，虽然它还有很多地方有待改进。基本上，LEAP 进行了两次 MS-CHAP Version 1 交换程序。第一次由使用者对网络进行验证，第二次由网络对使用者进行身分认证。动态密钥是衍生自 MS-CHAP 交换程序。

一些最糟糕的安全问题都是由 MS-CHAP version 1 所引起的。MS-CHAP version 1 有一些安全上的问题，容易导致字典式攻击。攻击 LEAP 弱点的程序码，目前已经广泛流传。

LEAP 算是一种过渡性的解决方案，虽然相较于手动设置密钥的 WEP 在安全性上有显著的优点，不过使用过时的 MS-CHAP 作为核心反而缩短了它的使用寿命。等到其他协议陆续问世，LEAP 就没有存在的必要了。目前，Cisco 建议使用 PEAP 或者 EAP-EAST 作为替代。

6.2.1.2 类型代码 13：EAP-TLS

Transport Layer Security（简称 TLS）协议原本就是设计来用在易遭窥视的链路层上。TLS 的前身是保护网际网络交易安全的协议 Secure Socket Layer（简称 SSL）。从许多方面来看，无线局域网络的使用案例（use case）与网际网络类似。数据必须在完全不可信赖且攻击者立的网络环境中进行传送。TLS 的目的，就是在不可信赖的网络环境中建立一条可信赖的沟通管道。

TLS 通过凭证交换来进行相互认证。使用者必须将数位凭证递交认证服务器以进行验证，但是认证服务器也必须提供本身的凭证。通过可信赖的凭证发行机构验证服务器的凭证真伪，用户端就可以确定所连接的网络经过凭证发行机构授权无误。

EAP-TLS 是第一个符合无线网络三项要求的身份认证方式。凭证提供牢靠的「使用者对网络」以及「网络对使用者」双向认证。相互认证可以防范所谓的「假」（rogue）基站，让用户端得以判定基站是否由正确的部门，而非为了窃取密码的有心人士所设立。TLS 还会建立一组主密码（master secret），用来衍生出链路层安全防护协议所需要的密钥。

EAP-TLS 虽然安全，不过并未被广泛使用。无线网络中任何潜在的用户都必须配备本身的数据凭证。产生与传递凭证以及遵循验证程序都是莫大的挑战。已经采用公开密钥基础建设（public key infrastructure，简称 PKI）的机构如要使用 EAP-TLS 就相当容易；有些机构并不想组建 PKI，而另外选用别种方式。

6.2.1.3 类型代码 21：EAP-TTLS 与类型代码 25：EAP-PEAP

实际上，需要使用 PKI 是无线局域网络上推行坚固的身份认证时主要的障碍。PKI 不论在技术或者程序上都是一项艰巨的任务。大多数的组织宁可利用现有的身份认证系统，例如 Windows domain 或 Active Directory，LDAP directory，或者 Kerberos realm。使用现成的帐号比起重

新建立一套平行的身份认证系统来得简单。有两种 EAP method 能够搭配所谓的“旧式身份认证方式”一起使用，分别是管道式 TLS (Tunneled TLS，简称 TTLS) 与防护型 EAP (Protected EAP，简称 PEAP)。

TTLS 与 PEAP 的运作方式类似。首先，协议会使用类似 EAP-TLS 的方式建立起一个 TLS 管道。进行下一个步骤之前，会先使用认证服务器的数位恋证来验证此网络是否可受信赖。第二个步骤是使用 TLS 管道为旧式的身份认证协议加密，然后以之验证使用者身份。有时候第一个步骤也称为「外层」(outer) 身份认证，因为它是用来保护第二个或者「内层」(inner) 身份认证的管道。

【注】有些以 *EAP-Cisco Wireless* 来称呼 LEAP。

认证还是免不了，但只有外层身份认证需要用到。TTLS 与 PEAP 将凭证数目从千百张缩减为屈指可数，只有认证服务器需要使用凭证。这就是为什么 TTLS 与 PEAP 远比 EAP-TLS 受到欢迎。一般机构可以自行设立小型的凭证管理中心，不必依赖外部凭证机构所签发的昂贵凭证。

TTLS 与 PEAP 之间有些微的差异，在于内层身份认证的处理方式。TTLS 使用加密管道来交换 attribute-value pair (「属性-值」对，简称 AVP)，PEAP 则是在管道内进行第二次 EAP 交换程序。采用 AVP 使得 TTLS 较具弹性，因为 AVP 可用来执行 EAP method 未提供的身份认证方式。

使用 TTLS 与 PEAP 的好处是，内层与外层身份认证可以使用不同的使用者名称。这两种协议在进行外层身份认证时可以匿名进行，只有在加密管道中才会显示使用者的真实身份，如此一来就不会在未经加密的帧中暴露使用者名称。不过并非所有用户端软件均可隐藏使用者的身份。

6.2.2 非加密式 EAP 认证方式

若无坚固的加密防护，有些 EAP method 并不适合直接用于无线网络。不过，它们可以作为 PEAP 或 TTLS 的内层身份认证方式。

6.2.2.1 类型代码 4: MD-5 Challenge (MD-5 挑战)

MD-5 Challenge (MD-5 挑战) 相当于 RFC 1994 所规范的 CHAP 协议。身份认证要求中包含了给用户端的挑战。用户端只要能够成功回应挑战，就可以证明它的确握有共享密钥。所有的 EAP 实现必须支持 MD-5 Challenge。不过，它在无线网络领域并未得到广泛使用，因为它无法在无线网络上提供动态密钥。

6.2.2.2 类型代码 6: Generic Token Card (一般标记卡)

RSA 公司的 SecurID 以及 Secure Computing 公司的 Safeword，这一类的 Token card (标记卡) 在某些机构里特别受到欢迎，因为它们 (以「随机」的方式) 提供类似抛弃式密码的安全性，但是没有单次密码 (one-time password，简称 OTP) 的种种麻烦。在「要求」信息中包含了身份认证所需要的 Generic Token Card 信息。要求信息的 Type-Data 字段长度必须大于零。在「答复」信息里，Type-Data 字段用来携带复制自 token card 的信息。在「要求」与「回复」封包里，EAP 封包的 Length 字段则是用来计算 Type-Data 要求信息的长度。

EAP-GTC 与 EAP 标准同样规范于 RFC 2284。它允许通过网络交换明文身份认证数据。除了搭配标记卡使用 EAP-GTC 通常会被当成以“使用者名称十密码”进行身份认证的 EAP 认证方式。如果数据库中既有的使用者帐号具有只能进行比较但无法读取的单向加密密码 (one-way encrypted password)，EAP-GTC 将能提供用来验证使用者身份的 EAP 认证方式。当然，如果想要以 EAP-GTC 来传输可重复使用的密码，那么你必须使用管道加以保护。

6.2.2.3 类型代码 29: EAP-MSCHAP-V2

Microsoft CHAP version 2 (简称 MS-CHAP-V2) 最早出现在 Windows 2000 过程系统, 规范于 RFC 2759。它被设计来解决 MS-CHAP 的缺陷, 除了移除旧式用户端进行密码编码时的弱点, 还提供相互认证以及改善密钥产生与更换的机制。

MS-CHAP-V2 广泛使用于 Microsoft 工作站, 通常作为内层身份认证方式, 并搭配 PEAP 一起使用。MS-CHAP-V2 是 Windows 网络最常见的内层身份认证方式。当作 EAP 认证方式使用时, EAP-MSCHAP-V2 可以搭配 TTLS 或者 PEAP 一起使用。

6.2.2.4 类型代码 13: EAP-SIM 兴类型代码 23: EAP-AKA

还有两种值得注意的 EAP 认证方式: LAP-SI_M 与 EAP-AKA, 它们已经通过标准制定程序, 主要是通过移动电话数据库进行身份认证。EAP-SIM 为 GSM 电话网络上的 SIM 卡数据库提供了一个界面。EAP-AKA 则是基于第三代移动电话网络上所使用的身份认证系统, 称为 Authentication and Key Agreement (简称 AKA)。

EAP-SIM 与 EAP-AKA 对想要以移动电话帐号整合计费功能的电信公司而言特别有用。他们可以使用现成的智慧型芯片以及使用者帐号来验证使用者的身份, 使用者不必另外指定新的密码即可访问数据网络。

6.2.3 其他的内层身份认证方式

TTLS 并不是只能搭配 EAP method 作为内层的身份认证方式。因此, 有些较旧的身份认证方式也可以搭记 TTLS 一起使用。有些网络存放用户数据库的方式无法搭配 EAP method 一起使用, 因为没有任何的 EAP method 能够提供可用的界面。

6.2.3.1 密码身份认证协议 (PAP)

PAP 规范于 RFC 1334, 原本是设计来搭配 PPP 一起使用。PAP 以未经加密的方式在网络上传递使用者名称与密码。PAP 不能直接使用于无线网络, 只能作为 TTLS 里的内层认证方式, 以确保不致泄露密码。

PAP 可以搭配任何类型的身份认证系统一起使用。网络登入可通过网络过程系统加以验证。标记卡 (token card) 服务器可用来验证明文标记码 (cleartext token code)。PAP 也可用于只能进行比较但无法读取的单向加密密码 (one-way encrypted password)。单向加密密码用在 Unix 的 /etc/password 密码档, 以及大多数的 LDAP 目录中 Kerberos 系统也是以单向加密来存放密码。

6.2.3.2 挑战磋商身份认证协议 (CHAP)

和 PAP 一样, CHAP 原本也是设计来搭配 PPP 一起使用, 规范于 RFC 1994。使用 CHAP 进行身份认证时, 认证服务器首先会发出挑战信息给用户端, 而用户端只要能够成功回应挑战信息, 就可以证明它的确握有共享密钥。

CHAP 原本是设计来避免以明文方式传递密码之类的安全问题。CHAP 的缺点是连接双方都必须知道明文密码。在服务器方面, 此密码要不是以明文方式存放, 就是尽管经过加密但有办法加以解密, 这样服务器软件方能将之还原为明文。

连接环境通常不会使用 CHAP, 除非既有的使用者数据库十分庞大, 而且所使用的就是 CHAP。

6.2.3.3 MS-CHAP, Version 1

MS-CHAP 是由 Microsoft 所设计，用来提供类似 CHAP 的功能，但是针对 Windows 过程系统提供加强型的功能。它是 Microsoft 的专属协议，不过规范于 RFC 2433。和 CHAP 不同，MS-CHAP 并不需要以明文方式将共享秘密存放于连接双方。MS-CHAP 将会使用 MD4 杂凑来存放使用者密码，而不是采用明文密码来作为共享的秘密。

有使用 Microsoft 身份认证数据库的环境中，MS-CHAP 比较有用。不过从安全性的观点来看，MS-CHAP 存在某些特殊的问题，除非必须支持相当老旧的 Microsoft 过程系统，例如 Windows 95/98，否则最好不要用。MS-CHAP 并不是 EAP method，只有 TTLS 才支持。

限制 EAP 认证方式

有些 EAP method 比较坚固。为了安全起见，有些设备厂商会在认证者当中限制可以使用的 EAP method。EAP-MD 5 通常列在 EAP 类型限制清单上，因为它比其他采用 TLS 的认证方式脆弱得多。

其实限制 EAP 认证方式并没有必要，实际上反而可能会妨碍良好的安全性。有些限制条件只允许采用 TLS 的管道认证方式（类型 13、21 与 25）。如果之后出现新的 EAP 认证方式，有些具备这项功能的实现产品预设上会予以禁用。允许调整限制条件或许是可行的解决方案。不过目前并未听说有这类实现产品出现。

从安全性的观点来看，限制 EAP 认证方式实际上并没有太大的价值。身份认证服务器可以强迫使用坚固的身份认证方式，拒绝那些使用脆弱方式的要求。不论如何，没有密钥素材就无法连接至网络。如果认证过程中无法产生所需要的密钥，有些基站就会将认证程序视为无效，并且将用户端踢出网络，要求对方重新进行身份认证。进行 EAP-MD5 身份认证，如果未能产生密钥，当基站解除用户端的连接时，就必须重新开始。

部分是因为这些问题，EAP 规格中并不允许限制 EAP 认证方式。RFC 3748 的 2.3 节，强制要求认证者必须将所有 EAP 认证方式转送给认证服务器处理。

6.3 802.1X：网络连接埠的身份认证

局域网络在 1990 年代被广为使用，其连接埠也如雨后春笋般四处涌现。某些形态的组织，例如大学，被要求开放的呼声所困扰。网络资源必须开放给使用者社群，不过社群本身并不固定。学生和其他网络使用者不同。他们经常游走于不同的电脑之间，而且没有固定的网络地址；他们会毕业，迁移，注册，离开校园，担任雇员，或因为其他改变而需要更改使用权限。虽然网络访问权限必须足以容纳整个变动不定的社群，不过学校的经费通常有限，因此如何防止未经授权的外来者访问网络变得十分重要。

简言之，要使用网络，必须经过登入程序。然而不只是学校受惠于此。经过身份认证方能访问网络资源，对 Internet 服务供应商而言早已司空见惯，企业之所以会被这种做法所吸引，主要是因为如此一来，雇用计划可以较有弹性。

在链路层（link layer）采用身份认证机制并不是什么新鲜事。网络连接埠的身份认证在拨接访问服务器上已经行之有年。大部分的机构早已采用各种机制，作为使用者身份认证之用，例如 RADIUS 服务器与 LDAP 目录服务。以 PPP over Ethernet（简称 PPPoE）的使用者认证，为 Ethernet 访问进行把关的做法并不难理解，不过如此一来会增加系统的负荷与复杂度。因此，

IEEE 采用 PPP 认证协议，据以开发针对局域网络的版本。最后出炉的标准称为 802.1X，即「连接埠网络访问控制」（Port-Based Network Access Control）。

6.3.1 802.1X 的架构及相关术语

802.1X 为认证对话程序定义了三个元件，如图 6-6(a) 所示。申请者（supplicant）是寻求访问网络资源的使用者机器。网络访问由认证者（authenticator）所控制；它扮演着传统拨接网络中访问服务器一样的角色。申请者与认证者在规格书中称为连接埠认证实体（Port Authentication Entities，简称 PAE）。认证者只负责链路层的身份认证交换程序，并不维护任何使用者信息。任何认证要求均会被转送至认证服务器（例如 RADIUS）进行实际的处理。

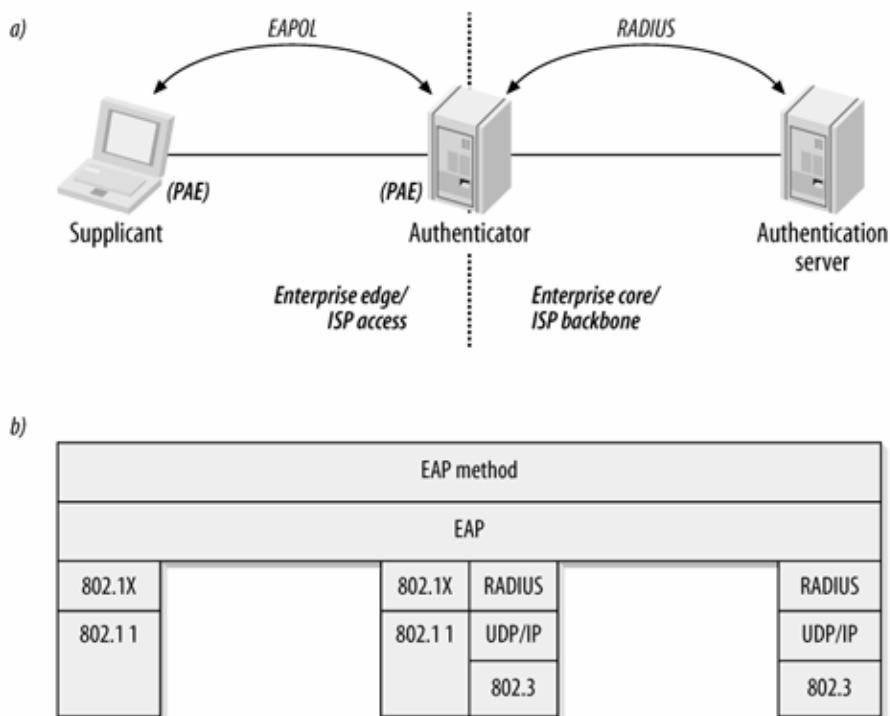


图 6-6: 802.1X 的架构

支持 802.1X 的设备上，各个连接埠若非处于授权状态（亦即可以使用该连接埠），就是处于未授权状态（亦即无法使用该连接埠）。不过就算处于未授权状态，规格书中还是允许使用 DHCP 以及其他初始化信息，如果网络管理人员允许的话。

整个身份认证交换程序在逻辑上是通过申请者与认证服务器来完成的，认证者只是扮演中介的角色。图 6-6(b) 所示为逻辑上的协议架构。申请者与认证者之间（即前端），使用由 802.1X 所定义的 EAP over LAN（简称 EAPOL）协议。在后端，则是通过 RADIUS 封包来传递 EAP。有些文献称之为 EAP over RADIUS。就算连接埠尚未得到授权，也尚未取得 IP 地址，申请者还是能够持续与 RADIUS 服务器进行 EAP 交换程序。

图 6-6 可以有两种不同的解读方式。在企业场合中，申请者乃是位于企业网络周边的一部主机，而 RADIUS 服务器则位于企业核心。本图同时显示了一家以 802.1X 认证使用者身份的 ISP，图左为 ISP 的访问范围，而图右则是 ISP 的骨干网络。

RADIUS 的好处是支持多种使用者数据库。除了本地的数据库，RADIUS 服务器也可以当成通往 LDAP directory、Unix NIS 或 PAM、Kerberos realms、Windows 使用者帐号、甚至是其他 RADIUS

服务器的闸道。RADIUS 相当有弹性，甚至可以用统一格式整合截然不同的使用者数据库。使用 RADIUS 在 Windows: domain 或者 Active Directory 上提供身份认证时，会有一些限制，这将于第 22 章加以探讨。

802.1X 只是一个架构，并非一套完整的规格。实际的认证机制，其实是通过认证服务器来完成的。802.1X 所提供的机制，主要是用来发出挑战信息以及确认或拒绝访问，实际上并不负责判断对方是否有权访问。改变认证的方式不需要大幅更动使用者的设备，或整个网络的基础建设。认证服务器可以重新设置配置，以便外挂其他新的认证服务，不必更换使用者所使用的驱动程序或交换器的韧体。

6.3.2 802.1X 的帧过滤

802.1X 要求任何数据通过之前，必须先通过身份认证，以此防范网络遭未经授权的使用者访问。处于未授权状态的连接埠通常限定只能传送身份认证帧，其他数据都会被丢弃。802.1X 标准对如何完成整个程序有正式的探讨。不过以本书而言，只要说明未授权连接埠会丢弃所有非 EAPOL 帧就够了。一旦工作站成功验证身份，就可以将数据帧送至适当的网络。

6.3.3 EAPOL 的封装格式

EAPOL 的基本帧格式如图 6-7 所示。目前有许多网络分析软件均可分析 EAPOL 的封装格式，包括 Ethereal。此帧的组成字段如下：

MAC 标头

图 6-7 所示为有线 Ethernet 以及 802.11 的封装格式。虽然 802.1X 帧中的承载数据 (payload) 相同，但是两者所使用的 MAC 标头并不一致。

Ethernet Type (以太网络类型)

和其他的 Ethernet 帧一样。Ethernet Type 字段包含了长度为 2 个位元的 type code (类型代码)，EAPOL 的类型代码为 88-8e。

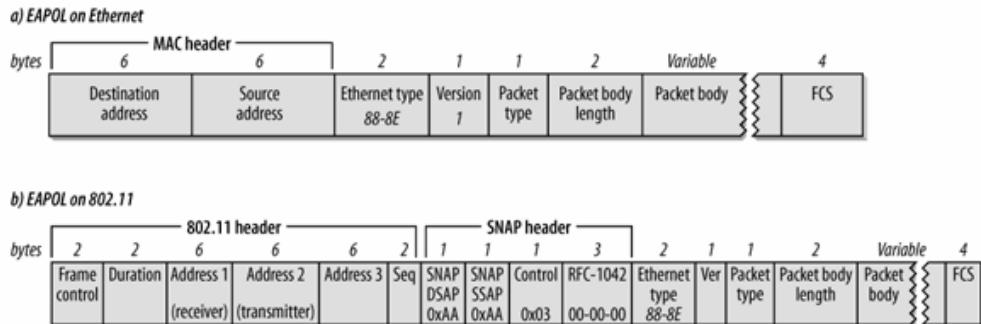


图 6-7: EAPOL 的帧格式

Version (版本)

第 1 版标准化于 2001 年版的 802.1X；第 2 版规范于 802.1X-2004。本章所描述的是 2001 年版，因为实现上比较常见。

Packet Type (封包类型)

EAPOL 是 EAP 的延伸。除了上一节所描述的 EAP 信息，EAPOL 还加入一些额外的信息，让 EAP 得以适用于连接埠导向的 LAN 环境。表 6-2 列出了所有封包类型及其说明。

表 6-2: LAPOL 帧的类型

封包类型	名称	说明
0000 0000	EAP-Packet	包含了一个经过封装的 EAP 帧。大部分的帧均属 EAP-Packet 帧。
0000 0001	EAPOL-Start	申请者可以主动送出 EAPOL-Start 帧，不必等候来自认证者的挑战信息。认证者会送出一个 EAP-Request/Identity 帧作为回复。
0000 0010	EAPOL-Logoff	当某个系统不再需要使用网络，便可发出一个 EAPOL-Logoff 帧，让连接埠重新回到未授权状态。
0000 0011	EAPOL-key	EAPOL 可用来交换加密密钥信息。
0000 0100	EAPOL-Encapsulated-ASF-Alert	Alerting Standards Forum (警告标准论坛，建成 ASF) 定义了一种方式，可让警告信息(例如 SNMP trap)通过此类型的帧传送给未经授权的连接埠。

Packet Body Length (封包主体的长度)

此字段本身的长度为 2 个位元，用来计算 Packet Body (封包主体) 字段的长度。如果没有封包内容，此字段的值为 0。

Packet Body (封包主体)

此字段的长度不定。EAPOL-Start 与 EAPOL-Logoff 信息除外，此字段会出现于所有的 EAPOL 帧中。EAP-Packet 帧所封装的是一个 EAP 封包，EAPOL-Key 帧所封装的是一把密钥，而 EAPOL-Encapsulated-ASF-Alert 帧所封装的则是一段警告信息。

6.3.4 定位

在类似 Ethernet 的共享介质中，申请者是将 EAPOL 信息送至 01:80:C2:00:00:03 这个群组地址。在 802.11 网络上并不存在类似的地址，而且只有在连接过程允许申请者(行动式工作站)以及认证者(基站)交换 MAC 地址之后，方能进行 EAPOL。

在 802.11 这样的环境里，EAPOL 会要求使用工作站的地址。

6.4 802.1X 与无线局域网络

802.1X 为任何局域网络，包括无线局域网络，提供了一个使用者身份认证的架构。就本书的目的而言，无线网络上 802.1X 中的连接埠，相当于无线设备与基站间的连接(association)。当链路层开始作用时，Association Request 与 Association Response 帧交换成功的信息会告知 802.1X 状态引擎(state engine)。一旦连接成功，工作站就可以开始进行 802.1X 帧交换程序，尝试取得授权。802.1X 身份认证交换程序与密钥传递完成后，使用者就会收到界面已经启用的信息。

6.4.1 802.11 网络上的 802.1X 交换程序范例

EAPOL 交换程序与 EAP 交换程序看起来几乎一样。主要的差别在于，申请者可以发出 EAPOL-Start 帧触发 EAP 交换程序，也可以在网络使用完毕后，发出 EAPOL-Logoff 信息解除连接埠的授权。本节的范例假定后端以 RADIUS 为身份认证服务器，因此范例中会显示认证者将来

自前端的EAP信息转换为后端的RADIUS信息。以RADIUS封包进行EAP身份认证，规范于RFC 2869。范例中亦显示出认证者系使用EAPOL-Key帧来传递密钥信息给链路层安全防护协议。图6-8所示为，在802.11网络上进行EAPOL交换程序的范例。此图所示范的是身份认证成功的例子，步骤如下：

- 1 申请者连接至802.11网络。连接只用到两个帧，这种简单的交换程序几乎都会成功。
- 2 申请者发出一个EAPOL-Start信息，开始进行802.1X交换程序。这个步骤并非必要。并非所有申请者都会送出EAPOL-Start信息，因此可能没有这个步骤。
- 3 “正常的”EAP交换程序开始。认证者（基站）发出一个EAP-Request/Identity帧。如果基站只为已经认证成功的连接转送帧，Request/Identity帧之前可能就没有EAPOL-Start。主动发出的Request/Identity帧用来指示申请者必须进行802.1X身份认证。
- 4 申请者以EAP-Response/Identity帧进行答复，此帧随后被转换为Radius-Access-Request封包送给RADIUS服务器。
- 5 RADIUS服务器判断需要使用那个类型的身份认证，并且在所送出的EAP-Request信息中指定认证方式类型。EAP-Request被封装于Radius-Access-Challenge封包送给基站。地台收到封包后。将EAP-Request传递给申请者。AP-Request信息通常会被表示为EAP-Request/Method。其中的Method代表所使用的EAP认证方式。如果目前使用的是PEAP，则传回的封包将以EAP-Request/PEAP来表示。
- 6 申请者从使用者方面取得回应，然后回传EAP-Response。认证者会将此回应转换为送给RADIUS的Radius-Access-Request封包，针对挑战信息所做的回应则存放于数据字段。
- 步骤5与步骤6不断重复进行，直到身份认证完成为止。如果所使用的是需要交换凭证的EAP认证方式，免不了要重复这些步骤几次。有些EAP交换可能需要在用户端与RADIUS服务器间，反覆进行10到20个回合。
- 7 既然RADIUS服务器送出一个Radius-Access-Accept封包允许对方访问网络，因此认证者会发出一个EAP-Success帧，并且授权使用连接埠。访问权限也可以由RADIUS服务器所回传的参数来决定。
- 8 收到Access-Accept封包后，基站会立即使用EAPOL-Key信息将密钥传给申请者。密钥的传递将于下一章讨论。
- 9 一旦申请者安装好密钥，就可以开始传送数据帧来访问网络。DHCP配置设置通常会在此刻进行。
- 10 当申请者不再需要访问网络，就会送出一个EAPOL-Logoff信息，使连接埠回复未授权状态。

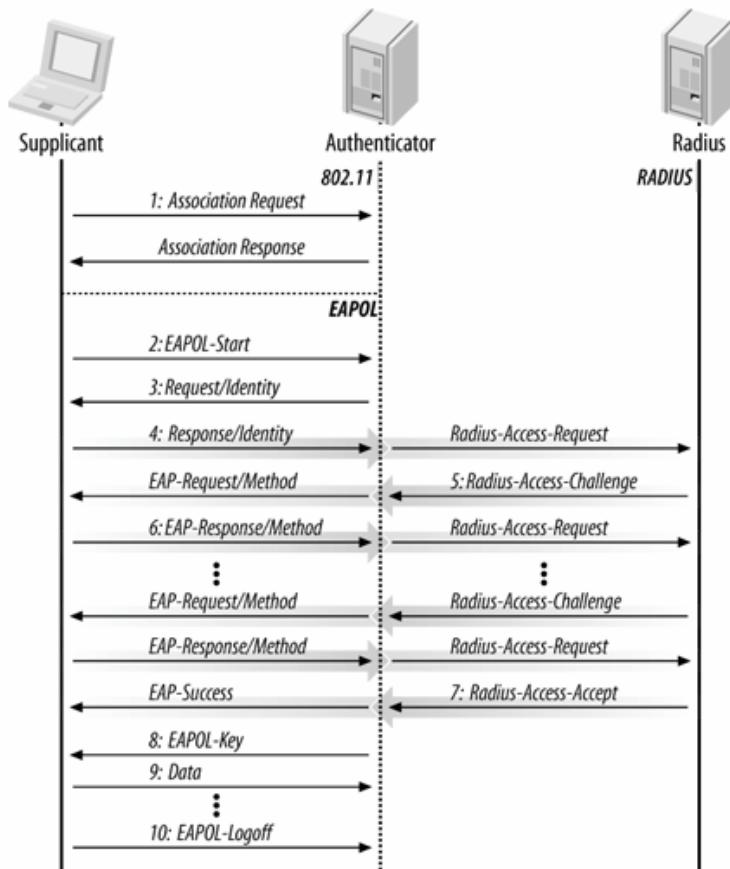


图 6-8: 802.11 网络上典型的 802.1X 交换程序

类似图 6-8 的交换程序可以在任何时间点进行。使用者并不需要发出 EAPOL-Start 信息来启动 EAPOL 交换程序。任何时刻，申请者都可以开始进行 EAPOL 交换程序，发出 EAP-Request/Identity 帧来更新认证数据。需要重新进行身份认证，通常是因为连接逾时，此时就必须更新密钥。

6.4.2 动态产生密钥

EAPOL-Key 帧让基站得以传送密钥给用户端，反之亦然。密钥交换帧只有在身份认证成功之后才会传送，如此可以避免密钥信息外泄。EAPOL-Key 帧也可以定期用来动态更新密钥。WEP 诸多弱点均肇因于长时间使用相同的密钥。如果很难为网络上所有工作站更新密钥，长期使用相同的密钥就在所难免。许多专家建议定期更换 WEP 密钥，不过一直没有实际的机制存在，至到 802.1X 问世之后，这个问题才得到解决。

第7 章 802.11i: RSN、TKIP 与 CCMP

802.1X 所提供的身份认证与密钥管理架构，解决了 WEP 在设计上的两项主要瑕疵。其他尚待解决的缺陷，主要是 WEP 的加密机制缺乏机密性。修正链路层加密协议的工作，是由 802.11 工作小组（working group）之任务小组（Task Group）I 负责。几经延迟，这项任务终于在 2004 年 6 月完成，可后正式成为标准。

802.11i 采双轨并行的做法以解决链路层加密协议的弱点。802.11i 组成自两种新的链路层加密协议。第一种称为 Temporal Key Integrity Protocol（临时密钥完整性协议，简称 TKIP），被设计来尽可能强化 pre-802.11i 硬件的安全性。另外一种则是重新打造的加密协议，称为 Counter Mode with CBC-MAC Protocol（「计数器模式」搭配「区块密码锁链—信息真实性检查码」协议，简称 CCMP），被设计来提供最高等级的安全性。

7.1 临时密钥完整性协议（TKIP）

第一种广为使用的新式链路层加密协议是「临时密钥完整性协议」（TKIP）。^{【注1】}开发 TKIP 的主要动机，是为了升级旧式 WEP 硬件的安全性。通常，具备 WEP 功能的芯片组均支持 RC4 加密机制。既然加密的重责大任是由硬件负责，那么只要通过软件或韧件，就可以达到升级的目的。TKIP 保留了 WEP 的基本架构与过程方式，因为它原本就是一个设计来升级 WEP 方案的软件。

7.1.1 TKIP 与 WEP 的差异

为了防范 WEP 易遭受攻击的弱点，TKIP 整合了许多新协议的功能。尽管保留了 WEP 的基本架构与过程方式，不过 TKIP 为 WEP 最易遭受攻击的弱点，另外绑上了「安全带」：

密钥阶层体系与自动密钥管理

不同于 WEP 直接使用单一主钥（master key）的做法，TKIP 使用到了多把主钥。最后用来加密帧的密钥，是由这些主钥衍生而来。另外，TKIP 也提供密钥管理过程，使得主钥的更新可以在安全的情况下进行。

为个别帧配钥（per-frame keying）

虽然 TKIP 保留 WEP 所使用的 RC4 帧加密机制，不过为了防范针对弱点密钥的攻击，它会为个别帧（从主钥）衍生出特有的 RC4 密钥。为每个帧准备独特密钥的程序，称为配钥（key mixing）。

序号计数器（sequence counter）

为个别帧编列序号，即可辨识出次序错乱的帧，如此便能防范所谓的重放攻击（replay attack），亦即攻击者先拦截有效封包，等候一段时间再予以重传的攻击。

新的「信息完整性检验」（message integrity check，简称 MIC）

TKIP 以一种比较牢靠，称为 Michael 的完整性检验杂凑算法，取代 WEP 所使用的线性杂凑算法。Michael 较为牢靠，检测伪造帧也更加容易。此外，来源地址受到完整性检验的保护，就可以检测出宣称来自特定来源的伪造帧。

信息完整性检验失败的反制措施

设计上，TKIP 是为了套用于现有的硬件，因此不免有所限制。Michael 可能遭受主动式攻击而被攻陷，因此 TKIP 包含了一些反制措施（countermeasure），以控制主动式攻击可能造成的损害。

此外，TKIP 也经常与基于 802.1X 的密钥管理协议并用，如此一来，就可以借由身份认证程序来产生 TKIP 主钥。

【注】制定标准的过程中，TKIP 原本称为 WEP2。当 WEP 最后被证明基本上存在瑕规，此协议就被更名为 TKIP，以便与 WEP 有所区别。

7.1.1.1 TKIP 初始向量的使用与配钥

WEP 的主要破绽，在于 WEP 的随机种子（seed）系由初始向量（initialization vector，简称 IV）以及 WEP 密钥所构成。既然随机种子是由 IV 与密钥串连而成，IV 本身就泄露了大部分的密钥结构。如此一来，攻击者就可以观察 IV 的重复使用情形，进一步挖掘出用以加密帧的相同密钥串。以 24-bit 的 IV 而言，大约可以容纳一千六百万（16 million）种帧。在比较繁忙的网络上，这个数目并不算多。更糟的是，此 IV 空间受限于当时所使用的密钥。如果使用静态 WEP，则 IV 空间是由网络上所有工作站所共享。何况，IV 本身构成密钥的前 24 个位元，早已众所皆知，难免会遭受第 5 章所提到的 Fluher/Martin/Shamir 攻击法所破解。

为了防范初始向量攻击，TKIP 将 IV 的长度从 24 位元为 48 个位元。如此一来，初始向量空间即由一千六百万（16 million）增加为二百八十一兆（281 trillion），可以有效防止 IV 空间在密钥的使用期限内耗尽。

TKIP 同时以配钥(key mixing)的方式来防范针对 WEP 的攻击。通过配钥，用来加个别帧的 RC4 密钥就会各自不同。在 TKIP 中，各个帧均会被特有的 RC4 密钥所加密。换句话说，配钥进一步扩展了初始向量空间，稍后对此会有更为详细的探讨。一旦配钥程序将传送者的 MAC 地址纳入计算，就算两部工作站使用相同的初始向量，也可以衍生出不同的 RC4 密钥来加密帧。此外，配钥亦有助于防范著名的 Fluhrer/Martin/Shamir 攻击。此类攻击要能奏效，必须搜集一些带有相同秘密位元的「弱点密钥」。只要各个帧使用不同密钥，TKIP 就能够防止攻击者搜集足够的数据，针对这些密钥发动攻击。

7.1.1.2 TKIP 序号计数器与重演攻击防护

除了空间变大之外，TKIP 初始向量本身也扮演序号计数器（sequence counter）的角色。每次安装新的主钥，初始向量/序号计数器就会被重设为 1。每传一个帧，序号计数器就会随之累加。

为了防范重演攻击(replay attack)，TKIP 会保留来自各工作站的最近序号。一旦成功接收到某个帧，就会以之与最近接收到的帧序号进行比对。如果大于前值就予以接受，否则就加以拒绝。

服务品质（quality of service）延伸功能系由任务小组 E 负责开发。目前 802.11e 草案中有一项区块回应(block acknowledgment) 协议。以单一帧回应多次传送。2005 年 1 月所出版的 802.11e 草案中规定，检测重演攻击之前，必须先完成因区块回应所导致的重新排序过程。

802.11 单点传播帧（unicast frame）必须加以回应。如果原始帧或其回应已经漏失，则该帧必须予以重传。在接收端，这就可能重复接收到相同的序号。序号重复，有可能只是因为连接出错，不必然就是有人正在进行主动式攻击。

7.1.1.3 Michael 完整性检验与反制措施

WEP 的完整性检验（integrity check）属于线性杂凑值，完全不适合加密应用。TKIP 在设计上所面临的主要挑战之一，就是在强化完整性检验的同时，还必须维持合理的效能。TKIP 设计当时，大多数 802.11 芯片组所使用的处理器功能都不够强，数学运算不够快，无法及时进行完整性检验。实现上，Michael 的实现方式完全是采用 swap、shift 之类的逐位元（bitwise）运算，甚至是通过丢弃特定位元的方式。因此，甚至在大多数 802.11 界面上所使用的微处理器，也不会对功能造成影响。（本章稍后将会详述 Michael。）

从 Michael 的设计，大致上可以看出它无法提供多少安全性。虽然远比循环冗馀检查码好，不过它还是无法抵挡持续执着的攻击。TKIP 整合了一些反制措施，以关闭网络与更新密钥来检测与因应主动攻击。

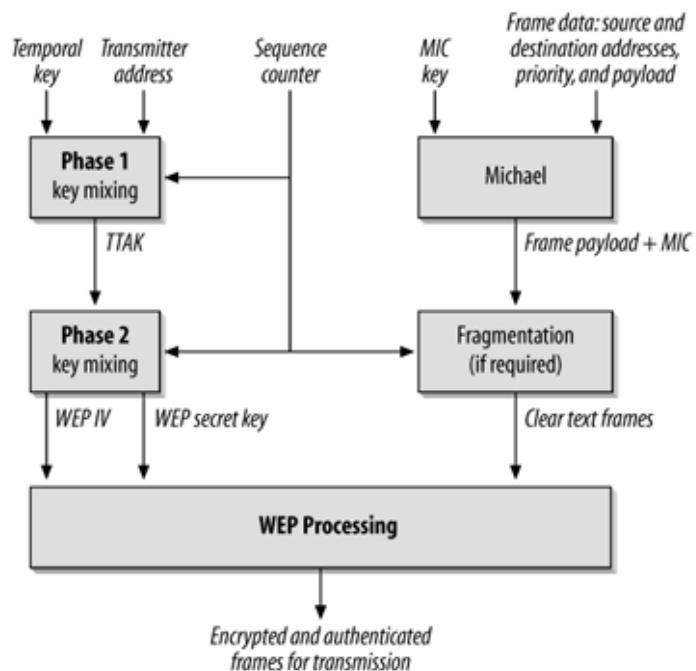
既然 Michael 需要准备反制措施，也就意味着底层所使用的密码学基础存在弱点。设计上，Michael 被迫必须与市面上目前采用 RC4 的大多数硬件相容。虽然存在上述种种限制，其实 Michael 的设计相当精致，也已经将功能发挥得淋漓尽致，不过它仍然是建造在浮沙上的高塔。Michael 是否够安全就留待时间说明；要是明年就出现针对它的攻击，我也会感到惊讶。不过，TKIP 在协议设计上的改良，有助于将恶意攻击的负面效果限制在某种范围。我认为 Michael 可能会屈服于阻绝服务（denial-of-service）攻击，但不致于导致大规模的网络失灵。

7.1.2 TKIP 的数据处理与过程

和 WEP 一样，TKIP 亦支持加密与完整性保护程序，如图 7-1 所示。从图中可以清楚看出，TKIP 可说是围绕著 WEP 而设计的一套安全功能。

TKIP 会以下列项目作为输入项：

- 帧。
- 用来加密帧的临时密钥（temporal key）。
- Michael 用来保护帧内容的 MIC 密钥。TKIP 会衍生出一对密钥，使得「工作站一至一基站」的 MIC 密钥不同于「基站一至一工作站」的 MIC 密钥。TKIP 与 WEP 不同之处，在于 MIC 使用了密钥。
- 传送端地址也会被当成 TKIP 的输入项，因为必须用它来进行来源身份认证。传送端地址可以由帧提供，不必来自上层软件。
- 由驱动程序或韧体所维护的序号计数器（sequence counter）。



译注 a 在 802.11i 标准中，Michael 有时指 TKIP 的 MIC（信息完整性检查码），有时指 MIC 的密算法。

译注 b TTAK 是 TKIP-mixed transmit address and key 的简称，它是传送端地址(TA)与临时密钥(TK) 经过 TKIP 运算后的中间产物。

图 7-1: TKIP 的帧处理一加密

7.1.2.1 TKIP 的配钥程序与密钥的配制

TKIP 会为所传送的每个帧配制一把独特的密钥。此密钥衍生自初始向量/序号计数器。帧的传送端地址（未必是帧来源）以及临时密钥。配钥（key mixing）可以确保各个帧所使用的密钥彼此间存在显著的差异，以及防范任何假定 WEP 密钥秘密成份维持不变的攻击。将传送端地址纳入配钥的计算，这样不同的工作站就算使用相同的初始向量，也会衍生出不同的 RC4 密钥。

配钥功能的设计，受限于 802.11 控制器的处理能力，如图 7-2 所示。TKIP 将配制密钥的计算过程分为两阶段。第一阶段是以传送端地址、序号的前 32 位元及 128 位元的临时密钥为输入项。输出项则是一个长度为 80 位元的值。虽然有点复杂，不过所有计算都是由一些简单的运算（如 addition、shifts 与 XORs）所组成，以便减轻计算上的负担。只要序号的前 32 位元为常数，第一阶段所计算出来的值也必然为常数，因此只要每 65535 个帧计算一次即可。

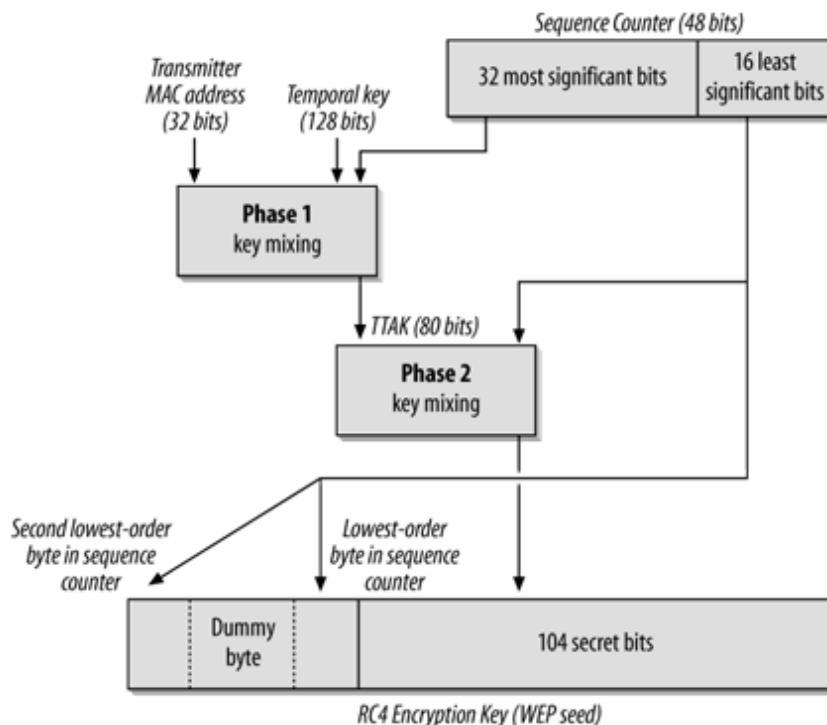


图 7-2: TKIP 配钥

配钥的第二阶段必须针对个别帧。第二阶段以第一阶段所计算的结果、临时密钥与序号的最后 16 位元为输入项。在这些输入项中，有所变动的只有序号。它的变动方式经过完整定义，因此在实现上，可以根据下一组序号值预先计算待传帧所需的数值。

配钥程序第二阶段的输出值是 128 位元的 RC4 密钥，可以作为 WEP 的随机种子。最后 16 位元则是用来产生一个 WEP IV 的高和低位元组。而 WEP IV 中间的位元组是一个值固定的虚设位元组 (dummy byte)，用来避免产生 RC4 弱点密钥。有些 802.11 界面可通过硬件的协助将 RC4 密钥当成输入项以产生密钥串，然后运用所得到的密钥串来加密帧。配钥程序第二阶段的输出项，可以直接传给那些配备此类支持硬件的 802.11 界面。

7.1.2.2 TKIP 的数据传输

帧产生后，接着交付 TKIP 传送，过程如下：

1. 将 802.11 帧置于伫列待传(queued for transmission)。其中包含帧标头以及承载数据 (payload)。和 WEP 一样，TKIP 只保护 802.11 MAC 的承载数据，至于 802.11 帧标头以及下层协议的标头则原封不动。

2. 计算信息完整性检验值 (Message Integrity Check，简称 MIC)。和 WEP 不同的是，TKIP 的 MIC 属于较完善的加密杂凑。它以秘钥 (secret key) 作为验证程序的一部分，而且不止保护 802.11 帧所承载的数据。除了帧数据，MIC 还纳入了来源与目的地址，以及未来 802.11e 标准将会用到的优先性位元 (priority bits)。

3. 赋予各个「帧片段」序号。与 WEP 初始向量不同，TKIP 的序号计数器会随每个帧片段累加。如果帧毋须切割，那么只要编列一个序号即可。如果帧被切割为数个片段，计数器则会依片段数量累加。

4. 每个帧均会以其独有的 WEP 密钥进行加密。通过配钥程序，TKIP 为每个帧产生 WEP 密钥。个别帧所拥有的密钥（per-frame key）将会传给 WEP，以作为 IV 与密钥之用；对个别帧而言，此二者均会随之变动。

5. 帧本身加上步骤二所得到的 Michael 信息完整性检验值，以及步骤四所得到的 RC4 密钥，一并交付 WEP，由 WEP 进行帧分封过程，如第五章所述。值得注意的是，这意味着，受到 TKIP 保护的帧，将会同时包含 WEP 的成份。

TKIP 帧具备类似 WEP 的分封程序。图 7-3 所示为受到 TKIP 保护的帧封装格式。IV/KeyID（初始向量/密钥识别码）保留自 WEP，但具有不同的含义。最前面三个位元组记载了部分的 TKIP 序号，以及目前使用的密钥编号。虽然 TKIP 支持多组密钥，实际上，只有 KeyID 0 会被流传使用。至于 Extended IV（延伸初始向量，简称 EIV）字段，则是用来记载其余的序号。接下来 TKIP 会将 MIC（信息完整性检查码）附加于所承载的数据之后。而 WEP 会加入本身的 ICV（完整性检验值），尽量维持 WEP 格式不受变动。

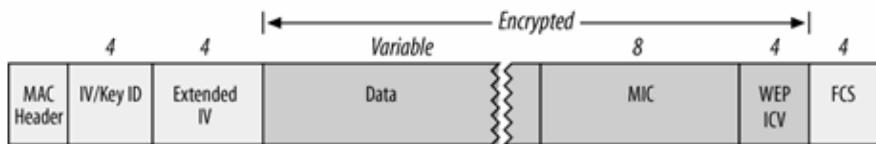


图 7-3: TKIP 封装格式

7.1.2.3 TKIP 的接收

接收到帧，TKIP 就会反转整个加密与传送程序。作为 WEP 的扩充版本，设计时，TKIP 在加密过程中新增了许多查核点（checkpoints），值得详细加以说明。由图 7-4 的方块图可知，在传递给较上层协议之前，有哪些情况会丢弃帧。

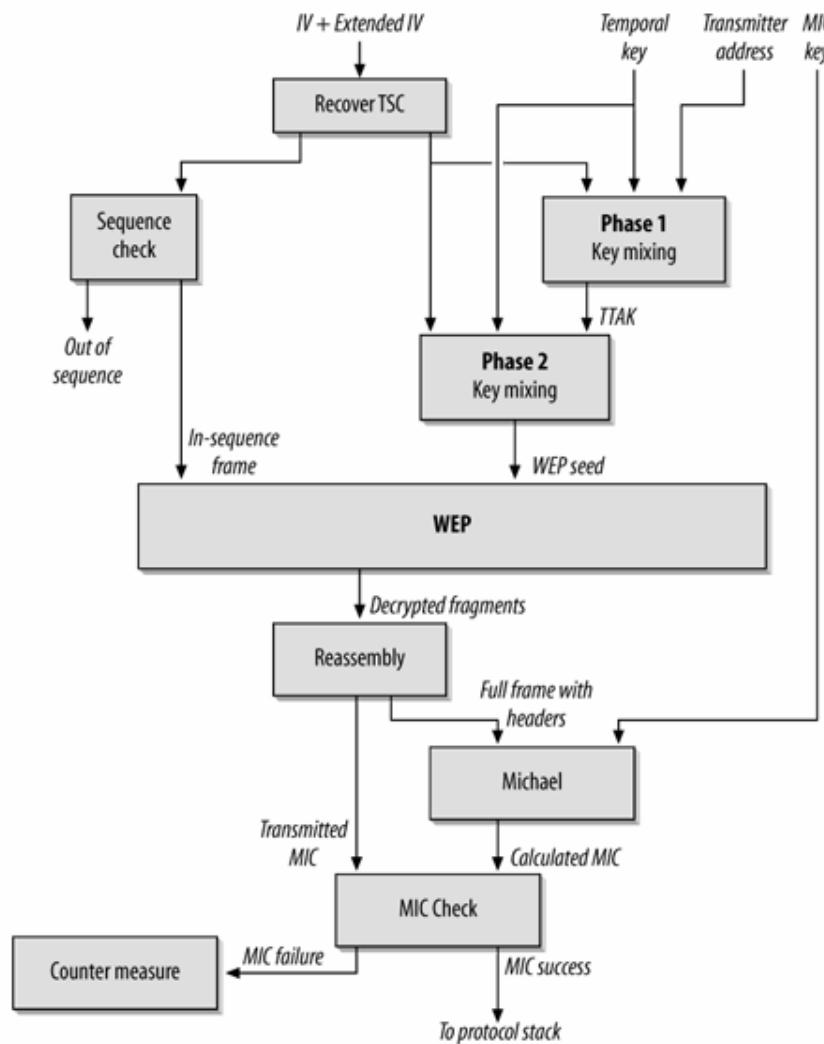


图 7-4: TKIP 的接收程序

1. 一旦无线界面接收到帧，如果通过帧检查程序确认不曾损毁，就会交付 TKIP 做进一步的验证。
2. TKIP 采取的第一个步骤是检查序号，以防范重演攻击。TKIP 的重演攻击防护机制，要求帧的接收必须依循相当严格的次序。如果帧序号小于或等于最近已接收到的有效帧，就会因为可能遭到重演攻击而被扬弃。不像其他技术容许最近到达的帧可以不必完全依照顺序，TKIP 的限制比较严格。不过对这样一种链路层技术而言，坚持依序接收并非无的放矢，因为在这种情况下，未能依序传送的机率应该是微乎其微。
3. 还原用来加密封包的 WEP 随机种子。借由传送端地址、临时密钥以及序号、接收端即可解锁 (unmix the key) 以还原 WEP 随机种子。
4. WEP 随机种子到手后，就可以除去帧外围所包覆的 WEP 层，然后还原内容。在还原内容的过程中，WEP ICV 必须接受检验。虽然并不牢靠，但还是可以用来防范一些无谓的攻击。
5. 如果涉及到帧切割，在重组完整数据之前，必须等到所有片段接收完成。不过帧切割在 802.11 中并不常用。

6. 帧重组之后，将会依帧内容计算其 Michael 值。如果所计算出来的值与封包所记载的 MIC 值相符，则会将帧传递给较上层协议，并且将序号设成帧当中所记载的序号。如果无法通过 MIC 检验，则会启动反制措施。

保留 WEP 封装的理由之一，是为了尽量回溯相容于现有硬件。同时，这种做法也可以避免由于 MIC 检验失败所触发的无谓动作。因电波链路杂讯而损毁的帧，通常无法通过 802.11 帧检验或者 WEP 完整性检验，因此在启动 MIC 失败反制措施之前就会被丢弃。

7.1.3 Michael 完整性检验

WEP 的最大弱点之一在于完整性检验，而完整性检验原本是用来确保帧在行经无线介质时不受篡改。WEP 时采用循环冗余检查码（cyclic redundancy check，简称 CRC），但经过证明，CRC 并不适合作为完整性检验之用。TKIP 的主要目标之一，即是以较稳固的密码学技术，设计出一种适用的信息完整性检验（message integrity check，简称 MIC）。最后出炉的算法称为 Michael，可说是多方妥协后的结果。相较于简单的线性杂凑，Michael 当然比较坚固，由于标准委员会希望尽量减轻实现上的负担，因而使得 Michael 在设计上受到严重的限制。

从架构的观点来看，Michael 被安插在 MAC 服务层中。换言之，Michael 必须处理由上层协议所传递下来的帧。Michael 并不保护个别的 802.11 帧，而是保护经过重组并交给 802.11 传送的数据单元。^{【注】}将 Michael 实现于 MAC 层之上，而非将之整合到 MAC 层的部分理由是，如此一来产品可以较有弹性，厂商可以选择以「特殊的硬件或是设备上所执行的驱动程序」来实现 Michael。旧有的芯片组与 802.11 界面并未内建可以支持 Michael 的特殊硬件，因为当时 Michael 根本尚未问世。这些产品可以通过驱动程序或者软件升级的方式来支持 Michael。新款的设备设计上通常已经将未来的标准考虑在内，如有必要，可以直接将 Michael 内建到芯片组，不需要通过驱动程序的支持。

开发 Michael 的动机，起因于先前提过的一些攻击。其中最值得注意的，即是位元篡改与标头篡改攻击。前者是利用 CRC 在密码学上的弱点。身为一个线性杂凑算法，只要更动 CRC 输入的任何位元，其输出也会有所改变，这早已是众所皆知。攻击者可以更动帧当中几个位元，同时变更 WEP 完整性检验值，以抵销因而所造成的不一致。在标头篡改攻击中，恶意的攻击者可能会伪造来源或传送端地址，或者更改目的地址，试图操纵帧的流向。

请别误会，Michael 并不算是特别安全的加密协议。它的设计，主要是为了那些设备不少的用户，在升级既有网络安全性的过渡时期，可以有点喘息的空间。换言之，它只是未来长期解决方案问世之前的短期措施。

7.1.3.1 Michael 的数据处理

Michael 会对上层传给 MAC 的帧进行加工处理。当上层帧置于位列符传，首要步骤即是计算信息完整性检验（MIC）值。Michael 所处理的输入项，如图 7-5（a）所示。除了目的地址（Destination address，简称 DA）与来源地址（Source address，简称 SA），Michael 会在加密数据之前，加入四个内容为零的位元组。其中，后三个位元组保留未用（Reserved），第一个位元组则是留给未来标准所使用的 Priority（优先性）字段。

【注】实际上，MAC 服务层与 MAC 协议层之间的区别并非必要。虽然 802.11 允许大小超过 2000 个位元组的帧，不过大多数的商业实现品均会参限制帧的大小，以便与 Ethernet 相容，避免切割上层帧。

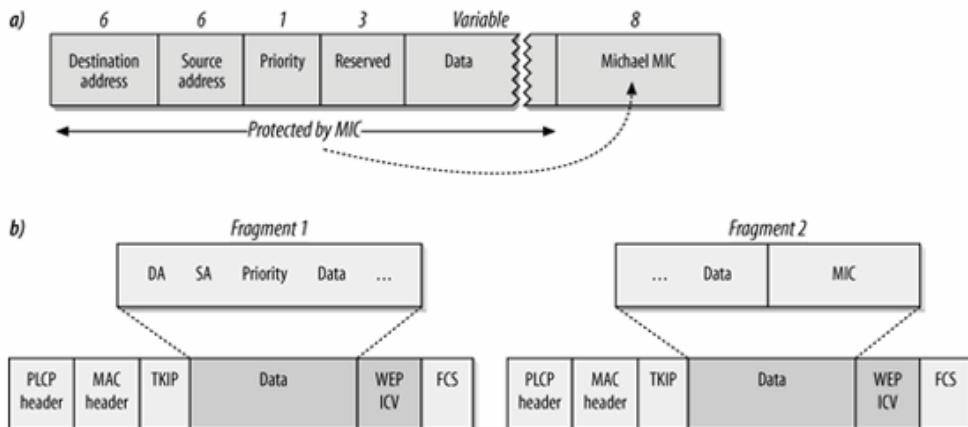


图 7-5: Michael 输入项

Michael 是以 32 位元的数据区块进行处理。如果数据并非 32 位元区块的倍数，就会补零。补零只是为了计算 MIC，实际上并不会被传送出去。Michael 是针对连续的 32 位元数据区块所计算出来的 MIC 值。

计算完成后，即将 MIC 附于数据帧之后，一并交付 802.11 传送。如有必要，就会进行切割。在切割过程中，MIC 值可能会散置于几个片段当中，这是可以接受的。图 7-5 中，来自上层的数据加上 MIC 之后经过切割，散置于不同的帧片段。这是完全可以接受的状况，因为在验证 MIC 之前，这两个帧片段会经过重组。图 7-5 (b) 说明了整个处理程序。来自图 7-5 (a) 的输入项经过切割后分置于两个帧，然后交付传送。每一层均有自己的 MAC 与 PCLP 标头，再由 TKIP 中的 WEP 层加以处理。

7.1.3.2 Michael 反制措施

Michael 防范攻击的能力不强，不过要能支持市面上这么多老旧的硬件，看来它已经算得上是梦幻选择了。Michael 无法抵抗顽强的主动式攻击，因此它纳入了一些反制措施 (countermeasure) 以为防御。

反制的动作是在 MIC 检验时进行的。如果行经至此，帧必然已经通过重放攻击防护以及 WEP 完整性检验值的验证。要能假造可以通过「重放攻击防护与 WEP 完整性检验」的帧并不容易，尤其是后者是根据个别帧的配钥值。

攻击者若能通过重放攻击防护与 WEP 完整性检验，就可以针对 Michael 完整性检验发动暴力攻击 (brute-force attack)。为了防止 Michael 被暴力攻陷，Michael 的反制措施就会停止通讯，从而限制特定密钥遭受主动攻击的次数。如果攻击持续进行，反制措施就会更新密钥，同时停止通讯。

如果工作站检测到 MIC 错误，就会执行下列程序：

1. 标记并登录该 MIC 错误。在验证 MIC 之前，此帧必须通过重放攻击防护以及 WEP 完整性检验。帧如果已递交 Michael 验证，事情就没那么单纯。因此，只要 MIC 验证失败，就可能发生安全相关问题，系统管理员必须加以探究。
2. 如果在 60 秒通讯之内发生两次以上 MIC 错误，反制措施会立即停止所有的 TKIP 通讯 60 秒。暂停通讯的做法，可以让攻击者无法立即再次发动持续性的攻击。

3. 更新密钥。工作站删除自己所持有的主钥副本，然后向认证者要求配发新的密钥，认证者负责产生与传递新的密钥。

虽然 802.11i 将 Michael 反制时间设为 60 秒，不过有些厂商允许将之设置为其他值。

何谓 WPA?

防护访问 (Wi-Fi Protected Access, 简称 WPA) 是由 Wi-Fi 联盟所推行的行销标准。Wi-Fi 联盟将打造标准的细节留给其他机构 (如 IEEE) 去伤神。不过一个商业组织, Wi-Fi 的作为则是确保外界对该产业维持正面的观感。

当 WEP 的基础首度瓦解之际，IEEE 便成立了一个工作小组，开发经改良的安全标准。不过，打造安全的加密协议并不简单，也因此 802.11i 几度谁延问世的时程。802.11i 规范了两种新的安全协议：TKIP 与 CCMP。TKIP 在设计上主要是为了能够和既有的硬件兼容，而 CCMP 本质上则是崭新的设计。因此，在 CCMP 就绪之前，TKIP 就已经完成了。

为了消弥市场对于安全性的疑虑，Wi-Fi 联盟加快脚步致力于 TKIP 的部署，提出名为 WPA 的过渡性行销标准。WPA 第一版以 802.11i 第三版草案 (2003 年中) 为准，WPA 第二版则是依循 2004 年中最后敲定的 802.11i 标准。

WPA 包含了 802.1X 身份认证与加密，分为两种：WPA Personal (相当于 802.11i 的 pre-shared key 身份认证) 以及 WPA Enterprise (使用认证密钥模式，从 TLS entropy 产生密钥)。

7.2 「计数器模式」搭配「区块密码锁链—信息真实性检查码」协议 (CCMP)

TKIP 比 WEP 优秀，不过能够确定的也是如此。既然 WEP 以串流密码锁 (stream cipher) 为基础，后续采用类似机制的做法，就无法摆脱众人对其安全性的怀疑。为了消弥 802.11 用户的疑虑，IEEE 工作小组着手开发一种以先进加密标准 (Advanced Encryption Standard, 简称 AES) 的区块密码锁 (block cipher) 为基础的安全协议。AES 的这种密码锁相当有弹性，适用于各种长度的密钥与数据区块。为了避免困惑使用者，802.11i 规定 AES 使用 128 位元密钥以及 128 位元数据区块。

802.11i 应该使用何种长度的密钥，向来就存在某些疑虑。AES 可以使用各种长度的密钥。美国国家安全部批准 AES 可以对「机密」(secret) 数据使用 128 位元或更长的密钥，至于更敏感的「最高机密」(top secret) 数据，则必须使用 192 或 256 位元的密钥。^{【注 1】} 有人据此论断 128 位元的密钥无法提供适当的安全性。姑且不论这些密钥长度的争论依据为何，128 位元的 AES 远比其他长度的 RC4 更适合用在 802.11 帧的加密。

这个以 AES 为基础的链路层安全协议称为 Counter Mode with CBC-MAC Protocol (「计数器模式」搭配「区块密码锁链—信息真实性检查码」协议，简称 CCMP)。^{【注 2】} 这个名称源自底层所使用的区块密码锁，属于 RFC 3610 所规范的 Counter Mode with CBC-MAC (简称 CCM) 模式。CCM 是一种「组合式」(combined) 过程模式，除了以相同的密钥作为加密的方式，也同时以之产生出密码学上认定为安全的完整性检验值。

2003 年 9 月，美国国家标准与技术研究院（National Institute of Standards and Technology，简称 NIST）开始了一项有关 CCM 的研究。2004 年 5 月，NIST 核准了 CCM，这使得 802.11i 成为安全无线局域网络在严格应用上的基础。

7.2.1 CCMP 的数据处理

和其他链路层加密法一样，CCMP 是以同样的程序支持加密与完整性保护，如图 7-6 所示。

【注 1】详见《National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information》（Committee on National Security Systems(CNSS) Policy No. 15, Fact Sheet No.1 网址为 http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf）。

【注 2】802.11i 标准几经迟延的原因之一，是因为 AES 算法原本是基于另一种过程模式，称为 AES-OCB。智慧财产权的疑虑，使得最后的规格采用 CCMP 而排除 AES-OCB。

CCMP 以下列项目作为输入项：

- 帧
- 临时密钥（temporal key），用来加密与确认帧真实性。这把密钥可同时用来为帧加密与确认帧真实性。
- 密钥识别码（key identifier）。虽然支持多组密钥，不过每个帧只会使用一把密钥。
- 边封包号码（packet number），用来辨识所传送的帧。每传一个帧，封包号码就会累加，不过对于重传帧，则维持不变。亦即，重传不会导致封包号码累加。

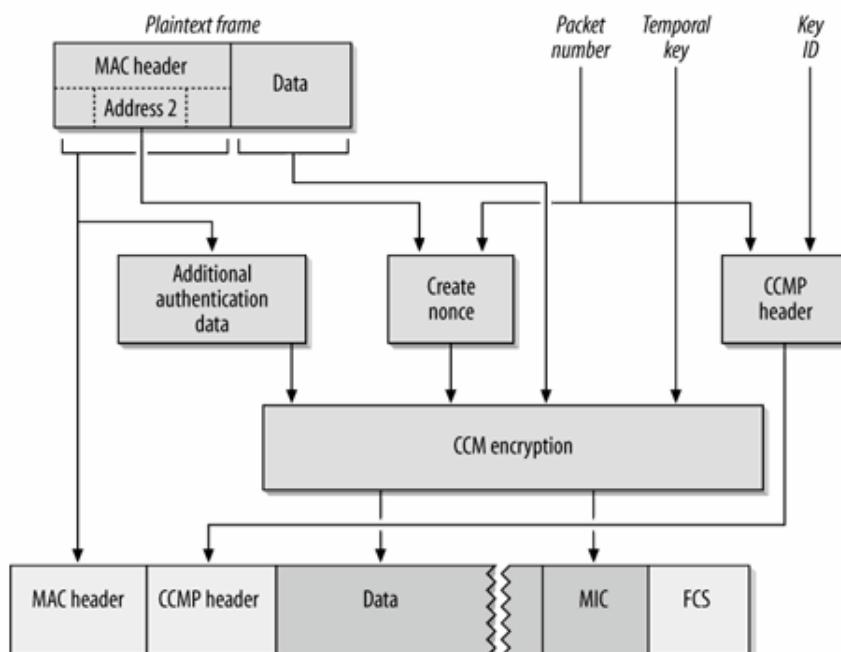


图 7-6：CCMP 帧处理一加密

7.2.1.1 CCMP 的数据传输

当帧产生且交付 TKIP 待传，就会进行下列程序：

1. 将 802.11 帧置于队列待传（queued for transmission）。其中包含帧标头（frame header）以及承载数据（payload）。和 WEP 一样，TKIP 只保护 802.11 MAC 的承载数据，至于 802.11 帧标头以及下层协议的标头则原封不动。
2. 赋予一个 48 位元的封包号码（Packet Number，简称 PN）。和 TKIP 序号一样，同一把临时密钥不会重复使用 PN。每次传送后 PN 就会累加，它同时也用来检测重演攻击。
3. 建立额外认证数据（Additional Authentication Data，简称 AAD）。其中包含帧标头的一些字段，这些字段必须通过真实性的检验，但又不能经过加密，否则 802.11 协议便无法进行过程。接收端同样会使用 AAD 字段，以确认这些字段在传输过程中未受更改。AAD 字段会保护 802.11 协议版本、帧类型、传输系统位元，以及片段与次序位元。它同时会保护来自 MAC 标头的地址字段，同时会将序号（不是片段编号）设为零，以保护顺序控制字段。它以两个（可有可无的）选项字段作为结尾：来自 MAC 标头的第四个地址字段（如果使用无线传输系统的话），以及服务品质（QoS）标头信息。
4. 其次，建立 CCMP nonce。[译注：在密码学中，nonce 系指用过即丢、抛弃式的随机值或乱数。]所谓 nonce，是指少数的数据位元，用以确保加密程序确实实现用于某些独特的数据。nonce 不应该于相同密钥中重复使用。在 CCMP 中，nonce 是由封包号码以及传送端地址组合而成，如此一来，不同的工作站也可以使用相同的封包号码。nonce 同时包含 QoS 会用到的优先性数据。
5. 其次，建立 CCMP 标头。它会将构成 PN（封包号码）的六个位元组拆开，然后将 Key ID（密钥识别码）置于其中。和 WEP 一样，CCMP 当中也包含四个密钥槽。Extended IV（延伸初始向量）位元在 CCMP 中永远设为 1，因为要能容纳 PN 这么大的字段，必定需要用到八个位元组的标头。COMP 标头如图 7-7 所示。
6. 至此 CCM 加密引擎所需要的输入项均已备齐它以 128 位元的临时密钥、步骤四所产生的 nonce、步骤三所产生的额外认证数据（AAD）以及帧本体作为输入项。所有这些数据是以长度为八个位元组的 MIC（信息完整性检查码）来确保其真实性，帧本体与 MIC 也经过加密。整个加密程序如图 7-6 所示。
7. 以原始的 MAC 标头、CCMP 标头与步骤六所产生的加密数据来组成待传的加密帧。帧产生之后，就会交付无线界面传送，如图 7-7 所示。

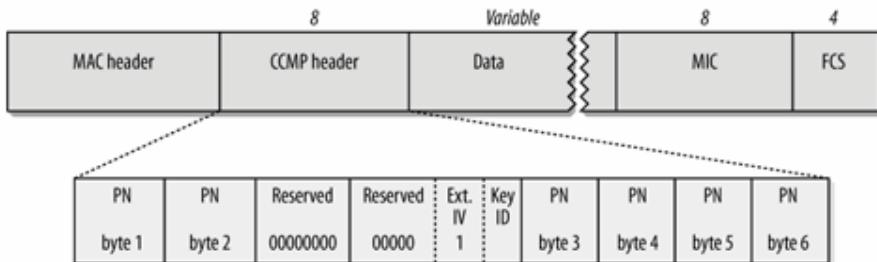


图 7-7：CCMP 的封包格式

受到 CCMP 保护的帧，其封装过程相当直接，如图 7-7 所示。在 MAC 标头之后，CCMP 标头记录了 PN（封包号码）与 Key ID（密钥识别码）。上层协议的帧及其 MIC（信息完整性检查码）加密后置于 FCS 临（帧检查码）之前。

7.2.1.2 CCMP 的接收

当 CCMP 接收到一个帧，就会反转整个加密与传送程序。由于没有相容性的包袱，不必用到 WEP 引擎，CCMP 的解密程序就是图 7-6 的直接倒转：

1. 一旦无线界面接收到帧，如果通过帧检验程序(frame check sequence) 确定未曾受损，就会交付 CCMP 进行验证。
2. 从所接收到的帧还原出 AAD (额外认证数据)。其中只包含帧标头，而且并未经过加密。
3. 从帧还原出 CCMP nonce。其中包含封包编号、传送端地址以及 QOS 字段的内容，这三者均可自未加密的帧标头中取得。
4. 接收端解读密文。此时需要临时密钥、步骤 3 所还原的 nonce、步骤 2 所得到的认证数据，当然还有加密过的帧本体。此一程序完成后，接收端就会得到一份经解密之帧的副本，以及经解密的完整性检查码。
5. 完整性检验是针对明文数据与额外认证数据进行计算。如果计算出的完整性检验值与步骤 4 所得到的完整性检验值相符，就继续进行。否则就终止程序。
6. 从 MAC 标头与步骤 4 所还原的数据组成明文帧。要能通过重放攻击检测检验，其封包号码必须大于或等于最近接收到之通过完整性检验程序的封包号码。

7.3 固安网络 (RSN) 的运作方式

除了 TKIP 与 CCMP，802.11i 还定义了一组程序，称为固安网络 (Robust Security Network，简称 RSN)。这组程序主要在定义密钥的产生与传递方式。

7.3.1 802.11i 密钥阶层体系

链路层加密协议使用了两种密钥。成对密钥 (pairwise keys) 用来保护工作站与 AP 之间往来的数据。群组密钥 (group keys) 用来保护 AP 至所连接工作站之间的广播或组播数据。成对密钥系产生自前一章所讨论的身份认证信息；群组密钥则是由基站动态产生然后传递给各工作站的。

7.3.1.1 成对密钥阶层体系

TKIP 与 CCMP 均使用单一主钥来产生帧保护过程所需要的其他密钥。利用衍生密钥，工作站得以更新加密密钥，毋须重新执行整个认证程序。主钥本身扮演着秘密根源 (root secret) 的角色，必须小心保护，因为所有配钥素材(keying materia)均衍生于此。密钥分级(key hierarchy)的部分目的，是为了衍生「用来保护临时密钥之递送」的密钥。

配钥是从主钥开始。在成对密钥体系中，主钥称为成对主钥 (pairwise master key，简称 PMK)，长度为 256 个位元，如图 7-8 所示。PMK 必然有其来源。在 WPA-PSK 中，便是使用成对主钥。在使用认证服务器的情况下，主钥是计算产生自 RADIUS 服务器中，然后以 Microsoft Point-to-Point Encryption (简称 MPPE) 这个厂商特有的 RADIUS 属性，送给基站。

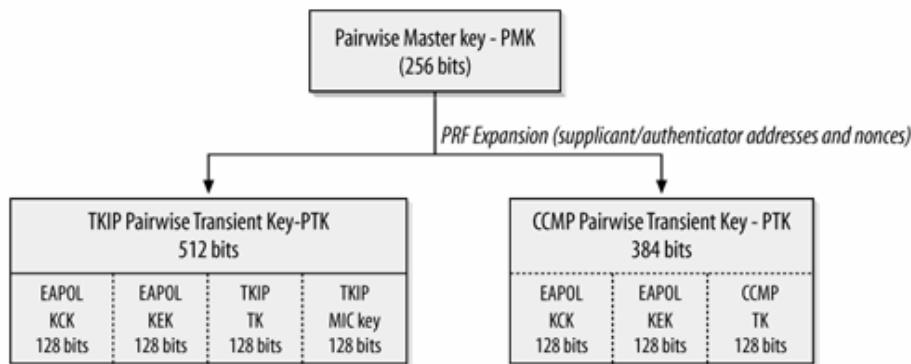


图 7-8：成对密钥阶层体系

为了得到本章之前所提到的临时密钥，必须使用预先定义好的准随机函式 (pseudorandom function)^[注1]来展开 PMK。为了使数据更为随机，此一展开过程是根据预设主钥 (pre-master key)、申请者与认证者 (supplicant and authenticator) 的 MAC 地址以及两个作为四道密钥交换磋商 (four-way key exchange handshake) 的随机 nonce 值。

TKIP 与 CCMP 均会使用准随机函式将 256 位元的 PMK 展开为成对临时密钥 (pairwise transient key，简称 PTK)。在 TKIP 与 CCMP 体系中，临时密钥的两组 128 位元区块，在传递过程中被用来保护临时密钥。

这两种密钥体系均始于两把 EAPOLEAPOL 密钥，通过前一章所提到的 EAPOLEAPOL-Key 信息，保护配钥素材的传输安全。其中使用了两把 128 位元的密钥。第一把是 EAPOLEAPOL 密钥确认密钥 (EAPOLEAPOL Key Confirmation Key，简称 KCK)，用来计算配钥信息 (keying message) 的信息完整性检验值。第二把 EAPOLEAPOL 密钥加密密钥 (EAPOLEAPOL Key Encryption Key，简称 KEK)，用来加密配钥信息。两者在四道磋商一节均会加以讨论。

【注】许多加密协议会利用准随机函式，将随机种子展开为较多的随机数据。TLS 或许是最广为人知的例子。

TKIP 的临时密钥总长度为 512 个位元，额外的 256 个位元，一半作为 TKIP 数据处理时所使用的 128 位元临时密钥，一半用于 Michael 完整性检验。TKIP 之所以需要两把额外的密钥，是因为它使用了传统的加密与认证机制，而会严格区分加密与认证。CCMP 的临时密钥只有 384 个位元，因为它只使用一把 128 位元密钥来进行认证与加密。

7.3.1.2 群组密钥阶层体系

链路层安全协议为广播与组播使用了另一组不同的密钥。已连接的各工作站均拥有不同的预设主钥 (pre-master key)，因此无法从认证过程中推衍出组播所需要的密钥。事实上，认证者拥有群组主钥 (group master key，简称 GMK)，以作为临时密钥的基础。通过准随机函式，群组主钥会被展开成群组密钥体系，如图 7-9 所示。在此并未产生密钥加密 (key encryption) 或密钥确认 (key confirmation) 密钥，因为密钥交换 (key exchange) 系以「成对 EAPOLEAPOL 密钥」 (pairwise EAPOLEAPOL keys) 来传递密钥。

PRFExpansion (authenticator address and nonce)

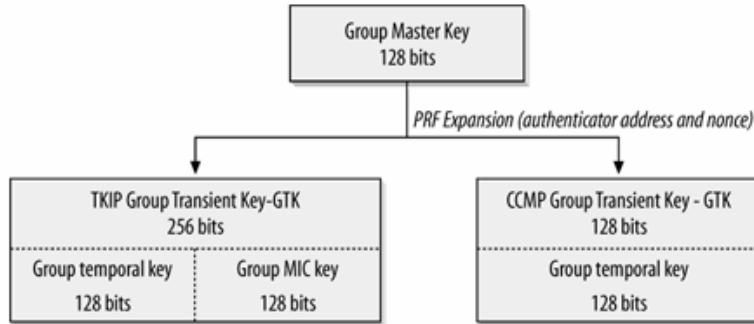


图 7-9: 群组密钥阶层体系

当工作站离开网络，不论是使用完毕或被踢出网络，网络系统即可更新群组密钥。在 TKIP 中，反制措施也会导致系统重新产生群组密钥。

7.3.2 802.11i 密钥的产生与传递

802.11i 规范了一种衍生密钥的机制，而不仅是采用主键并以之为加密协议的输入项。为了防范重放攻击，密钥的交换使用了随机乱数，并且需要经过磋商。成对与群组密钥系分别通过各自的磋商加以更新，如图 7-10 所示。

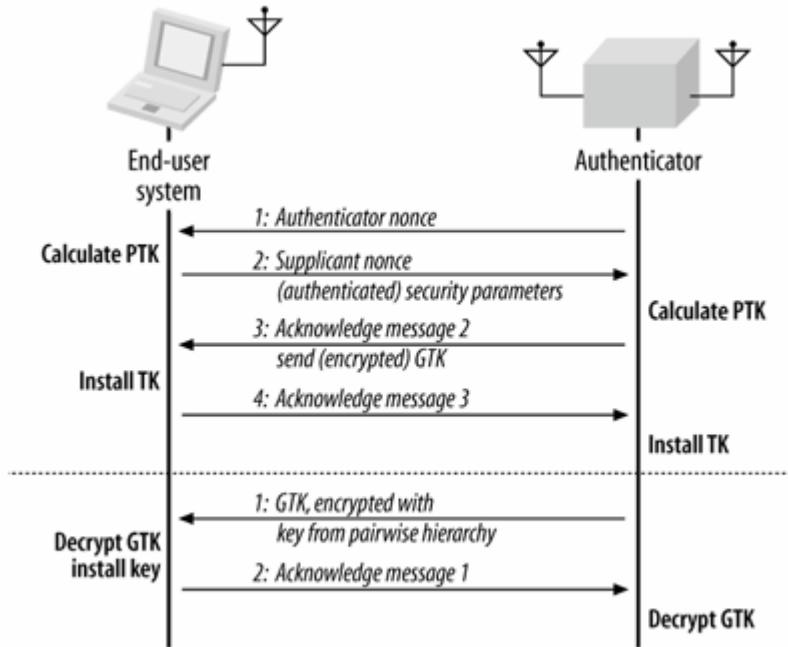


图 7-10: 密钥交换磋商

7.3.2.1 更新成对密钥：四道磋商

成对(pairwise)或单点传播(unicast)密钥，系通过所谓的四道磋商(four-way handshake)加以传递，如图 7-10 所示。申请者(suppliant)与认证者(authenticator)均持有一把共享的成对主钥。四道磋商交换用以产生临时密钥的参数，以及确认双方均已准备就绪，可以开始进行加密传输。依序传送的信息是由下一个信息来代表回应。

1. 认证者将 nonce 传给申请者；nonce 是防范重放攻击的随机值。信息本身并未经过认证，但并没有被篡改的危险。如果信息遭人更改，磋商就会失败并重新执行。

至此，申请者就可以将成对主钥展开成完整的成对密钥阶层体系。展开的过程中，需要用到申请者与认证者的 MAC 地址、成对主钥以及两个 nonces。

2. 申请者所送出的信息中包含申请者的 nonce 以及初次与网络连接时所取得的安全参数副本。整个信息系经过「以 EAPOL 密钥确认密钥计算而来的完整性检验值」的验证。

认证者接收到信息，取出申请者的 nonce，依此衍生出完整的密钥阶层体系。此密钥体系中，包含用来「签证」（sign）信息的密钥。如果认证者无法验证此信息。整个磋商即告失败。

3. 此时磋商双方的密钥均已就绪，但仍需要确认。认证者会将一个信息传给申请者；此信息代表将被加入之成对密钥的序号。它同时包含了目前的群组临时密钥（group transient key，简称 GTK），以便后续能够更新群组密钥。GTK 经过「EAPOL 密钥加密」密钥的加密，整个信息系经过「密钥确认」密钥的认证。

4. 申请者最后会送出确认信息给认证者，告诉认证者已经接收到配钥信息，可以开始使用这些密钥。此信息系经过「密钥确认」密钥的认证。

7.3.2.2 更新群组密钥：群组密钥磋商

群组密钥磋商（group key handshake）显然较四道磋商简单，部分是因为它利用了四道磋商所得出的部分结果。由于群组临时密钥系经过成对密钥体系中的「密钥加密」密钥的加密，因此进行群组密钥磋商之前，四道磋商必须已经成功完成。它包含了两个步骤：

1. 认证者送出群组临时密钥（GTK），并以成对密钥体系中的「密钥加密」密钥进行加密。此信息亦经过「密钥确认」密钥计算出来的检验值的认证。

2. 申请者送出回应信息，告诉认证者开始使用新的群组密钥。此信息也是使用密钥确认密钥进行认证的。

虽然群组密钥磋商所更新的是许多工作站所共用的密钥，但是使用「密钥加密」密钥来保护数据，意味着此一磋商程序其实是成对的。当群组密钥更新后，每部工作站都必须再进行一次群组密钥交换。

虽然群组密钥更新一般是由认证者所主导，但是工作站也可以主动送出确认信息，要求更新群组密钥。

7.3.3 混合加密类型

为了支持不同加密协议的替换，以及纳入只支持 WEP 加密功能的老旧设备，802.11i 定义了一种可信赖的加密协议体系。使用 40 位元密钥的 WEP 是最弱的加密协议，之后分别是使用 104 位元密钥的 WEP、TKIP 与 CCMP。

作为网络连接的初始程序，各个工作站可以协商使用何种加密协议进行单点传播与组播传输。惟一的限制是，群组密钥必须使用相同强度或较弱的加密协议。基站在群组密钥上采用了「最小公分母」（lowest common denominator）的做法。在网络上，如果能力最低的工作站只具备动态 WEP 的能力，就会以动态 WEP 作为群组密钥。不过，其他工作站可以使用较强的单点传播保护机制。有些基站支持连接政策控制，用来设置可接受的最低加密强度，以及防止工作站以强度低于网管人员所要求的协议与网络连接。

802.11i 标准允许混用几乎所有的加密方式，但使用 CCMP 传输群组帧（group frame）的工作站只能以 CCMP 进行单点传播帧（unicast frame）传输，这是惟一的例外。不过，有些驱动程序并不支持所有可行模式。最值得注意的是，驱动程序通常不支持下述的混搭方式，亦即单点传播数据（unicast data）使用 CCMP，群组密钥 group key 使用较旧的 RC4 帧加密。

7.3.4 密钥快取

成对主钥（PMK）算是 802.11i 的安全防护基础。如果成对主钥是通过 802.1X 交换程序产生的，代价其实不斐。大部分的 EAP 方式都需要用到好几个信息，每个步骤也都需要大量的计算。802.1X 认证程序需时好几秒，此时使用者并无法收发数据。介于两部基站边界的工作站特别容易受到影响，如果它的无线界面因为两部基站的信号强度相当而在两边来回切换的话。

PMK 快取的动机，在于减轻认证负担，如图 7-11 所示。与基站进行连接时，工作站会先参考既有连接的成对主钥安全连接识别码（PMKSA），而非每次都进行完整的 802.1X 交换程序。如果基站中存在连接纪录，就会接受连接且迳行至四道磋商。在四道磋商过程中，申请者与认证者将会证明各自所快取的 PMK。

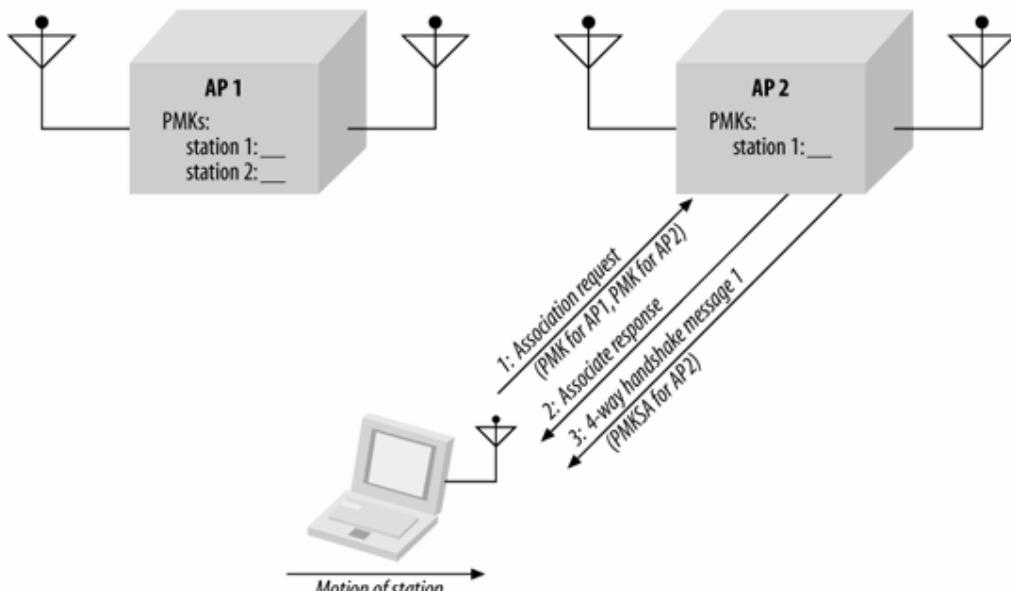


图 7-11：PMK 快取

没有快取主钥的工作站必须进行完整的 802.1X 认证，这样才能产生主钥。事先认证（pre authentication）的动机之一，即是在换手（handoff）发生之前，在基站中产生主钥备用。事先认证将于下一章讨论。

第8 章 过程管理

虽然具备不受有线网络束缚的优势，无线网络也不是没有任何问题。无线介质并不稳定，何况既然没有实体的界限，未经授权的使用者便可趁虚而入，而且如果所使用的设备以电池供电，则电源管理就十分重要。802.11 协议的管理功能，就是设计来降低这些问题的效应。基本上，管理过程就是无线网络设备在幕后进行的所有任务。借此，无线网络连接感觉上就跟其他类型的网络连接没什么两样。

802.11 管理过程是由用户端设备与网基础结构彼此分工合作。遗憾的是，绝大部分的协议过程均由用户端设备所掌握，但这些设备之间或许差异甚大。有些设备驱动程序允许使用者自订本章所探讨的管理功能。不过应该注意的是，设备驱动程序的功能因产品而异，而且无线网络的市场现况是，有些厂商试图生产功能最丰富的产品，有些则是针对低成本市场，致力生产最简单的产品。要知道可以使用哪些功能，惟一的方法就是了解协议本身具备哪些功能。如此一来，不论面对何种硬件设备，你都可以应付自如。

8.1 管理架构

概念上，802.11 管理架构由三个元件组成：MAC 层管理单元（MAC layer management entity，简称 MLME），物理层管理单元（physical-layer management entity，简称 PLME）以及系统管理单元（system management entity，简称 SME）。不同管理单元之间，以及其与 802.11 相关成份之间的关系，如图 8-1 所示。

802.11 规格中并未正式规范 SME。SME 是使用者和设备驱动程序跟 802.11 网络界面互动和取得状态信息的方式。MAC 与 PHY 协议层皆可访问管理信息库（management information base，简称 MIB）。MIB 包含了许多物件，有些物件可供查询状态信息，有些则可以启动特定的行为。

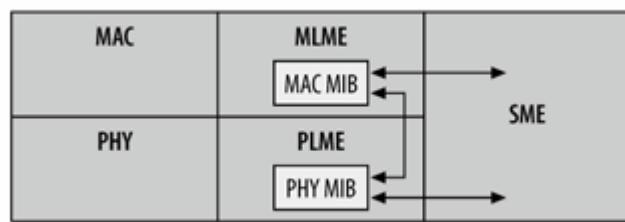


图 8-1：管理单元与 802.11 规格的关系

在这些管理元件之间定义了三个界面。SME 可通过 MLME 和 PLME 服务界面来更改 MAC 与 PHY MIB。此外，MAC 有所改变，相对地 PHY 也要有所变动，所以在 MLME 与 PLME 之间必须存在一层界面，让 MAC 得以变更 PHY。

8.2 扫描

使用任何网络之前，首先必须找出网络何在。使用有线网络，要找出网络所在并不难，只要循着网线或者找到墙上的插座即可。在无线领域中，工作站加入任何相容网络之前，必须先经过一番辨识的工作。于所在区域辨识现有网络的程序称为扫描（scanning）。

扫描过程中会用到几个参数。这些参数可由使用者来指定；有些产品则是在驱动程序中为这些参数提供预设值。

BSSType (independent、infrastructure 或 both)

扫描时，可以指定所要搜寻的网络属于 independent ad hoc、infrastructure 或同时搜寻两者。

BSSID (individual 或 broadcast)

工作站可以针对所要加入的特定网络（individual）进行扫描，或者扫描允许该工作站加入的所有网络（broadcast）。在行进间将 BSSID 设为 broadcast 不失为一项好主意，因为扫描的结果会将该地区所有的 BSS 涵盖在内。

SSID (“network name”)

SSID 系用来指定某个延伸服务组合（extended service set）的位元串。大部分的产品会将 SSID 视为网络名称（network name），因为此位元串通常会被设置为人们易于辨识的字串。工作站若打算找出所有网络，应该将之设置为 broadcast SSID。

ScanType (active 或 passive)

主动（active）扫描会主动传送 Probe Request 帧，以辨识该区有哪些网络存在。被动（passive）扫描则是被动聆听 Beacon 帧，以节省电池的电力。

ChannelList

进行扫描时，若非主动送出 Probe Request 帧，就是在某个频道被动聆听目前有哪些网络存在。802.11 允许工作站指定所要尝试的频道表（ChannelList）。设置频道表的方式因产品而异。物理层不同，频道的构造也有所差异。直接序列(direct-sequence)产品以此为频道表，而跳频(frequency-hopping)产品则以此为跳频样式(hop pattern)。

ProbeDelay

主动扫描探测某个频道期间，为了避免工作站一直等不到 Probe Response 帧，所设置的逾时计时器，以微秒为单位。用来防止某个闲置的频道让整个程序停摆。

MinChannelTime 与 MaxChannelTime

以 TU（时间单位）来指定这两个值，意指扫描每个特定频道时，所使用的最小与最大的时间量。

8.2.1 被动扫描

被动扫描（passive scanning）可以节省电池的电力，因为不需要传送任何信号。在被动扫描中，工作站会在频道表（channel list）所列的各个频道之间不断切换，并静候 Beacon 帧的到来。所收到的任何帧都会被暂存起来，以便取出传送这些帧之 BSS 的相关数据。

在被动扫描的过程中，工作站会在频道间不断切换，并且会记录来自所收到之 Beacon 信息。Beacon 在设计上是为了让工作站得知，加入某个基本服务组合（basic service set，简称 BSS）所需要的参数，以便进行通讯。在图 8-2 中，行动式工作站以被动扫描找出该区所有 BSS；通过聆听来自前三部基站的 Beacon 帧。如果该工作站并未收到来自第四部基站的 Beacon，就会回报目前只发现三个 BSS。

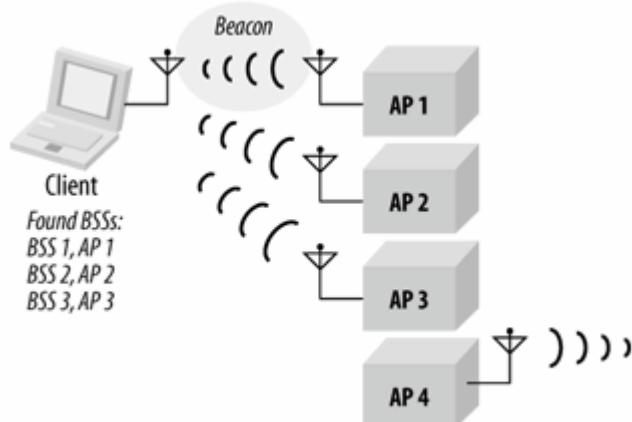


图 8-2：被动扫描

8.2.2 主动扫描

在主动扫描 (active scanning) 中，工作站扮演比较积极的角色。在每个频道上，工作站都会发出 Probe Request 帧，请求某个特定网络予以回应。主动扫描系主动试图寻找网络，而不是听候网络宣告本身的存在。使用主动扫描的工作站将会以如下的程序扫描频道表所列的频道：

1. 跳至某个频道，然后等候来讯显示 (indication of an incoming frame)，或者等到 ProbeDelay 计时器逾时。如果在这个频道收得到帧，就证明该频道有人使用，因此可以加以探测。此计时器用来防止某个闲置频道让整个程序停摆；工作站不会一直听候帧到来。
2. 利用基本的 DCF 访问程序取得介质使用权，然后送出一个 Probe Request 帧。
3. 至少等候一段最短的频道时间 (即 MinChannelTime)。
 - a. 如果介质并不忙碌，表示没有网络存在。因此可以跳至下个频道。
 - b. 如果在 MinChannelTime 这段期间介质非常忙碌，就继续等候一段时间，直到最长的频道时间 (即 MaxChannelTime)，然后处理任何的 Probe Response 帧。

当网络收到搜寻其所属之延伸服务组合的 Probe Request (探查要求)，就会发出 Probe Response (探查回应) 帧。为了在舞会中找到朋友，各位或许会绕著舞池大声叫喊对方的名字。(虽然这并不礼貌，不过如果真想找到朋友，大概没有其他选择。) 如果对方听见了，她就会出声回应，至于其他人根本就不会理你 (希望如此)。Probe Request 框的作用类似，不过在 Probe Request 帧当中可以使用 broadcast SSID，如此一来，该区所有的 802.11 网络都会以 Probe Response 加以回应。(这就好比在一场比赛中大喊「失火了」，可以确定每个人都会加以回应！)

每个 BSS 中，至少必须有一部工作站负责回应 Probe Request。传送一个 Beacon 帧的工作站，也必须负责传送必要的 Probe Response 帧。在 infrastructure (基础型) 网络里，是由基站负责传送 Beacon 帧，因此它也必须负责回应以 Probe Request 在该区搜寻网络的工作站。在 IBSS (独立型基本服务组合) 中，工作站彼此轮流负责传送 Beacon 帧，因此负责传送 Probe Response 的工作站会经常改变。Probe Response 属于单点传播 (unicast) 管理帧，因此必须符合 MAC 的正面回应 (positive acknowledgment) 规范。

单一 Probe Request 导致好几个 Probe Response 的情况十分常见。扫描程序的目的，在于找出工作站可以加入的所有基本服务区域，因此一个 broadcast (广播式) Probe Request 会收到范围内所有基站的回应。各独立型 BSS 之间如果互相重叠，也会予以回应。

图 8-3 所示为 Probe 帧之间的关系，以及扫描时可以设置的各种时间间隔。

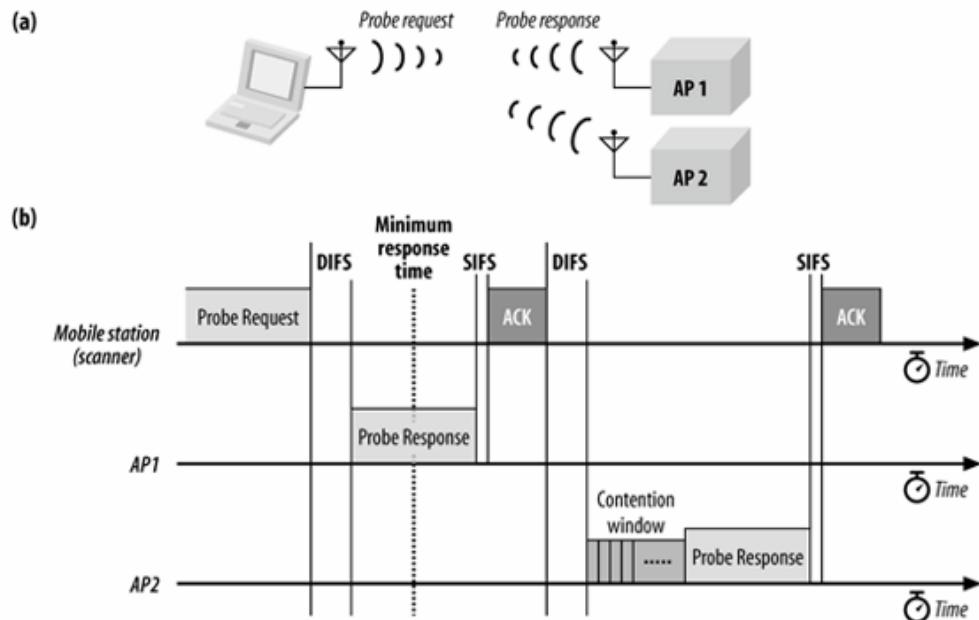


图 8-3：主动扫描程序以及介质访问

在图 8-3(a) 中，某部行动式工作站发出 probe request（探查要求）信息，而有 2 部基站加以回应。在介质（medium）中进行的动作如图 8-3(b) 所示。在取得介质使用权后，进行主动扫描的工作站会送出 Probe Request。接著有 2 部基站适时以 Probe Response（探查回应）加以答复，其中包含它们的网络参数。值得注意的是，第 2 个 Probe Response 受限于分散式协调功能（distributed coordination function）的规则，在传送之前必须等待竞争时期（congestion window）结束。第一个回应在最短回应时间（minimum response time）结束之前即已送出，因此工作站会继续等候至最长回应时间（maximum response time）结束，才会检验所收到的信息。在网络林立的区域，或许必须调整每个频道的最长等候时间（maximum channel time），才有办法处理区域内每个基站所发出的答复信息。

8.2.3 扫描结果

扫描结束后会产生一份扫描报告。这份报告列出了该次扫描所发现的所有 BSS 及其相关参数。进行扫描的工作站可以利用这份完整的参数清单，加入（join）其所发现的任何网络。除了 BSSID、SSID 以及 BSSType，这些参数还包括：^{【注】}

Beacon interval (信标间隔；整数值)

每个 BSS 所传递的 Beacon 帧，均可指定自己的间隔，以 TU 为单位。

DTIM period (DTIM 期间；整数值)

DTIM 帧属于省电（power-saving）机制的一部分。

Timing parameters (计时参数)

有 2 个字段可让不作站的计时器与 BSS 所使用的计时器同步。Timestamp 字段代表扫描工作站所收到的计时值；另一个字段则是让工作站得以符合计时信息，以便加入特定 BSS 的调整值（offset）。

PHY 参数、CF 参数以及 IBSS 参数

这三个网络参数均具备各自的参数组合，相关细节在第四章已经探讨过了。频道信息（channel information）包含在物理层参数（physical-layer parameters）中。

BSSBasicRateSet

基本速率组合（basic rate set）是打算加入某个网络时，工作站必须支持的数据传输率清单。工作站必须能够以基本速率组合中所列的任何速率接收数据。基本速率组合是由管理帧之 Supported Rates 信息元素的必要速率所组成，细节参见第四章。

名称的内涵为何？

（或者，隐藏式 SSID 的安全性谬误）

SSID 是相当重要的扫描参数。工作站进行扫描时会搜寻特定的 SSID，或者列出可用的 SSID 供使用者挑选。作为网络独一无二的辨识名称，SSID 通常带有某些安全性的神秘色彩，虽然实际上它并不拥有这些性质。

802.11 刚问世时，SSID 是通过 Beacon 帧公开进行广播的。只需要一片 802.11 网卡，对准正确的无线电频道就可以收听到。进入 802.11 的石器时代以后，有家厂商开始将 SSID 视为具有安全价值的标记。只要在他们的设备上启用 close network（封闭式网络）选项，就不会将 SSID 置于 Beacon 帧，借此“保护”网络免遭攻击。为了进一步“保护”SSID 不受窥视，这类封闭式网络的基站对于 Probe Request 信息也不会回复广播型 SSID。

—————
【注】实际输出哪些项目，因软件而异。

封闭式网络也阻绝了被动扫描，因为不再能够轻易搜集得到 SSID。不过为了避免封闭式网络完全自绝于工作站，基站必须回应那些指定了正确 SSID 的 Probe Request。管理帧并未加密，而且 SSID 的内容就明白写在 Probe Request 帧里。严格来讲，封闭式网络或许提供了些微的安全性，因为 SSID 只有在工作站搜寻网络时才会曝光，而不是每秒钟出现在 Beacon 帧好几次。

隐藏 SSID 可能导致 802.11 管理上的问题。并非所有 802.11 界面与驱动程序都能够处理隐藏式 SSID。隐藏 SSID 并不符合标准规范，而且可能导致其他问题，更无法提供真正的安全性。为了顾及互通性，不妨让 SSID 出现在 Beacon 帧，如有必要，应该采用真正的安全性解决方案，例如 802.1X。

8.2.4 加入网络

扫描结果汇整之后，工作站即可选择其中一个 BSS 加入。加入网络（joining）是建立连接的前置过程；相当于拿起武器。不过此时还不能访问网络。访问网络之前，必须经过身份认证以及形成连接。

选择加入哪个 BSS 和实现有关，有时甚至需要使用者的介入。属于相同 ESS 的 BSSs 允许采用本身所决定的方式；通常用来决定加入哪个网络的判断标准是功率准位（power level）与信号强度（signal strength）。外人无法判断一部工作站在何时加入某个网络，因为加入程序纯属节点内部的过程；其中牵涉到调整内部参数，以配合所选 BSS 要求的参数。其中最重要的一项任务，就是行动工作站与网络之间计时信息的同步，此一程序在 8.7 节（计时器同步）会有更详尽的探讨。

此外，工作站还得符合 PHY 参数，此参数用以保证，该 BSS 的任何传输过程均会在正确的频道中运作。（计时器同步也可以保证，跳频工作站能够在正确的时间切换频道。）使用 BSSID 可以确保目前是与正确的工作站进行传输，同时忽略其他 BSS 的工作站。^{【注】}扫描结果还包含 Capability 信息，可确认是否使用 WEP，以及任何的高速功能。工作站必须采用所选 BSS 的 Beacon 间隔以及 DTIM 期间，虽然就能否进行通讯而言，这些参数比较不是那么重要。

试图破坏网络安全性的恶意攻击者，可以轻易规避这些规定而截取封包，大多数现有产品，并未正确实现这些过滤规则。

8.3 身份认证

对所有恶意的侵犯而言，任何无线网络介质都是开放的，因为攻击者实际上可以隐身于网络介质之中。只要置身其中，要取得立足之地就十分容易。请各位准备好进入身份认证的阴阳魔界（twilight zone）。802.11 提供了多种形式的“身份认证”，对真正的安全专家而言，有些根本不值一提。

提到身份认证，大多数网管人员认为只有坚固的身份认证（strong authentication）才算真正的身份认证。如果不是以密码学（cryptography）为基础就不能算数。只要搭配正确的 EAP 认证方式，802.1X 身份认证就相当坚固，不过系统必须在连接前先进行低价的 802.11 “身份认证”，才可以交换 802.1X 信息。

8.3.1 802.11 “身份认证”

802.11 要求工作站在传送帧之前必须确认身份。起初，只要工作站打算连接到网络，就必须进行 802.11 “身份认证”。不过应该强调的是，这些并无法提供真正有意义的网络安全。因为不但没有传递或验证任何密码学等级的秘密（cryptographic secret），也并未进行相互认证程序。比较正确的看法，是将 802.11 的低价身份认证，视认工作站连网时的磋商程序起点，以及一种对网络表明身份的方式。

—————
【注】技术上，只有在工作站遵循帧接收的过滤规定时，这种说法才算成立。

目前，802.11 身份认证有点像是单行道。打算加入某个网络的工作站必须通过身份认证，然而网络方面并无义务对工作站证明自己的身份。802.11 的设计者或许认为基站属于网络基础架构的一部分，因此具备某种特权。

8.3.1.1 开放系统身份认证

开放系统身份认证（open-system authentication）是 802.11 要求必备的惟一方式。称之为身份认证有点曲解这个名词的意义。在开放系统身份认证中，基站并未验证移动式工作站的真实身份，只是作作表面功夫。（想像一下，类似的身份认证应用在银行提款机，是什么光景！）网络安全必须建立在现有的网络连接基础之上。开放系统身份认证的过程用到两个帧，如图 8-4 所示。

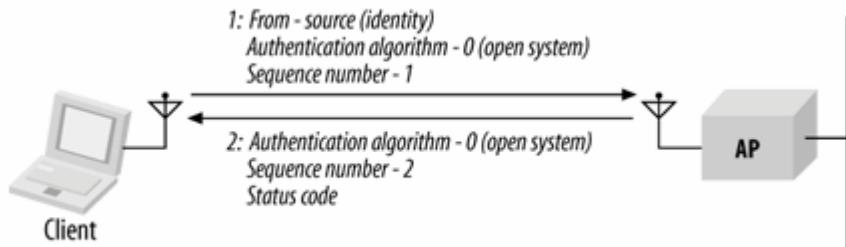


图 8-4：开放系统身份认证的交换程序

由行动式工作站所发出的第一个帧被归类为 authentication（身份认证）的管理信息。802.11 在规格中并未正式将此帧视为身份认证要求（authentication quest）。不过实际上的作用即是如此。在 802.11 中，工作站是以 MAC 地址为身份证明。和 Ethernet 网络一样，网络上的 MAC 地址必须独一无二，因此可作为工作站的身份证明。基站以这些帧的来源地址作为发送者的身份证明，此外，并没有以该帧其他字段作为身份证明之用。

身份认证要求包含两个信息元素。首先，身份认证算法代号（Authentication algorithm Identification）被设置为 0，代表使用开放系统认证方式。其次，身份认证交易顺序编号（Authentication Transaction Sequence number）被设置为 1，代表该帧实际上为交易顺序中第一个帧。

基站接着会处理身份认证要求，然后传回结果。和第一个帧一样，回应帧亦是该类型为 authentication 的管理帧。其中包含三个信息元素：身份认证算法代号 位被设置为 0，代表使用开放系统身份认证，顺序编号为 2，另外还有一个状态码（status Code）用来显示身份认证要求的结果。状态码的各种可能值如表 4-6 所示。

地址过滤（MAC “身份认证”）

802.11 并未强制使用 WEP，一些早期的产品只实现了开放系统身份认证功能。为了提供更安全的身份认证，有些产品会提供所谓「经授权的 MAC 地址列表」。网管人员可以键入一组经过授权的工作站地址，只要是表上有名的工作站就可以跟网络连接。

虽然地址过滤功能聊胜于无，不过还有相当大的改进空间 MAC 地址通常可以通过软件或轫体加以修改，因此打算访问网络的攻击者可以轻易得逞。此外，要将这些可以访问网络的工作站地址列表传给网络上所有设备也是件苦差事。何况，这份名单的内界还有待商榷。例如购买新的网卡、旧的网卡已经报废，离职员工带走网卡等问题。

授权地址的过滤可作为安全方案的一部分，但非解决方案的关键。尽可能使用 802.1X 使用者身份认证，不要依赖 MAC 地址过滤。只要网管人员费心验证使用者身份，就可以达到标准所提供的安全性。地址过滤只是徒增管理上的复杂度，没有实质利益可言。

3.3.1.2 旧式的共享密钥身份认证

共享密钥身份认证（shared-key authentication）必须使用 WEP，因此只能用于实现了 WEP 的产品上，虽然目前已经很难找到不支持 WEP 的产品。正如其名，「共享密钥身份认证」要求在进行身份认证之前，必须传递共享密钥给工作站。共享密钥身份认证的理论基础是，如能成功回

应传给它的挑战信息，就证明工作站拥有共享密钥。「共享密钥身份认证」交换程序，使用到了四个被归类为 authentication（身份认证）的管理帧，如图 8-5 所示。

第一个帧几乎和「开放系统身份认证」交换程序的第一个帧相同。和开放系统帧一样，其中所包含的信息元素，可用以识别所使用的认证算法以及顺序编号；身份认证算法代号被设置为 1，代表使用「共享密钥身份认证」。

共享密钥交换程序的第二个帧扮演把关的角色，而不是盲目地允许网络访问。第二个帧最多包含四个信息元素。通常，这些信息元素包括身份认证算法代号、顺序编号，以及状态码。基站可能以此帧拒绝身份认证要求，从而中止整个交易程序。要进行下一个步骤，状态码必须为 0（代表成功），如图 8-5 所示。如果状态码显示成功，则此帧还会包含第四个信息元素，亦即挑战口令（Challenge Text）。挑战口令的长度为 128 个位元组，由 WEP 密钥串流产生器（keystream generator）利用随机密钥（random key）及初始向量（initialization vector）产生。

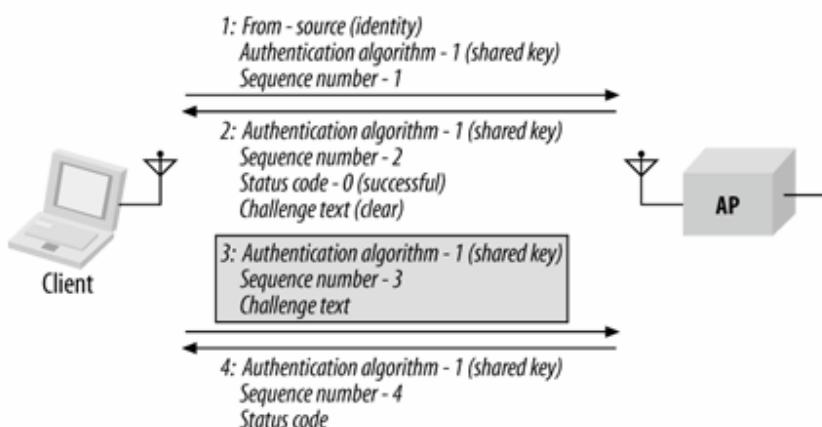


图 8-5：「共享密钥身份认证」交换程序

第三个帧是行动式工作站对挑战所做出的答复。为了证明本身具备访问网络的权限，行动式工作站将会以三项信息元素组成一个管理帧：身份认证算法代号、值为 3 的顺序编号，以及挑战口令。在传送此帧之前，行动式工作站将会以 WEP 进行处理。标头部分会保留不予处理，因为必须利用它来辨识，其是否为身份认证帧，至于信息元素部分则通过 WEP 予以加密。

收到第三个帧后，基站会试图予以解密，然后验证 WEP 的完整性。如果可从该帧中解读出挑战口令，而且通过完整性检查（integrity check）的验证，基站就会以成功的状态代码来回复。若能成功解读挑战口令，证明该行动式工作站已经设置好加入该网络所需的 WEP 密钥，因此应该准予访问网络。如果有任何问题发生，基站便会传回代表失败的状态码。

8.3.1.3 破解共享密钥身份认证

共享密钥身份认证很容易屈服于简单的攻击。共享密钥身份认证程序的核心，就是挑战口令的加密。收到随机的挑战信息后，拥有 WEP 密钥的工作站便可从 WEP 密钥衍生出所需要的密钥串流，然后以之和数据进行「exclusive-OR」运算。不过，关系到挑战口令、密钥串流与挑战回应的「exclusive-OR」属于一种可逆的（reversible）运算。只要知道其中两项，就可以逆向推算出第三者。攻击者可以观察挑战口令与挑战回应，以之推算出密钥串流。虽然攻击者可以使用还原的密钥串流来回应新的挑战信息，并且通过网络的身份认证，如果未能还原出 WEP 密钥，攻击者仍旧无法传送任何数据。

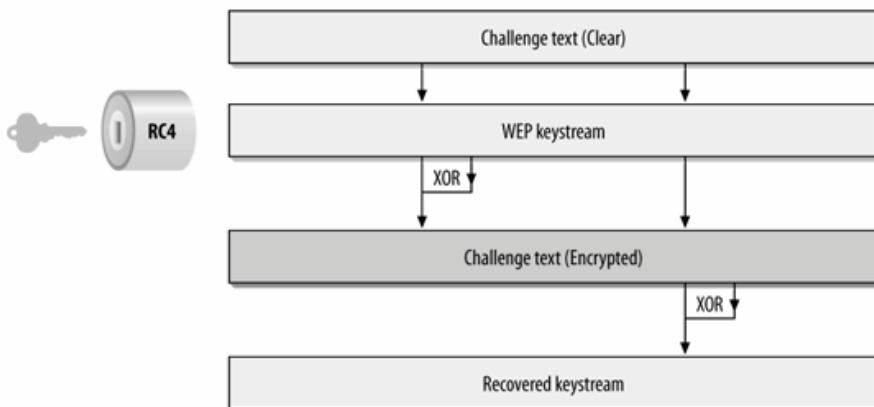


图 8-6：破解共享密钥身份认证

由于攻陷共享密钥身份认证只是举手之劳，因此通常不建议使用密钥身份认证。802.11i 就不允许以共享密钥通过 802.11 身份认证的工作站连接至固安网络（Robust Security Network）

8.4 事先身份认证

事先身份认证（preauthentication）系用来加速连接关系的移转。从工作站决定转移至新基站，到新基站开始传送帧给工作站，身份认证是这段期间内最容易造成延宕的因素。事先身份认证的目的就是缩短这段时间，在需要之前先进行这项费时的过程以建立彼此的关系。由于低价的 802.11 身份认证与 802.1X 身份认证均使用「身份认证」（authentication）这个名词，因此有两种不同类型的事先身份认证。不过，如同网络工程师的习惯用法，「身份认证」通常是指 802.1X 身份认证。

8.4.1 802.11 事先身份认证

在与基站连接之前，工作站必须先经过身份认证，不过 802.11 标准并未要求低价身份认证之后必须立即进行连接过程。在扫描阶段，工作站可以跟几部基站进行 802.11 身份认证，如此一来，当有需要时，就可以立即进行连接过程。这种做法称为事先身份认证（pre authentication）。事先身份认证的好处是，一旦进入基站的涵盖范围，工作站就可以立即与基站重新连接，而不必等候认证交换程序。

图 8-7 左右两边都可以看到，由两部基站所构成的延伸服务组合（ESS）。为了简化起见，此处只会用到一部行动式工作站。假定行动式工作站一开始与图左的 AP1 连接，因为它位于 AP1 的涵盖范围内。当该行动式工作站向右移动时，最后必须跟 AP2 连接，因为它已经离开 AP1 的涵盖范围。

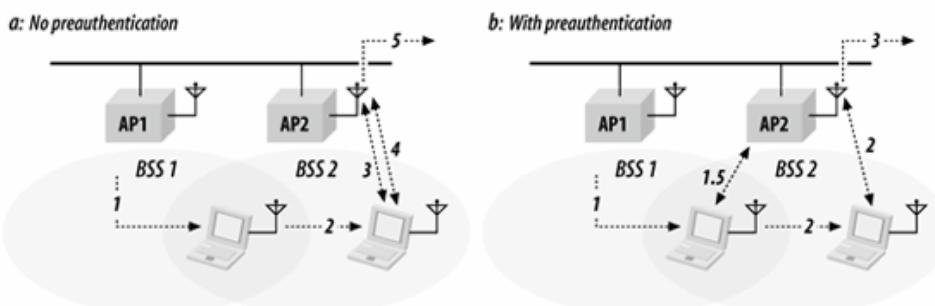


图 8-7：省时的事先身份认证

大多数有关 802.11 的文字说明,都未提到事先身份认证(preeauthentication),如图 8-7(a)所示。当行动式工作站移动至右边,来自 AP1 的信号会逐渐减弱。工作站会持续监测来自 ESS 的 Beacon 帧,最后终于注意到 AP2 的存在。至此,工作站或许会选择与 AP1 解除连接,然后与 AP2 进行身份认证与重新连接。这些步骤在图中已有交待,其中出现的数字为表 8-1 所列的时序值。

表 8-1: 图 8-7 的时序

步 骤	不采用事先身份认证: 8-7 (a)	采用事先身份认证: 8-7 (b)
0	工作站与 AP1 形成连接	工作站与 AP1 形成连接
1	工作站向右移至 BSS1 与 BSS2 的重叠区	工作站向右移至 BSS1 与 BSS2 的重叠区, 并且检测到 AP2 的存在
1.5		工作站与 AP2 进行事先身份认证
2	AP2 的信号比较强, 所以工作站决定与 AP2 形成连接	AP2 的信号比较强, 所以工作站决定与 AP2 形成连接
3	工作站与 AP2 进行身份认证	工作站开始使用网络
4	工作站与 AP2 重新连接	
5	工作站开始使用网络	

图 8-7(b) 显示了采用事先身份认证的工作站会发生什么情况。只要稍微修改软件,让工作站只要检测到 AP2,即可与 AP2 进行身份认证。当工作站离开 AP1 的管辖范围,就已经同时与 AP1 和 AP2 完成了身份认证。当工作站离开 AP1 的涵盖范围时,省时的效用就出现了:它可以立即跟 AP2 重新连接,因为已经事先经过身份认证。事先身份认证可以让漫游更为顺畅,因为身份认证可以在需要连接之前完成。图 8-7(b) 中所显示的每个数字,为表 8-1 所列的时序值。

8.4.2 802.11i 事先身份认证与密钥快取

如果网络采用 802.1X 进行身份认证,从加入 802.11 网络,到能够送出网络协议封包,最费时的步骤就是 802.1X 身份认证,特别是搭配需要来回传送好几个帧的 EAP 认证方式。事先身份认证让工作站得以在与基站连接之前,事先建立一个安全的过程环境,如图 8-8 所示。基本上,事先身份认证将连接过程与安全程序加以拆解,让它们能够独立进行。WPA 则明确排除了事先身份认证的使用。

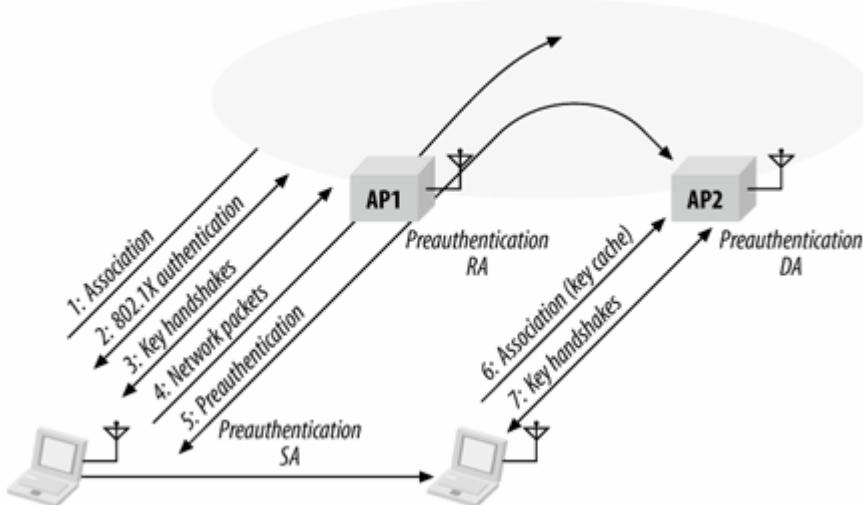


图 8-8: 802.11i 事先身份认证

图 8-8 显示了如下几个步骤:

1. 工作站连接到它在网络上所发现的第一部基站。之所以选择与这部基站连线，是根据工作站韧体的判断标准 (criteria)。
2. 连接之后，工作站就可以进行 802.1X 身份认证。这个步骤使用第六章所提到的 EAPOL 帧，它的 Ethertype 类型代码为 88-8E(十六进制)。基站会将 EAPOL 帧转换为 RADIUS 封包，连接 (session) 的真实性也经过验证 (authenticated)。
3. 双方分别会产生无线电波链路所使用的动态密钥，以四道磋商 four-way handshake 产生成对密钥 (pairwise keys)，以群组密钥磋商 (group key handshake) 产生群组密钥。
4. 当密钥配置设置完成，工作站就等于「上线」(on the air) 了，可以收发网络协议封包。

工作站软件掌控了漫游的行为，如果对它有利，就可以进行漫游。在移动的过程中，工作站发现 AP2 似乎是较好的选择，所以开始进行事先身份认证，加快移转到 AP2 的程序。不过，工作站并不是一并移转所有事项，而是利用事先身份认证，缩短收送网络封包因此中断的时间。

5. 工作站送出一个 EAPOL-Start 信息给新的基站，揭开事先身份认证的序幕。工作站每次只能与一部基站连接，因此事先身份认证帧必须通过旧基站转达。事先身份认证本身属于完整的 802.1X 交换程序。

a. 事先身份认证帧使用编号范围 88 到 C7 (十六进制) 的 Ethertype，因为大多数基站对正常的身份认证 Ethertype 会做特别的处理。此帧的来源地址为工作站，接收端地址为目前基站的 BSSID (在本例中为 AP1 无线界面的 MAC 地址)，而目地端地址则是新基站的 BSSID (在本例中为 AP2 的无线界面)。

b. AP1 收到以后，就会通过传输系统 (distribution system)，将帧传给 AP2。基站本身只有一个 MAC 地址。如果这两部基站不是位于相同的 Ethernet 广播网域，必须通过别的方式在两者之间传递事先身份认证帧。

- c. 在整个过程中，工作站仍然与 AP 保持连接，也可以使用目前经加密的连接来收发网络封包。由于工作站仍在线上，因此不会发生需要进行其他身份认证的情况。
- d. 事先身份认证的结果，是与 AP2 建立起一个安全的过程环境（security context）。工作站与 AP2 各自产生对主(pairwise master key)，进一步处理后，以之产生工作站与 AP2 之间的密钥。工作站与基站均将成对主钥存放于密钥快取中。
- 6. 当工作站扣下扳机（pull the trigger），连接关系就会移转到 AP2。作为初始连接程序的一部分，工作站将会提供密钥快取的副本，告诉 AP2 它已经通过身份认证。
- 7. AP2 收到身份认证要求，开始搜寻本身的密钥快取。找出可用密钥之后，便立刻启动成对密钥的四道磋商程序。在衍生密钥的过程中，短时间内工作站将无法正常收送封包。当 802.11 事先身份认证启动时的 802.1X EAP 身份认证之际，还是可以通过原本已验证的连接收送网络帧。第一次连接过程较慢，因为需要进行完整的 EAP 交换程序。使用事先身份认证之后，即可大幅缩短后续连接的换手时间。

8.5 连接过程

一旦完成身份认证，工作站就可以跟基站进行连接（或者跟新的基站进行重新连接），以便获得网络的完全访问权。连接（association）属于一种记录(recordkeeping) 程序，它让传输系统(distribution system) 得以记录每部行动式工作站的位置，以便将传送给行动式工作站的帧，转送给正确的基站。形成连接之后，基站必须为该行动式工作站在网络上注册，如此一来，发送给该行动式工作站的帧，才会转送至其所属基站。其中一种注册方式系送出一个 ARP 信号，让该工作站的 MAC 地址得以跟「与基站连接的交换埠」形成连接。

连接只限于 infrastructure（基础型）网络，在逻辑上等同于在有线网络中插入网线。一旦完成此程序，无线工作站就可以通过传输系统与整个世界连接，而其他人也可以经由传输系统予以回应。802.11 在规格中公开禁止工作站同时与一部以上的基站形成连接。

8.5.1 连接程序

基本的连接程序如图 8-9 所示

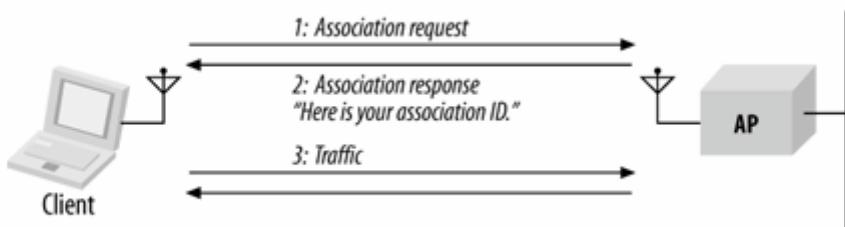


图 8-9：连接程序

和身份认证一样，连接过程是由行动式工作站发起的。在此并不需要用到顺序编号，因为连接程序只牵涉到三个步骤。其中所用到的两个帧，被归类为 association 管理帧。和单点传播(unicast) 管理帧一样，连接程序的步骤系由一个连接帧及必要的链路层回应所组成：

1. 一旦行动式工作站与基站完成身份认证，便可送出 Association Request（连接要求）帧。尚未经过身份认证的工作站，会在基站的答复中收到一个 Deauthentication（解除连接）帧。

2. 基站随后会对连接要求进行处理。802.11 标准并未规范如何判定准许连接与否；这因基站的实现而异。较常见的方法为，考虑帧暂存所需要的空间大小。以 Association Request（连接要求）帧中的 Listen Interval（聆听间隔）字段来推算，大致上可以粗略推估。

a. 一旦连接要求获准，基站就会以代表成功的状态代码 0 及连接识别码（Association ID，简称 AID）来回应。AID 本身是数值形式的识别码，在逻辑上则是用来辨识暂存帧所要传递的行动式工作站。此一程序大部分的细节，参见 8.6 节〈节省电力〉。

b. 连接要求如果失败，就只会传回状态码，并且中止整个程序。

3. 基站开始为行动式工作站处理帧。在常见的产品中，所使用的传输系统介质通常是 Ethernet。当基站所收到的帧目的地为「与之连接的行动式工作站时」，就会将该帧从 Ethernet 桥接至无线介质，如果该行动式工作站处于省电（power-saving）状态，则为之暂存帧。在分享式 Ethernet 中，该帧会被送至所有基站，不过只有正确的基站会进行桥接处理。在交换式 Ethernet 里，该工作站的 MAC 地址得以跟某个特定的交换埠（switch port）形成连接。当然，该交换埠必须连接到目前为该部工作站提供服务的基站。

8.5.2 重新连接程序

重新连接（reassociation）是指将连接关系自旧基站移转至新基站的程序。在空气中，这个过程几乎和连接（association）没什么两样；不过在骨干网络方面，基站之间会彼此沟通，以便移转帧。当工作站从某部基站的涵盖范围移转至另一基站时，就会进行重新连接程序，以便把自己的新位置通知 802.11 网络。此一程序如图 8-10 所示。

整个程序开始之前，行动式工作站必须已连接某部基站。工作站会持续监测从「目前的基站以及同一个 ESS 中其他基站」所收到的信号品质。一旦行动式工作站检测到其他基站或许是较好的连接对象时，就会启动重新连接程序。用以做出转台决定的考虑因素，因产品而异。所收到的信号强度可根据每个帧加以判定，Beacon（信标）的传送是否恒常也可以作为判定基站信号强度的基准。在进行第一个步骤之前，行动式工作站必须先与新的基站完成身份认证的程序。

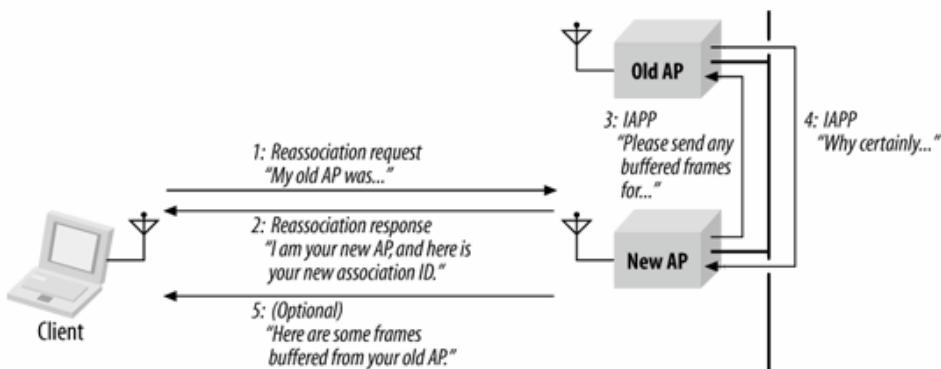


图 8-10：重新连接程序

图 8-10 描述了以下步骤：

1. 行动式工作站对新的基站发出 Reassociation Request（重新连接要求）。Reassociation Request 的内容与 Association Request（连接要求）相同，唯一的差别，在于 Reassociation Request 帧中包含了一个用来记载旧基站地址的字段。新基站必须与旧基站取得连系，以判定该工作站之前的连接是否存在。虽然 IEEE 已经定义出标准的基站间协议（inter-access point

protocol，简称 IAPP），不过有些实现产品还是使用自行开发的专属格式。如果新基站无法验证旧基站是否已经对工作站进行过身份认证，新基站就会回应一个 Deauthentication（解除身份认证）帧，同时中止整个程序。

2. 基站开始处理 Reassociation Request（重新连接要求）。Reassociation Request 的处理方式与 Association Request 类似，以同样的决定因素来判定是否允许重新连接：

- 如果 Reassociation Request 获准，基站就会传回代表成功的状态码。, 以及 AID。
- 如果 Reassociation Request 失败，则只会传回状态码，而程序也会跟着中止。

3. 一新基站和旧基站取得连系，以完成整个重新连接程序。基站间的连系属于 IAPP 的一部分。

4. 旧基站把「为该行动式工作站所暂存的帧」移交给新基站。802.11 标准并未规范基站间如何沟通；填补这项遗漏是当前 802.11 工作小组的主要任务之一。移交暂存帧后：

- 旧基站为该行动式工作站所暂存的帧均会被移转给新基站，以便传递给该行动式工作站。
- 旧基站中止其与该行动式工作站间的连接关系。行动式工作站同时间只能与一部基站连接。

5. 新基站开始为该行动式工作站处理帧。当基站收到目的地为该行动式工作站的帧时，就会将此帧由 Ethernet 桥接至无线介质，如果该行动式工作站处于省电模式，则为之暂存帧。

如果工作站离开之后重新返回某部基站的涵盖范围，也可以用重新连接程序再度加入该网络。如图 8-11 所示。

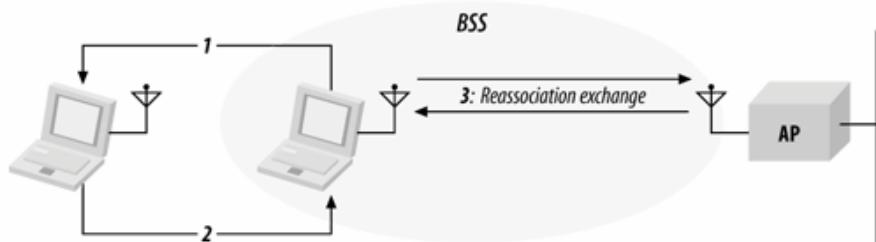


图 8-11：与同一部基站重新连接

何谓漫游（roaming）？

802.11 标准完全没有提到漫游（roaming）这个字眼。（最近才成立一个任务小组负责解决漫游问题，但是离见到成果还有一段距离。）不过在谈论 802.11 时，很多人经常会使⽤漫游这个非正式的名词。“一般而言，多数人都认为漫游就是从一部基站转换到另一部。”

过去几年，漫游一直受困于「名词泛滥」（buzzword overload）的处境，如今，漫游对不同的使用者而言有不同的意涵。基本上，漫游是指工作站转换基站的程序。工作站如何决定是否转换凭据呢？802.11 标准对此完全不置一词。决定是否转换基站完全取决于所使用的软硬件，由各家厂商自行决定。有些用户端设备会选择界面刚启动时最强的信号，然后与之终身厮守，只有在完全收不到信号时才会转换基站、有些设备永远追随信号最强者，要是有两个信号难分轩轾，就会在基站间不断切换。一些其他的设备则会将最近的连接纪录纳入考虑，避免在两部邻近的基站间进行不必要的切换。工作站如何决定是否以及何时转换基站，完全视厂商如何决定。原谅我套句 Milton Friedman 的话，「不论何时何

地，漫游均属用户端现象」（roaming is always and everywhere a client phenomenon）。

【译注】

【译注】Friedman 是美国著名的经济学家。换个比较通俗的说法作者的意思是「不论何时何地，漫游与否都是用户端的自由」。

深究第二层涵义，「漫游」意味着工作站如何能够在转换基站的同时，仍然维持原有的网络连接（network connection）。如果涉及 IP 子网络的界限问题，复杂度就相形提高，这说必须在所有标准以外加以解决。第 21 章在探讨如何组建一个无线局域网络时，还提到了如何达到跨网络拓朴的无间隙漫游。

有时候漫游会被赋予其他意义，意指从某一种网络连接（例如 802.11 无线局域网络）切换到性质截然不同的网络（例如 3G 移动电话网络）的过程 IEEE 已经成立另外的工作小组，负责定义可以在不同 IEEE 802 网络中转移网络连接与状态的漫进过程。

8.6 节省电力

无线网络的主要优点在于，当节点访问网络时，不必位于特定位置上。要充份利用移动性的优点，就不能有什么因素限制节点的位置，包括电源的供应。因此，移动性同时意味着，行动设备会使用电池供电。不过电池的电力有限，只能够维持一些时间。至少，要求行动用户经常转回以市电供电就很不方便。有些无线应用需要较长的电池供电时间，以免影响到网络连接品质（connectivity）。

和其他网络界面一样，在无线网络中关闭收发器（transceiver）将能节省可观的电力。只要关闭收发器，该界面可说是进入休眠（sleeping）、假寐（dozing）或省电（power-saving，简称 PS）模式。当收发器再度打开，该界面则可谓重新苏醒（awake）、欧动（active）或者简单称为开机（on）。对 802.11 而言，其节省电源的方式为，尽量减少后者所花费的时间，同时尽量延长前者所持续的时间。不过，802.11 这种做法并不会牺牲掉网络的连接品质。

8.6.1 Infrastructure（基础型）网络的电源管理

在 Infrastructure 网络中，电源管理可得到最大的效用。所有传送给行动式工作站的数据都必须流经基站，因此基站是暂存数据的理想地点。大多数数据均可以被暂存。标准当中禁止暂存需要依序传送（in-order delivery）或者设置 Order 位元的帧，因为暂存过程在实现上有可能将帧重新排序。基本上并没有必要设计分散式暂存系统，因为如此一来每部工作站都得实现这项功能；所以不如将整个工作交给基站负责。在定义上，基站必须知道每部行动式工作站的位置，而且行动式工作站可以对所属基站交待本身的电源管理状态。此外，基站必须随时保持清醒；前提是，基站必须持续得到电力供应。因此，在 infrastructure 网络中，基站在电源管理上扮演著关键性的角色。

基站具备两项与电源管理相关的任务。其一，因为基站知道所连接的每部工作站的电源管理状态，因此只要该工作站处于作用（active）状态，基站即可判定，应该将帧传送至无线网络，否则就得为之暂存帧。不过，只是为之暂存帧，并不足以让行动式工作站得知应该提取等待中的帧。在 infrastructure 网络中，周期性地公告暂存状态，对于电力的节省也不无贡献。开启接

收器聆听暂存状态，远比周期性地送出探查帧，所耗费的电力要少得多。除非收到必要的通知，否则工作站根本不用耗费电力来启动传送器送出探查帧。

电源管理在设计上是针对以电池供电之行动式工作站的需要。行动式工作站可以休眠一段时间不去使用无线网络界面。在连接要求中，与此相关的参数是 Listen Interval（聆听间隔），代表行动式工作站可以选择休眠几个 Beacon 周期。较长的聆听间隔，会用掉基站较多的暂存空间；因此，聆听间隔是评估「支持某个连接所需资源」时会用到的关键参数之一。聆听间隔可以视为工作站与基站的一项契约。一旦同意在休眠期间为工作站暂存帧，表示基站同意在丢弃这些帧之前，至少须等候聆听间隔所设置的时间。如果在每个聆听间隔之后，行动式工作站并未检视暂存帧，基站就会直接将帧丢弃，而不再另行通知。

8.6.1.1 暂存单点传播帧，以及使用 TIM 来传递

当有帧被暂存（buffered）时，目的节点的连接识别码（Association ID，简称 AID）可以在该帧及其目的地之间提供逻辑链路（logical link）。逻辑上，每个 AID 可将「暂存帧」连系至该 AID 所指定的行动式工作站。组播（或多点传播）与广播帧被暂存时，会被连系至数值为 0 的 AID。被暂存之组播与广播帧的传递将会在下节说明。

光是做到了暂存还不够。如果工作站一直未能提取为之暂存的帧，根本毫无意义。为了通知工作站有帧待传，基站会产生所谓的数据待传指示信息（traffic indication map，简称 TIM），并且通过 Beacon 帧加以传送。TIM 本身是由 2008 个位元所构成的虚拟位元对映表（virtual bitmap）；由于采用 offset（偏移量）的处理方式，因此基站只须传送虚拟位元对映表的一小部分。如果只有少数工作站有暂存帧待传，这种做法可省下不少网络资源。TIM 中的每个位元均会对映到特定 AID；设置与特定 AID 相应的位元旗标，代表基站为该 AID 所对映的工作站暂存了单点传播帧。

无线工作站必须苏醒过来，并进入作用（active）模式，聆听 Beacons 帧，以便接收 TIM。只要检视 TIM，工作站即可判定基站是否有帮自己暂存帧。要撷取基站所暂存的帧，行动式工作站可以使用 PS-Poll 控制帧。如果基站同时为多部行动式工作站暂存帧，这些工作站在传送 PS-Poll 之前，必须使用随机 backoff 算法来决定访问顺序。

每个 PS-Poll 帧只用于撷取一个暂存帧。帧从暂存区被移除之前，必须得到接收端的正面回应。正面回应是必要的，如此一来可以避免第二个或重试的 PS-Poll 被自动当成回应信息（implicit acknowledgment）。整个过程如图 8-12 所示。

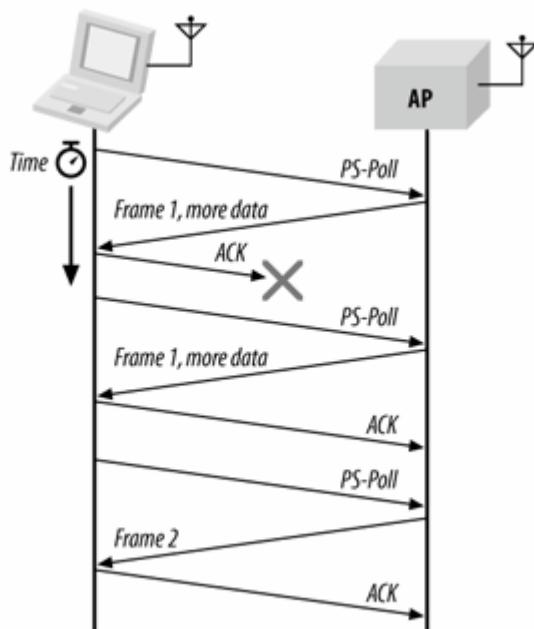


图 8-12：以 PS-Poll 捷取暂存帧

如果基站为某部行动式工作站暂存的帧不只一个，Frame Control(帧控制)字段的 More Data (尚有数据)位元就会设置为 1。行动式工作站可据此发送额外的 PS-Poll 要求给基站，直到 More Data 位元变为 0。在 802.11 标准中对此并无时间限制。

传送 PS-Poll 之后，行动式工作站必须保持清醒，直到整个交易完成，或 TIM 中与自己的 AID 相应的位元旗标已被清除。第一种情况理由十分明显：行动式工作站已经自基站成功取得暂存数据；整个交易过程包含工作站即将回复休眠状态的通知信息。第二种情况允许行动式工作站回到省电模式，如果基站将暂存帧弃置的话。当准备送给某部工作站的所有帧传送完毕，或是被基站丢弃，该工作站即可回复休眠状态。

整个暂存与递送程序如图 8-13 所示，其中显示了介质与一部基站（AP），以及与基站连接之两部处于省电模式的工作站（Station 1 与 Station 2）。时间轴上的垂直线标代表信标间隔（beacon interval）。在每个信标间隔区间，基站都会通过 Beacon 帧传送 TIM 信息元素。（本图有点简化。还有一种特别的 TIM 信息可传递组播数据，下一节会加以描述。）Station 1 的聆听间隔为 2，因此每隔两个 Beacon 周期就得醒来接收 TIM。station 2 的聆听间隔为 3，因此每隔三个 Beacon 周期即会醒来处理 TIM。工作站轴线上方的线段，代表接收端聆听 TIM 的启动（ramp-up）程序。

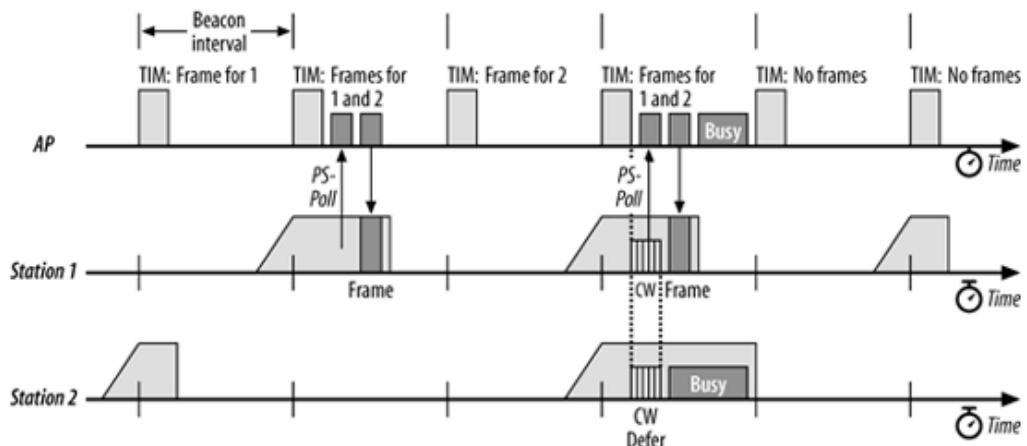


图 8-13: 暂存帧的撷取程序

在第一个信标间隔区间，只有 Station 1 的暂存帧。由于 Station 2 并无帧暂存，因此可以立即返回休眠状态。在第二个信标间隔区间，根据 TIM 的指示，基站同时存在给 Station 1 及 Station 2 的暂存帧，不过此时只有 Station 1 醒著聆听 TIM。Station 1 发出 PS-Poll 帧并且收到暂存帧，接著 Station 1 返回休眠状态。在第三个信标间隔区间，Station 1 与 Station 2 皆处在休眠状态。在第四个信标间隔区间，Station 1 与 Station 2 皆醒著聆听 TIM，根据 TIM 的指示，基站同时存在给 Station 1 及 Station 2 的暂存帧。Station 1 与 Station 2 皆准备好送出 PS-Poll 帧。并依照竞争时期 (contention window, 简称 CW) 递延程序取得介质使用权 (参见第三章)。由 Station 1 先取得介质使用权，因为它的随机延迟较短。于是 Station 1 发出 PS-Poll，并且收到基站为它所暂存的帧。在此期间，Station 2 会不断递延。假设在帧传送之后，另外一部图中并未显示的工作站取得了介质使用权，那么 Station 2 必须一直保持清醒，直到下一个 TIM 到来。如果基站此时用尽暂存空间，因而丢弃为 Station 2 暂存的帧，第五个信标的 TIM 就会显示并无暂存帧待传，此时 Station 2 终于可以返回省电模式。

工作站可以在任何时候从省电模式切换为作用模式。膝上型电脑如果使用 AC 电源，通常会充份供应周边设备电源以全力运行，只有在使用电池时才会节省电力。如果一部行动式工作站由休眠状态切回作用模式，可以不用等候 PS-Poll 即开始传送帧。PS-Poll 帧用以指示某部处于省电状态的行动式工作站临时切换为作用模式，并且准备接收被暂存的帧。在定义上，作用中的工作站，其收发器是处于持续运作的状态。切换到作用模式后，基站可以假定接收端处于运作状态，就算未收到任何告知信息。

基站为行动式工作站暂存帧的时间必须够久，方能让工作站顺利提取这些帧，不过用来暂存帧的记忆体 (buffer memory) 却是一项有限的资源。802.11 强制要求基站必须使用某种老化功能 (aging function)，以便判定帧是否暂存过久，能否加以丢弃。802.11 标准留下了相当大的空间给开发人员自行斟酌，只规范了一项限制。基站为工作站暂存数据，至少必须保存至连接时 listen interval (聆听间隔) 所指定的时间。而且标准里头还限定，如未逾越 listen interval 所指定的时间，老化功能就不能丢弃帧。除此之外，各厂商有相当大的空间，可以自行开发不同的暂存管理功能。

8.6.1.2 传递组播与广播帧：数据待传指示传递信息 (DTIM)

指定组播地址的帧，无法使用轮询算法 (polling algorithm) 来传递，因为在定义上，这些帧是发给某个特定群组的。因此，802.11 纳入了一种机制，用来暂存与传递广播与组播 (或

多点传播) 帧。暂存的方式与单点传播帧一样, 但不同于为处于休眠状态之工作站所暂存的帧。经暂存的广播与组播帧是通过 AID 0 加以储存。基站会将 TIM 的第一个位元设置为 0, 代表有广播或组播帧暂存; 此一位元相应于 AID 0。

每个 BSS 均具有一个称为 DTIM Period 的参数。TIM 是以 Beacon 信息来传送的。每当经过几个固定的 Beacon interval (信标间隔), 就会发送一个特殊的 TIM, 称为数据待传指示传递信息(Delivery Traffic Indication Map, 简称 DTIM)。Beacon 帧中的 TIM 元素包含了一个计数器, 用来倒数计时至下一个 DTIM 来临。在 DTIM 帧中, 此计数值为 0。经暂存的广播与组播数据会在 DTIM Beacon 之后加以传送。如有多个暂存帧, 则会依序加以传送。Frame Control 字段中的 More Data 位元, 用以指示是否尚有其他帧待传。频道使用权的取得规则也适用于暂存帧的传送。基站或许会选择暂缓处置所收到的 PS-Poll 要求, 直到传送完暂存区中的广播与组播帧。

图 8-14 显示了一部基站及一部与之连接的工作站。基站的 DTIM interval (数据待传指示传递间隔) 被设为 3, 因此每隔三个 TIM 就会有一个 DTIM。Station 1 处于休眠模式, 其 listen interval (聆听间隔) 为 3。每三个 beacon 周期, Station 1 就会醒来接收经暂存的广播与组播帧。每传送一个 DTIM 帧, 就会接着传送经暂存的广播与组播帧, 其后伴随与所连接工作站之间的 PS-Poll 交换程序。在第二个 beacon interval (信标间隔) 区间, 暂存区中只有广播与组播帧, 这些帧随即会被传送到 BSS。在第五个 beacon interval (信标间隔) 区间, Station 1 还有一个经暂存的 (单点传播) 帧。Station 1 可以监视 DTIM 中的指示信息 (map), 等到经暂存的广播与组播帧传送完毕后, 再发送 PS-Poll 信息。

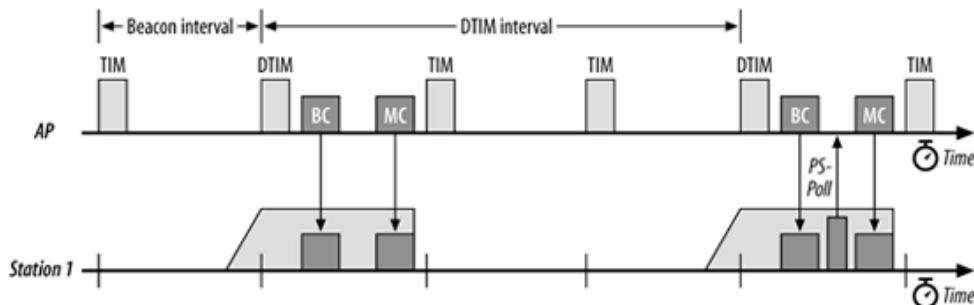


图 8-14: DTIM 之后, 传送广播与组播帧

要接收广播与组播帧, 行动式工作站必须醒著接收 DTIM 信息。不过 802.11 标准并未规范 infrastructure (基础型) 网络里进入省电模式的工作站必须醒来聆听 DTIM 信息。如果系统管理人员认为电池使用时间比接收广播与组播帧重要, 可以不用根据 DTIM 来设置工作站的聆听间隔。有些文献以极低电源作 (extremely low power)、超省电模式 (ultra power-saving mode)、沉睡 (deep sleep) 或者类似名词称之。有些产品允许设置 DTIM interval。将 DTIM interval 加长可以让行动式工作站休眠一段较长的时间, 如此可以延长电池的使用时间, 不过代价是无法即时传送数据。较短的 DTIM interval 着重在立即传送, 代价则是工作站必须经常开开关。如果电池使用时间比即时接收广播与组播帧重要, 则可以采用较长的 DTIM。至于是否适合使用较长的 DTIM, 取决于需要哪一方面的应用, 以及能否允许长时间的链路层迟延。

8.6.2 IBSS 的电源管理

IBSS 的电源管理，效率不如 infrastructure 网络。在 IBSS 中，发送端必须承受较重的负担，以确保接收端处于清醒状态。接收端也被必须更常保持清醒，不能像在 infrastructure 网络中那样休眠太久的时间。

和 infrastructure (基础型) 网络一样，independent (独立型) 网络的电源管理是以数据待传指示信息 (traffic indication message) 为基础。independent 网络必须利用某种传输系统，因为并不存在任何逻辑上的中央协调者 (central coordinator)。independent 网络中的工作站使用 ATIM(announcement traffic indication messages; 数据待传指示通知信息)，有时亦称为 ad hoc traffic indication message (特设数据待传指示信息)，强迫其他工作站保持清醒。在同一个 IBSS 当中，所有工作站皆必须在 Beacon 传送后的特定期间内聆听 ATIM 帧。

如果有某部工作站为另一部工作站暂存帧，它可以送出 ATIM 来通知对方。实际上，ATIM 帧是让收发器保持开启的信息，因为有数据待传。没有收到 ATIM 帧的工作站是否要进入省电模式，则悉听尊便。在图 8-15(a)里，Station A 为 Station C 暂存了一个帧，因此在 ATIM 传送期间 (transmission window)，会送出一个单点传播式 ATIM 帧给 Station C，目的是在告诉 Station C 不该进入省电模式。不过，Station B 可以随意关闭其无线界面。图 8-15 (b) 显示了使用中的组播式 ATIM 帧。该帧是用来通知一组工作站，不要进入低电源模式。

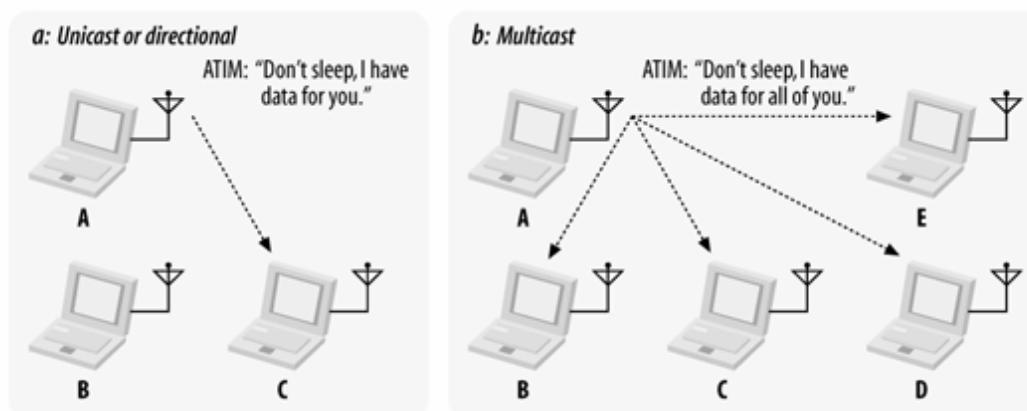


图 8-15: ATIM 的运用

信标信息之后的一段时间区间 (time window) 称为 ATIM 期间 (ATIM -window)。在这段期间，每个节点都必须保持清醒。在 ATIM 期间，任何工作站都不准关闭其无线界面。这段期间始于预料信标即将到来，终于 IBSS 建立后某个特定时点。如果因为流量负载过重，导致信标信号迟到，ATIM 期间可以使用的时间就会等量缩减。

ATIM 期间是产生 IBSS 唯一必要的参数。将之设置为 0 即可免除电源管理。图 8-16 显示了 ATIM 期间与信标间隔之间的关系。其中，第四个信标信息因为介质忙碌而迟。ATIM 期间维持不变，还是从原本预计的信标间隔起算，持续经过一个 ATIM 期间。当然，ATIM 期间可使用的时间会因为信标传送的迟延而等量减少。

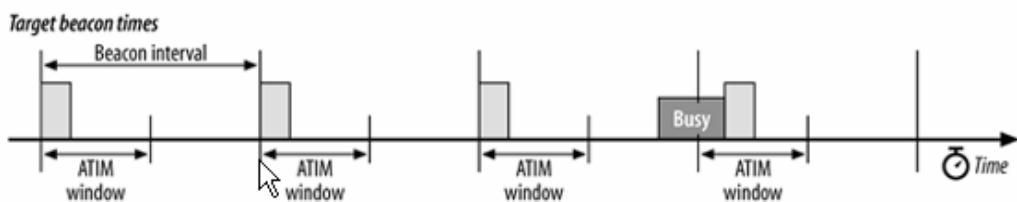


图 8-16: ATIM 期间

为了监视整个 ATIM 期间，工作站必须在信标传送之前醒来。如此一来可能会遇到以下四种情况：工作站送出一个 ATIM、收到一个 ATIM、无传送亦无接收，以及同时传送与接收。传送 ATIM 帧的工作站不能休眠。ATIM 代表传送暂存数据的企图，因此也表示准备保持清醒的意愿。ATIM 帧所针对的工作站也不可休眠，如此方能收到 ATIM 发送端所要传递的帧。如果一部工作站既传送亦收到 ATIM 帧，就会保持清醒。只有既不传送亦未收到 ATIM 帧的工作站，才可以进入休眠状态。当一部工作站因 ATIM 而保持清醒时，就会一直持续到下一个 ATIM 期间结束为止，如图 8-17 所示。其中，工作站在第一个 ATIM 期间清醒。如果该工作站未收发任何 ATIM 帧，等到该 ATIM 期间结束即可休眠。如果同时收发 ATIM 帧，工作站就会一直保持清醒，直到第三个 ATIM 期间结束，如图中第二个 ATIM 期间所示。

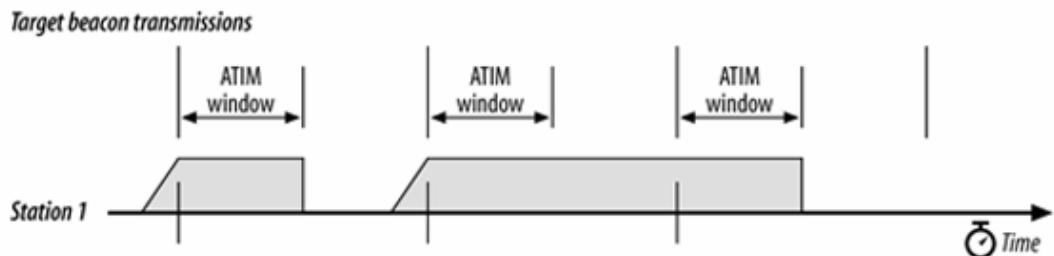


图 8-17: ATIM 对省电模式的影响

在 ATIM 期间，只能传送特定的控制与管理帧。除了 Beacon、RTS、CTS 和 ACK，当然还包括 ATIM 帧。传送时必须依循 DCF 规则。ATIM 帧之所以只能在 ATIM 期间传送，是因为在这段期间以外，工作站可能处于休眠状态。如果 IBSS 中其他工作站皆处在休眠状态，此时送出 ATIM 帧便毫无意义。同样地，单点传播式 ATIM 帧也需要得到正面回应，因为这是保证对方的确收到 ATIM 信息，并在信标间隔剩余时间保持清醒的唯一方式。组播式 ATIM 帧并不需要得到正面回应，因为要一大群工作站同时回应组播帧太没效率了。如果所有 ATIM 帧的潜在接收端都必须进行正面的回应，这些回应信息可能会打断所有的网络服务。

经暂存的广播与组播帧会在 ATIM 期间结束后予以传送，以符合 DCF 的规范。广播与组播帧传送之后，工作站可以接著传送 ATIM 所通知的单点传播帧，同时由接收端得到正面回应信息。所有的 ATIM 通知信息传送之后，工作站可以将未经暂存的帧直接传送给已知处在清醒状态的其他工作站。工作站如果有送出信标、ATIM 信息，或不能休眠时，就必须保持清醒。如果争夺介质使用权的情形十分严重，将导致之前发布 ATIM 的工作站无法如期送出暂存帧，则该工作站必须在下一个 ATIM 期间开始之后，重新发布 ATIM。

图 8-18 显示了以上所提到的某些规则。在第一个信标间隔，Station 1 传送了一个组播式 ATIM 给 Station 2、3 和 4。组播式 ATIM 帧无须得到正面回应，不过 ATIM 的发布，意味着所有工作站都必须保持清醒直到下一个 ATIM 期间结束，以便从 Station 1 处接收组播帧。当 ATIM

期间结束，Station 1 即可传送经暂存的组播帧给其他三部工作站。之后，Station 4 可以利用下一个信标到来之前的剩余时间，传送一个帧给 Station 1。这个帧并非通过 ATIM 发布，但它知道对方必定处于清醒状态。

在第二个信标间隔区间，Station 2 与 Station 3 均有准备传送给 Station 4 的暂存帧，因此它们会各自送出一个 ATIM。而 Station 4 则分别加以回应。在 ATIM 期间结束之后，Station 1 既未传送也未收到任何 ATIM 信息，因此可以进入省电状态，直到下一个信标间隔开始。不过，Station 2 的帧相当大，因此剥夺了 Station 3 传送帧的机会。

当第三个信标间隔开始时，Station 3 仍然有一个经暂存的帧要给 Station 4。因此 Station 3 会重新传送一个 ATIM 帧给 Station 4，而 Station 4 亦会加以回应。此时 Station 2 和任何 ATIM 的交换都没有关系，因此在 ATIM 期间结束后即可进入省电状态。由于此时已经没有任何暂存的广播或组播帧，因此 Station 3 可以开始传送之前宣布要给 Station 4 的帧。帧传送完毕之后，Station 4 可以趁下一个信标帧来临之前，传送一个帧给 Station 3，因为 ATIM 交换程序的缘故，可以推论 Station 3 必然还处于清醒状态。

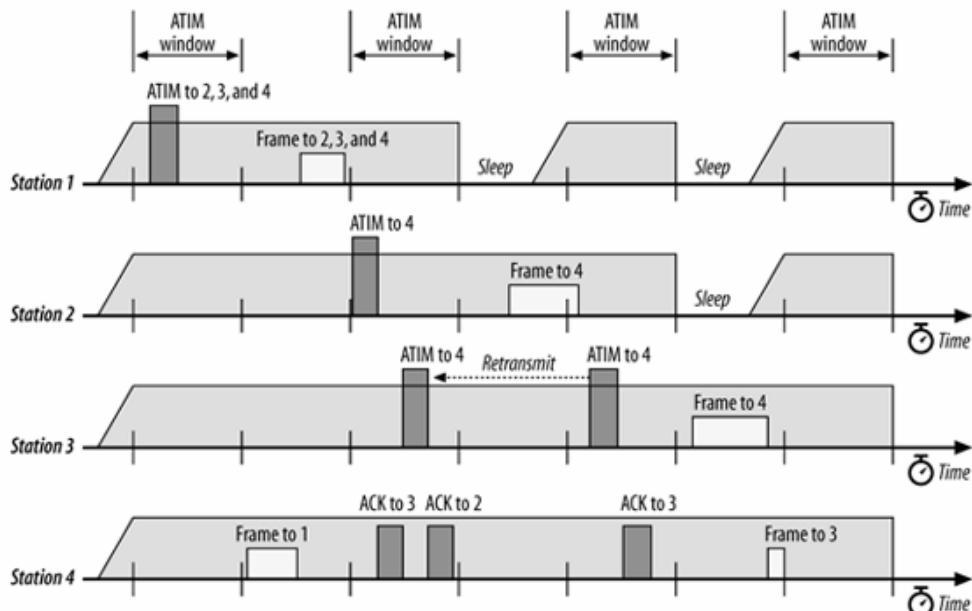


图 8-18: ISSS 网络中，ATIM 对省电模式的影响

工作站必须负责维持足够的记忆体供暂存帧之用，不过要使用多大的暂存区，实际上必须在挪作他用与否之间做出取舍。802.11 标准允许 independent（独立型）网络中的工作站丢弃暂存过久的帧，不过实际做判断的算法并不在标准的范围之内。对任何暂存管理功能而言，惟一的要求是暂存帧至少得保存一个信标周期。

8.7 计时器的同步

和其他无线网络技术一样，802.11 十分仰赖传递给各节点的计时信息。在跳频网络中，计时信息特别重要，因为网络上所有工作站都必须以事先协调好的样式切换频。在介质保留机制中，也会用到计时信息。

除了工作站内部的计时，基本服务区域中每部工作站都必须保存一份计时同步功能 (timing synchronization function，简称 TSF) 的副本；该副本是与基本服务区域中所有其他工作站之

TSF 同步过的内部计时器。TSF 以 1-MHz 的时脉运作着，每微秒「作用」（tick）一次。Beacon 帧的另一个作用，就是定期对网络上的工作站发布 TSF 值。在 timestamp（时戳）字段中，所谓「now」（现在）是指时戳第一个位元到达传送端物理层的时刻。

8.7.1 Infrastructure 的计时同步

电源管理在 infrastructure 网络中相当简单，这是因为有基站作为数据传输与电源管理功能的协调中心。在 infrastructure 网络中，计时功能也采取类似的做法。由基站负责维护 TSF 时间，任何与之连接的工作站都必须将基站的 TSF 视为有效而加以接受。

一旦基站准备传送 Beacon 帧，基站计时器就会被复制到 Beacon 帧的 timestamp 字段。与该基站有连接关系的工作站，会从所收到的 Beacon 帧中取得该值，不过会稍作调整，将天线与收发器的处理时间纳入计算。与基站连接的工作站会维护内部的 TSF 计时器，因此即使漏失掉某个 Beacon 帧，也可以粗略与整体的 TSF 维持同步。无线介质充满杂讯是可以预期的，不过 Beacon 帧无须加以正面回应。因此，经常会漏失 Beacon 帧早在预料当中，工作站内部的 TSF 计时器可以减缓偶尔漏失 Beacon 帧的影响。

为了协助进行主动扫描的工作站符合 BSS 所要求的参数，计时值也会出现在 Probe Response（探查回复）帧中。当工作站借由扫描发现一个网络时，就会从该网络的 Beacon 或 Probe Response 帧记录下 timestamp 及收到 timestamp 时本身计时器的值。为了将内部的计时器调整到与网络计时器相符，工作站会随即从所收到的网络公告中取出 timestamp，然后加上收到该 timestamp 后所经过的时间。图 8-19 显示了这整个过程。

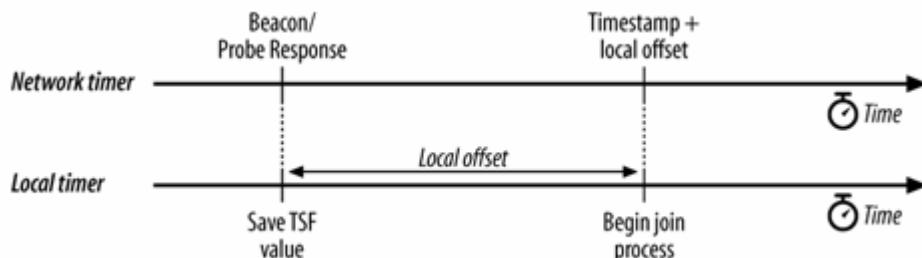


图 8-19：让内部计时器与网络计时器相符

8.7.2 IBSS 的计时同步

IBSS 并不存在中央协调单元，因此 Beacon 是由工作站轮流传送的。TSF 的维护工作属于 Beacon 产生过程的一部分。时间会被切割成相当于两个 Beacon 帧中介时间的片断。Beacon 帧预设会在信标间隔结束时发送，这就是所谓的信标预定传送时间（target Beacon transmission time，简称 TBTT）。Independent（独立型）网络是以 TBTT 作为导引方针。

IBSS 中所有工作站会准备在预定时间（target time）传送 Beacon 帧。当预定时间接近时，所有其他传输都会暂停。Beacon 或 ATIM 除外，所有的帧传输计时器均会中止，等候介质净空，以便传送更重要的管理帧。IBSS 中所有工作站都会为 Beacon 传输产生一个 backoff（延后）计时器；所谓 backoff 计时器，是介于 0 与该介质 minimum contention window（最短竞争期间）两倍时间的随机延迟（时间）。TBTT 结束后，所有工作站即从 Beacon backoff 计时器的值倒数至 0。如果工作站在传送时间之前就收到 Beacon 帧，该预定要进行的 Beacon 传输就会被取消。

在图 8-20 中，每部工作站各自选择了一个随机迟延值；Station 2 所产生的随机迟延值最短。当 Station 2 的计时器逾时，即会传送一个 Beacon（信标）、此时 Station 1 与 Station 3

均会收到该帧。因此，Station 1 与 Station 3 均会取消 Beacon 的传输。由于计时器同步可以确保所有工作站的计时器均已对时。所以同时出现几个 Beacon 帧并不会造成问题。接收端只要多处理几次 Beacon 帧，多更新几次 TSF 计时器即可。

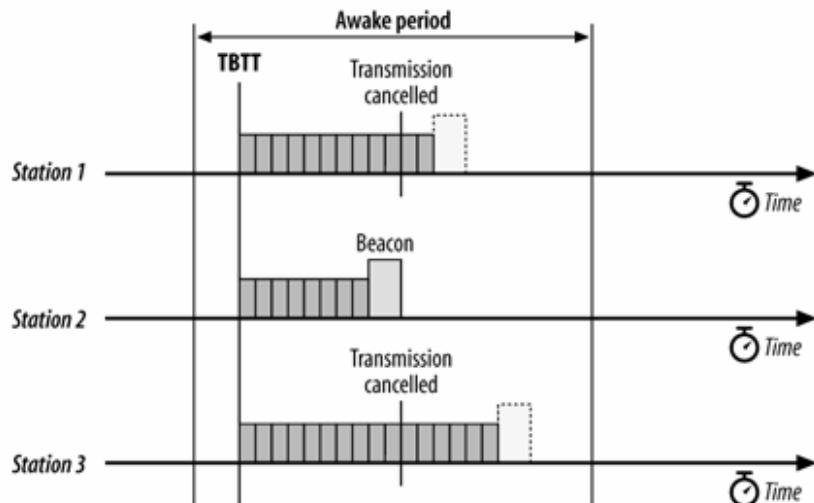


图 8-20：轮流产生 Beacon 信息

Beacon(信标)的产生与电源管理的关系十分密切。Beacon 帧的发出时间，必须在每个 Beacon interval 的作用期间，如此一来，所有工作站方能同时醒著处理该帧。此外，帧的传送端不可进入低电源(low-power)状态。必须一直保持清醒，直到下一个作用期间结束。这个规则能够确保至少有一部工作站处于清醒状态，以便回复正在进行扫描、准备加入网络的新工作站。

在 independent 网络中，是否采用所收到的 timestamp，判断的规则比较复杂。既然没有中央标准时间，802.11 标准的做法是采用 BSS 中运作时脉最快的计时器。收到一个 Beacon 帧之后，该 timestamp 会被稍作调整，并计算处理时所耗费的迟延时间，然后与工作站内部的 TSF 比较。只有当所收到的 timestamp 晚于内部计时器，才会以该 timestamp 更新内部计时器。

8.8 频谱的管理

802.11a 原本只是针对美国所开发的标准。欧洲对于 5GHz 频段的管制较为严格，因此若要适用于欧洲，就必须对 802.11 MAC 进行特别的修改。这项过程的开发成果，最后在 2003 年成为 802.11h 标准。

8.8.1 传输功率控制 (TPC)

欧洲管制当局要求使用传输功率控制 (Transmit Power Control, 简称 TPC)，^{【注 1】} 是为了确保 5GHz 频段的无线电波发射器符合功率限制，以及避免干扰特定的卫星服务。能够更精确地控制传输功率同时带来其他好处，其中一些是移动电话产业早已熟知的。高功率的用户端传输可以涵盖非常大的范围。在基站密集的网络中，高功率工作站的传输距离或许大于所需。传输距离较长不见得都是好事。以高功率运作的无线电波发射器会缩短电池使用时间。如果传输距离大于所需，额外可及的范围就代表「浪费掉」的功率。功率较大也可能导致网络传输量下降，因为用户端设备之间会产生不必要的干扰。

为了说明高功率工作站所导致的问题,请参考图 8-21。图中的网络配置了九部基站。Client#1 连接到了位于第一列中央的基站。如果该工作站设置以最大功率进行传输,那么传输距离将可到达外圈所标示的范围。不过,它和基站之间的传输只需要用到内圈的功率。两个同心圆之间的差异,就是所超出的传输范围。无线电波发射器使用高于必要的功率,将会比使用适当功率更快消耗电池的使用时间。(为了延长手机电池的使用时间,移动电话网络已经采用功率控制技术多年。)

- 【注 1】ERC/DEC/(99)23 可自 <http://www.ero.dk/doc98/Official/Pdf/DEG9923E.PDF> 取得。
- 【注 2】配置九部基站的网络中只规划了三个非重叠频道是不可能的,这就是在基站密集的环境中应该使用 802.11a 的最佳理由。

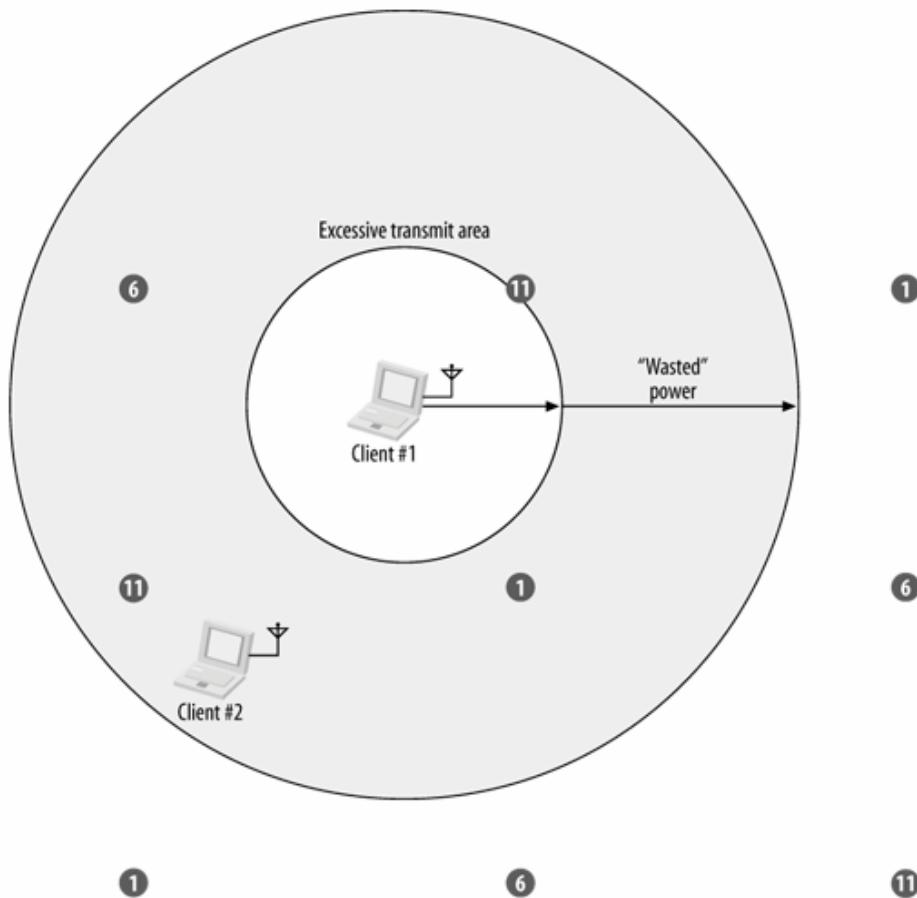


图 8-21: 高功率工作站与基站间的干扰

控制传输距离也可以让网络运作得更加顺畅。所有传输过程都必须取得无线电波介质的独家使用权。如果功率过高,传输过程的涵盖范围就会超过所必须的。位于外圈之内使用 11 频道的任何工作站,都会因为 Client#1 正在进行传输而受到影响。最佳传输功率与额外功率之间的

阴影区代表受到影响的地帶，因为 Client#1 正以过高的功率进行传输。例如，Client#2 这时就无法与邻近的基站进行传输，因为它必须和 client#1 共用无线电波介质。降低传输功率到适可而止的水准，可避免邻近基站间产生重叠，从而改善整体传输量。

8.8.1.1 传输功率控制的基本过程方式

传输功率控制 (TPC) 是一项 802.11 服务，主要是为了尽量降低传输功率至可用水准。除了考虑管制当局所允许的最大功率，还会考虑到其他限制。虽然设计上是为了满足管制当局的要求，传输功率控制也会带来其他好处。

任何无线电波传输的绝对上限是由管制当局所规定，通常列在当局所出版的相关文件或法规当中，最大管制功率可以在基站或工作站中加以设置，也可以从包含 Country 信息元素的 Beacon 帧中得知。此外，无线电波的传输或许还有其他进一步限制最大传输功率的规范。欧洲管制当局的规定更为严格，至少必须再降低 3dB 以避免干扰卫星服务。

最大传输功率是由 Beacon 帧中的 Country 信息元素所指定，因此任何连接到网络的工作站均可得知。Country 信息元素用来指定最大管制功率 (regulatory maximum power)，至于 Power Constraint 信息元素则是用来指定网络可以使用的最大传输功率 (maximum transmission power)，这个数值通常较低。

开始过程之前，工作站必须计算出可以使用的最大传输功率。通常，它的计算方式是以最大管制功率减去任何额外的限制。例如，网管人员或许会指定本地网络所允许的最大传输功率，以缩小传输距离与避免干扰。

8.8.1.2 连接程序的变动

当具备频谱管理能力的工作站连接 (或重新连接) 到基站时，首先必须在 Power Capability 信息元素中提供最小与最大的传输功率。基站可以将工作站所提供的信息纳入连接程序中，并且任意使用这些信息。至于基站如何或是否使用这些信息，802.11 标准并未明确规范。功率过高以致于可能违反管制规定的工作站，便有可能无法通过相关检验。基站也可以拒绝传输功率能力太差的工作站；标准认为这会增加隐藏节点的机率，虽然似乎不致于。

8.8.1.3 变更传输功率

基站与工作站均可动态调整个别帧的传输功率。接收端可以计算出每个帧的链路边际 (link margin) 也就是把接收到的功率减去最低可接受值的差额。链路边际就是安全边际。如果接收到的功率只达工作站传输的最低可接受值，链路边际就等于零，这代表任何细微的变动均可能导致连接中断。大多数工作站均以缩小链路边际为目标，不过标准并未规范特定的链路边际计算方式，以及使用何种特定值。

为了得知传输功率的变动，工作站可以要求进行无线电波链路量测 (radio link measurement)。工作站可以送出一个 Action 帧要求提供传输报告。传回的 Action 帧中包含了一个 TPC Report 信息元素，其中具有两项描述性的统计数据。首先，它包含了报告帧 (report frame) 本身的传输功率。根据此传输功率，接收端可以估计无线电波链路的路径损耗 (path loss)。其次，此回报帧中包含链路边际值，告诉接收端已收到功率 (received power) 与最低可接受功率 (minimum acceptable power) 之间的比值。举例而言，假设最低可接受功率为 -70dBm 而实际接收到的信号 -60dBm，那么链路边际即为 10dB。如果链路边际“太高”，就可以降低传

输功率。如果链路边际“太低”，就应该提高传输功率。和 802.11 标准其他组成部分一样，“太高”或“太低”与否均留给软件自行决定。

设计上，标准是用来确保最大传输功率不致逾越规定，但并未限制功率的选择方式。对于比较进阶的功能，标准并没有提出特别的要求。不难理解为何有些支持传输功率抑制的高价基站会去追踪，将无线电波送到每部已连接工作站所需要的功率，因为较近的工作站所需要的功率将少于较远的工作站。

8.8.2 动态选频 (DFS)

除了传输功率控制之外，欧洲管制当局也要求工作站必须避免干扰 5GHz 的雷达系统，以及将功率展开到所有可用频道当中。动态选频 (Dynamic Frequency Selection，简称 DFS) 机制便是用来达成这项任务。

8.8.2.1 DFS 的基本过程方式

动态选频包含了一组程序，可以让 802.11 设备根据量测结果 (measurement) 与管制要求 (regulatory requirement) 变更无线电波频道。它可以影响一开始的连接程序以及后续的网络过程。

当工作站首度连接到网络，Association Request 帧里包含了一个 Supported Channels 信息元素，其中列出了工作站支持的频道。根据此信息元素的内容，基站可以选择是否拒绝此项连接过程，虽然标准并未规范此种行为。有项做法是干脆拒绝那些支持“太少”(too few) 频道的工作站，理论上是因为它会限制基站切换频道的能力，因为基站必须选用所有已连接工作站均支持的频道。

一旦用于实际的网络，DFS 就会定期检测频道是否可能干扰其他无线电波系统，特别是 5GHz 的欧洲雷达系统。检测频道时会暂停网络所有传输过程，然后量测潜在干扰，如果有必要，就会广播即将更换频道。

8.8.2.2 频道禁声

检测无线电波频道是在禁声期 (quiet period) 或禁声期间 (quiet interval) 进行。禁声期间是指 BSS 所有工作站临时停止传输的时间，有助于测量是否存在雷达系统的潜在干扰。禁声期是由 Beacon 与 Probe Response 帧中的 Quiet 信息元素进行排程，指定何时停止传输以及历时多久。惟有最新的 Quite 信息才算有效。如果问时间有好几个 Quite 信息，最新的一份信息会取代之前所有已排程的禁声期。在禁声期间，所有工作站均将网络配置向量 (NA1) 设为禁声期的长度，确保虚拟载波检测算法会递延所有传输过程。

当已排程的禁声期即将来临，无线电波频道还是以正常的方式访问无线电波介质，不过另外附加一项规则，亦即在禁声期开始之前，任何帧交换均必须完成。如果已经排定的帧交换过程无法完成，工作站就会释放频道的控制权，等到禁声期结束后再继续传送。不过，禁声期所导致的帧传送失败会增加重传的次数。当禁声期结束，所有工作站必须再度竞争访问无线电波频道。没有所谓跨禁声期的频道访问。

在基础型网络里，频道禁声排程完全由基站控制。基站可以决定禁声期长短，禁声期间相隔多久，或甚至完全停用。独立型网络是在网络成立时选择禁声期的排程。轮到新工作站负责发送 Beacon 与 Probe Response 帧时也无法改变禁声期参数，只能沿用之前的参数。

8.8.2.3 量测

任何时刻均可进行无线电波频道量测。工作站可以要求其他工作站进行无线电波频道量测。来自工作站的量测信息对基站而言特别有用，因为这些提供报告的工作站可能分布在各个不同的地理区位。不论是否在禁声期间，均可以进行量测过程。

任何工作站均可要求其他工作站进行量测。此要求系通过 Measurement Request 帧来发送，如图 8-23 所示。基础型网络里，所有帧均必须流经基站。已连接的工作站只能要求基站提供无线电波信息。只要适时发出要求帧，基础型网络的基站即可要求单一或一组工作站进行量测。独立型网络并没有中枢控制单元，因此任何工作站均可发出要求给单一或一组工作站。虽然允许使用群组地址字段来提出要求，不过接到要求的工作站也可以不予理会。

送出量测要求后，工作站会假定对方需要一些时间来为它的回应搜集数据。送出量测要求后，工作站不得再发送任何其他帧。

接收到 Measurement Request 帧后，工作站必须判断如何回应。Measurement Request 帧非回应不可，即使答复的内容是拒绝进行量测。要进行处理，量测要求必须有足够的时间进行设置与量测。量测要求中会指定进行量测的时间。如果要求被置于伫列的同时正在进行冗长的传输，不难想见它会在要求量测的时点之后才到达目的地。工作站可以不理会这些“迟到”的要求。接收到量测要求的一方必须搜集要求中所指定的数据。能否支持所有要求，视接收端的硬件而定。并非所有 802.11 硬件均能够支持多频道过程，虽然这种情况已经日渐减少。^{【注】}如今，市面上还是有些卡片不支持多频道过程，因此无法应付量测目前过程频道以外的要求。工作站可以因为其他不明原因拒绝进行量测，除非提出的一方强制要求(mark the request as mandatory)。

除了要求进行量测的轮询过程，就算无人提出要求，工作站也可以主动发送 Measurement Report 帧，提报相关的统计数据。

8.8.2.4 雷达扫描

【注】例如采用 Radiata 芯片组的 Cisco CB-20 网卡只能支持八个较低的 802.11a 频道。这类卡片就应当拒绝较高的 U-NII 频段的量测要求。

要求频道禁声的一个主要理由，是为了搜寻是否存在欧洲所使用的 5GHz 雷达系统。至于采用何种搜寻方式，管制当局并未强制规定。^{【注】}管制当局只要求当信号强度超过某个特定干扰门槛，就必须进行雷达检测。

启用无线电波界面时，必须搜寻所使用的频道是否存在雷达信号。除非“毫无危险”(coast is clear) 且确定附近没有雷达会遭受干扰，否则不准进行传输。过程中必须定期进行雷达检测。一旦检测到雷达信号，网络就必须进行频道切换以避免干扰。

频谱管理服务允许网络切换到其他频道。之所以决定切换频道，或许是因为出现雷达干扰，不过除了用来符合欧洲无线电波管制，频道切换机制还有其他用处。有能力变更过程频道的网络。可以把对其他 802.11 设备的干扰降至最低，因此可以优化无线电波的使用计划。

频道切换是设计来尽可能将已连接的工作站移往新的频道，不过和其中一些（甚至是所有）工作站的通讯还是可能因此中断。标准中并未限制该如何选择新频道，只是提到基站应该尝试选用多数工作站均支持的频道。有些管制当局已经草拟出一些规定，强制必须将无线电波能量展开至整个频段，如此一来，管制规定强迫切换的频道，有可能无法得到所有工作站的支持。

在基础型网络里，过程频道的选择完全由基站所掌控。作为连接程序的一部分，基站会搜集已连接工作站支持哪些频道，基站将通过管理帧以及 Action 帧中所包含的 Channel Switch Announcement（频道切换宣告）信息元素，通知已连接的工作站何时将进行频道切换。为改善基站传送频道切换宣告的能力，可以在 PCF 帧间隔（PIFS）之后随即传送频道切换宣告。如此一来，相较于介质的基本过程，它就具备较高的优先性。标准建议，但并未要求，频道切换必须提供充分的准备时间。好让处于省电状态的工作站有机会恢复过程，并且接收频道切换宣告。

8.8.2.5 IBSS 过程

相较于基础型网络，要在独立型网络中变更过程频道显然比较困难，因为没有逻辑上的控制单元可以进行频率选择过程。独立型网络并没有基站内建的功能，而是通过 DFS owner（动态选频负责人）服务来协调各个工作站进行频率选择服务。

网络中会有一部工作站被指定为 DFS owner，负责搜集量测报告以及监控频道中是否出现雷达信号。如果独立型网络中有任何一部工作站检测到雷达信号，就会在频道对映表的子字段中汇报。一旦被告知检测到雷达信号，DFS owner 就会进行切换频道的动作。

DFS owner 负责决定使用哪个新频道，并且送出频道切换宣告帧。有时候也许无法选出一个既符合规范要求，又同时为所有工作站支持的频道。独立型网络并不存在搜集数据的中枢单元，因此就算所有工作站均支某个特定频道，也无法保证 DFS owner 有办法知道。

在独立型网络中，DFS owner 有可能改变。就像 Beacon 信号的产生，工作站可能来来去去（join or leave the network），DFS owner 也一样。万一 DFS owner 离开网络，所有工作站就会进入 DFS owner 遴选模式（recovery mode）。在这个模式当中，可以有好几部工作站同时担任 DFS owner，并且排程产生标准所要求的频道切换宣告帧中。不过，第一部传送频道切换帧的工作站才会成为 DFS owner，其他工作站则会放弃这个角色。DFS owner 遴选的概念类似图 8-20 所讨论的分散式 Beacon 帧之产生过程。

【注】ETSI EN301 893 可自 <http://www.etsi.org> 取得。

8.8.3 Action 帧

Action（行动）帧用来要求工作站采取必要的行动。频谱管理服务使用 Action 帧提出量测要求。搜集量测的结果以及宣布任何必要的频道切换。图 8-22 显示了 Action 帧的格式，基本上它是一个 category 字段加上 category 的行动细节。「行动细节」将会因为 category 字段值的不同而有所变动。

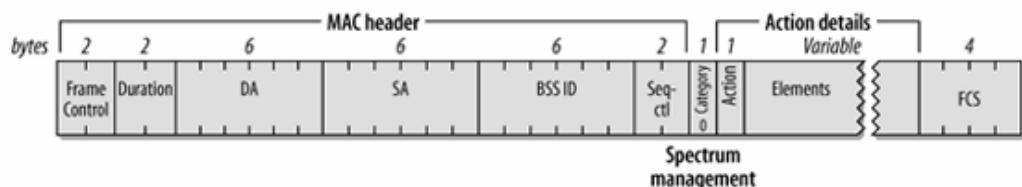


图 8-22: Action 帧

Category（种类）

设置为 0，代表频谱管理。

Action（行动）

所有频谱管理帧均使用「行动细节」的第一个位元组来指定即将采取的行动类型。表 8-2 列出了 Action 字段所有可能的值。没有列出的值代表保留未用。

Elements (元素)

频谱管理行动帧是以信息元素 (Elements 字段) 来承载信息。一些信息元素的细节详见第四章。一些额外的信息元素定义于 802.1h 并将于本节予以探讨。

表 8-2：频谱管理行动帧类型

值	频谱管理行动帧类型
0	量测请求
1	量测报告
2	TPC 请求
3	TPC 报告
4	信道切换宣告

8.8.3.1 Measurement Request 帧

Measurement Request (量测要求) 帧用来要求工作站进行量测，并将结果回传。它的格式如图 8-23 所示。此帧是由一系列量测要求信息元素所组成。可量测的项目受到帧大小而非其他因素的限制。

标准允许定期进行量测。如要启用或停用定期报告，可以传送一个量测要求，指示工作站启用或停用定期量测。基础型网络里的工作站无法要求基站停用量测功能。

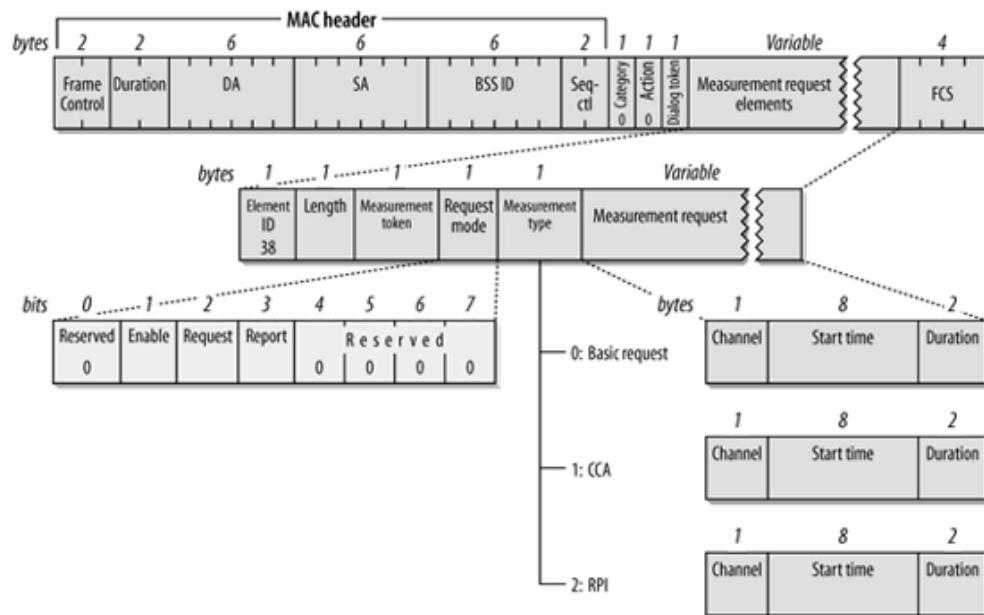


图 8-23: Measurement Request 帧

Category (种类)

设置为 0 代表频谱管理行动帧。

action (行动)

设置为 0 代表量测要求。

Dialog Token (对话标记)

此字段的作用如同序号。它会被设置为非零值，协助将量测回应对映至现有的要求。单独一个 Measurement Request 帧可以要求好几次量测，只要在帧主体中使用多个 Measurement Request 信息元素即可。如图 8-23 所示，每个信息元素组成自以下字段：

Element ID (元素识别码)

Measurement Request 元素的类型编号为 38。

Length (长度)

此字段之后的信息元素的长度，以位元组为单位。

Measurement Token (量测标记)

每个 Measurement Request 帧可以同时包含好几个要求，只要在帧主体中涵括多个 Measurement Request 元素即可。每个要求均会被赋予一个量测标记值，如此才有办法区别不同的要求。

Measurement Request Mode bitmap (量测要求模式位元对映表)

在 Measurement Request Mode bitmap 中有三个位元用来指定帧支持哪些类型的频谱管理帧。位元编号 2 (从 0 开始编号) 代表 Request 位元，设置为 1 是指传输器将处理传进来的量测要求。位元编号 3 代表 Report 位元，设置为 1 是指传输器将接受多余的报告。当这两个位元皆有效时，Enable 位元会被设置为 1。

Measurement Type (量测类型)

信息元素中所要求的量测类型，如表 8-3 所示：

Measurement Request (量测要求)

如果有量测要求，就会额外以一个字段来指定计时参数。目前已经标准化的三种量测均有相同的格式，由频道编号、量测开始时间的计时器函数值，以及量测持续时间所构成。计时器的初始值如果为零，代表应该立即进行量测。如果所发出的帧是用来启用或停用量测功能，这个字段就不会出现。

表 8-3 量测类型值

量测类型值	名称
0	基本量测
1	争空频道评估
2	接收功率指示分布图

8.3.3.2 Measurement Report 帧

Measurement Report (量测报告) 帧用来回传量测结果给提出要求者。它的格式如图 8-24 所示。此帧由一系列量测报告信息元素所组成。可量测的项目受到帧大小而非其他因素的限制。

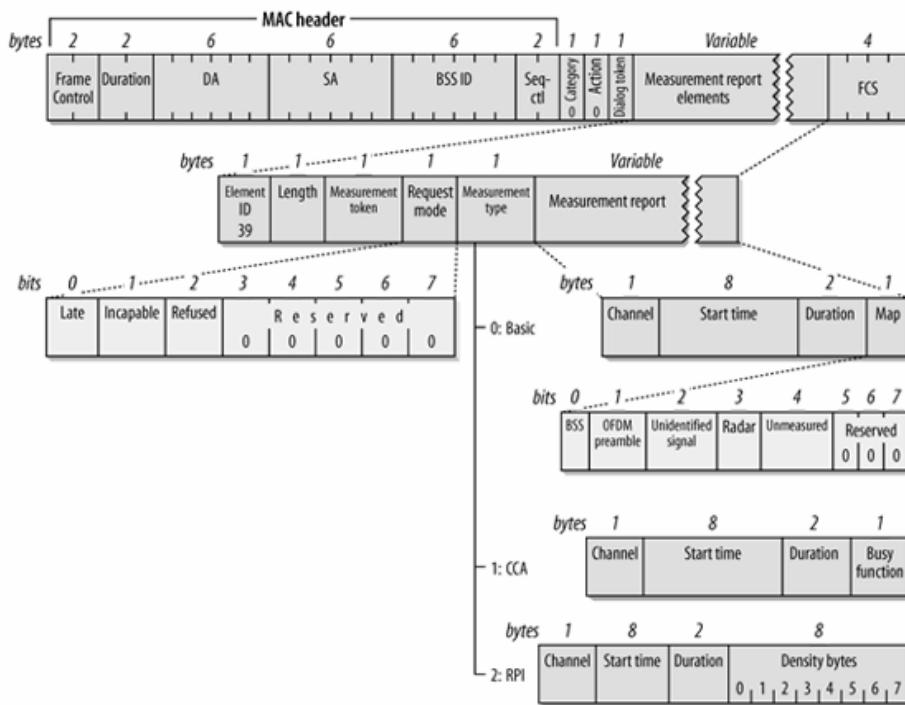


图 8-24: Measurement Report 帧

Category (种类)

设置为 0 代表频谱管理行动帧。

Action (行动)

设置为 0 代表量测报告。

Dialog Token (对话标记)

如果此量测报告用来回应另一个工作站的量测要求，要求帧中的 Dialog Token 字段就会被复制到回应信息中。如果此帧是主动发送的报告 (unsolicited report)，则 Dialog Token 为 0。

单独的 Measurement Report 帧中可以包含数个量测结果，各自以本身的信息元素进行传输。为了清楚起见，信息元素标头中只显示了一个信息元素、其所包含的三个可能的报告元素如下所示。

Element ID (元素识别码)

Measurement Report 元素的类型编号为 39。

Length (长度)

此字段之后的信息元素的长度，以位元组为单位。

Measurement Token (量测标记)

每个 Measurement Request 帧都可以提出数个要求，只要在帧主体中涵括数个 Measurement Request 元素即可。每个要求均会被赋予一个量测标记值，如此才有办法区别不同的要求。

Measurement Report Mode bitmap (量测报告模式位元对映表)

在 Measurement Report mode bitmap 中有三个位元用来指定为何量测要求被拒，如果报告帧被用来拒绝量测的话。如果量测要求到达时已经超过指定的开始时间，Late 位元就会被设置为 1。如果工作站能力不足，Incapable 位元就会被设置为 1。如果工作站有能力但不愿进行量测，Refused 位元就会被设置为 1。

Measurement Type (量测类型)

信息元素可以要求的量测类型，如表 8-3 所示。

Measurement Report (量测报告)

Measurement Report 帧包含了要求量测的数据。和 Measurement Request 不同，每种报告的内容均不相同。所有三种报告均显示于信息元素标头之下。它们分享共同的标头，此标头用来报告量测要求所指定的频道数，开始进行量测的时间，以及量测持续时间。不过，每种量测类型的报告方式均不相同。

在 basic (基本) 报告中，所显示的数据是一系列跟频道有关的位元旗标：

BSS (1 个位元)

如果在量测期间检测到来自其他网络的帧，此位元将被设置。

OFDM Preamble (1 个位元)

如果检测到 802.11a 的短同步信号，但帧其余部分并未伴随出现，此位元将被设置。HIPERLAN/2 网络使用一样的同步信号，但帧构造并不相同。

Unidentified Signal (1 个位元)

当接收到的功率够高，但无法分辨究竟是来自其他 802.11 网络（因此必须设置 BSS 位元）。OFDM 网络（因此必须设置 OFDM Preamble 位元）或者雷达信号（因此必须设置 Radar 位元），此位元将被设置。标准并未规范功率准位多高才应该设置此位元。

Radar (1 个位元)

如果在量测期间检测到雷达信号。此位元将被设置。需要检测哪些雷达系统，由管制当局定义，而非 802.11 任务小组。

Unmeasured (1 个位元)

如果未对频道进行量测，此位元将会被设置。如果没有进行量测，当然不会在频段中检测到任何信号，因此前四个位元均将被设置为 0。

在 CCA (净空频道评估) 报告中，主要字段是 CCA Busy Fraction，用来描述净空频道评估功能被设置为忙碌的时间。它的长度为一个位元组，因此这段时间会被乘上 255，以范围 0 到 255 的整数来表示，数值越高代表频道经常是比较忙碌的。

RPI histogram (RPI 直方图) 报告用来汇报界面所收到功率的分布情况。工作站可以要求一份 RPI histogram 报告，用来判断其他工作站从目前网络所取得的信号强度，或者在即将切换过程频道时，使用这项报告来对其他频道进行评估。RPI histogram 报告中包含了所收到信号的强度信息，和单一帧量测不同的是，它能够显示整个量测期间所收到之信号的功率分布情形，让接收端得以了解整体的传输准位。Histogram 包含了八个位元组，每个位元组代表所收到之信号的功率范围，如表 8-4 所示。每个位元组的值，代表信号落在该范围的功率量 (fraction of power)。所收到的信号，落在此位元组所代表之功率范围的时间量 (fraction of time)，以范围 0 到 255 的刻度来表示，这些值的大小，因各功率准位所收到信号的时间量而定。^{【注】}

表 8-4: RPI 功率对映表

RPI 值	响应功率 (dbm)
0	少于 -87
1	-87~ -82
2	-81~ -77
3	-76~ -72
4	-71~ -67
5	-66~ -62
6	-61~ -57
7	-56 或更高

8.8.3.3 TPC Request 帧与 TPC Report 帧

TPC Request 与 TPC Report 帧如图 8-25 所示。两者均很简单，由频谱管理类型的 Action 帧所组成。每个帧包含其所对应的信息元素，如第四章所述。和其他帧一样，Dialog Token 字段用来对映要求与回应之用。

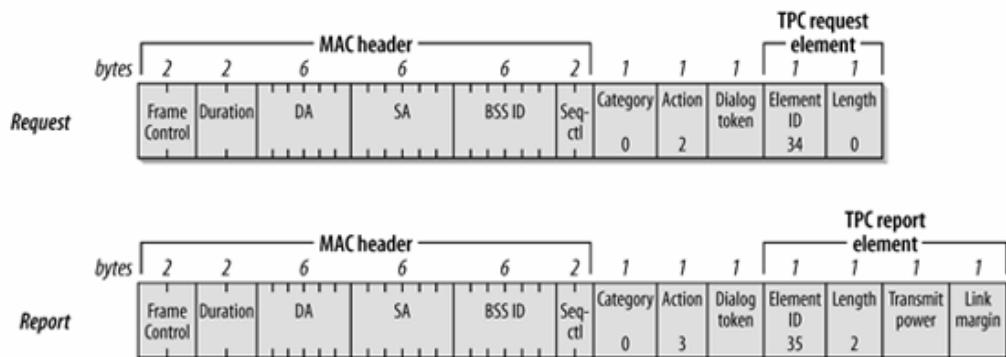


图 8-25: TPC Request 与 TPC Report 帧

8.8.3.4 Channel Switch Announcement 帧

必须变换频道时，就得通知网络上各个工作站，让它们得以准备切换到所指定的新频道。图 8-26 所显示的 Channel Switch Announcement (频道切换宣告) 帧，基本上是以 Action 帧包装第四章所描述的 Channel Switch Announcement 信息元素。因此，它们皆具备频道切换宣告元素的所有功能，用来指定网络即将切换至新频道的时间。

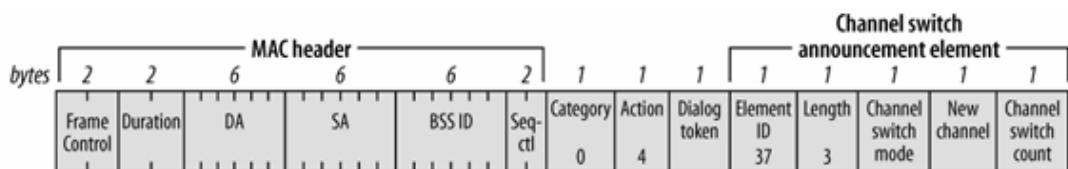


图 8-26: Channel Switch Announcement 帧

【注】虽然理论上每个位元组约值最高只到 255。不过标准中提到由于取近似值的缘故 (rounding effect)，有时候可能会累计到

第9 章 PCF 免竞争服务

为了支持需要近乎即时服务的应用，802.11 在标准中纳入了第二种协调功能，以提供

另外一种无线介质的访问方式。中枢协调功能(**point coordination function**, 简称 **PCF**) 可让 802.11 网络提供较为「公平」的介质访问机制。就某些方面而言，以 PCF 访问介质有点类似以权杖式 (**token-based**) 介质访问控制机制，由基站掌控权杖。本章主要在说明 PCF 的媒介访问 • PCF 帧的剖析图，以及电源管理与 PCF 的互动关系。

实际上，PCF 并未广泛使用。有一款家用介质服务器 (**media server**) 在产品中实现

了 PCF 功能，然而销售上并不理想。有些企业级产品之所以使用 PCF，是因为在控制无线介质的访问上，PCF 可以赋予基站更大的权限。就算某些蛮横的工作站使网络陷于无政府状态，PCF 也可以协助收回网络控制权。本章对某些读者来讲可能无关痛痒，如果目前使用的产品并不支持 PCF 功能，就没有必要阅读本章，除非各位对标准本身有兴趣。

9.1 以 PCF 提供免竞争访问

如果需要用到免竞争传输，便可运用 PCF。在 802.11 规格书中，PCF 属于选项功能 (**optional**)；实际产品不见得非得实现这项功能。IEEE 之所以设计 PCF，是为了让仅具备分散式协调功能 (**distributed coordination function**, 简称 **DCF**) 的工作站能够与中枢协调单元 (**point coordinator**) 交互运作，彼此相容。

免竞争服务 (**Contention-free service**) 并非随时供应。免竞争服务时间的长短，系由「中枢协调单元」负责仲裁，并与标准的分散式服务 (**DCF-base service**) 交相运用。免竞争期间 (**Contention-free period**) 的长短是可以设置的。802.11 规格书将【免竞争期间】描述为【近乎等时】 (**near isochronous**)，因为【免竞争期间】并非总是在预期时间内开始，如 9.1.3 节<免竞争期间的长短> (**Contention-Free PeriodDuration**) 所述。

【免竞争服务】采用中央访问控制机制，只有「中枢协调单元」可以访问介质。所谓「中枢协调单元」乃是基站所实作的一项特定功能。与之连接的工作站，只有在「中枢协调单元」允许的状况下，才可以传送数据。在某些方面，通过 PCF 进行【免竞争访问】有点类似权杖式 (**token-based**) 网络协议，只是「中枢协调单元」的轮询 (**polling**) 取代了权杖的地位。不过，802.11 模型的基础仍在。虽然访问系由某个中央单元所控管，但所有传送均须得到正面回应。

9.1.1 PCF 作业

图 9-1 显示了利用 PCF 进行传输的范例。使用 PCF 时，介质时间会被划分为免竞争期间 (**contention-free period**, 简称 **CFP**) 以及竞争期间 (**contention period**, 简称 **CP**)。免竞争期间的介质访问受到 PCF 的宰制，而竞争期间则是由 DCF 以及第 7 章所提到的规则所控管 • 竞争期间不能过短，至少要能够传送一个最大帧 (**maximum-size frame**) 及其回应。免竞争服务与竞争式服务以固定周期轮替，两者合称免竞争重覆间隔 (**contention-free repetition interval**)。

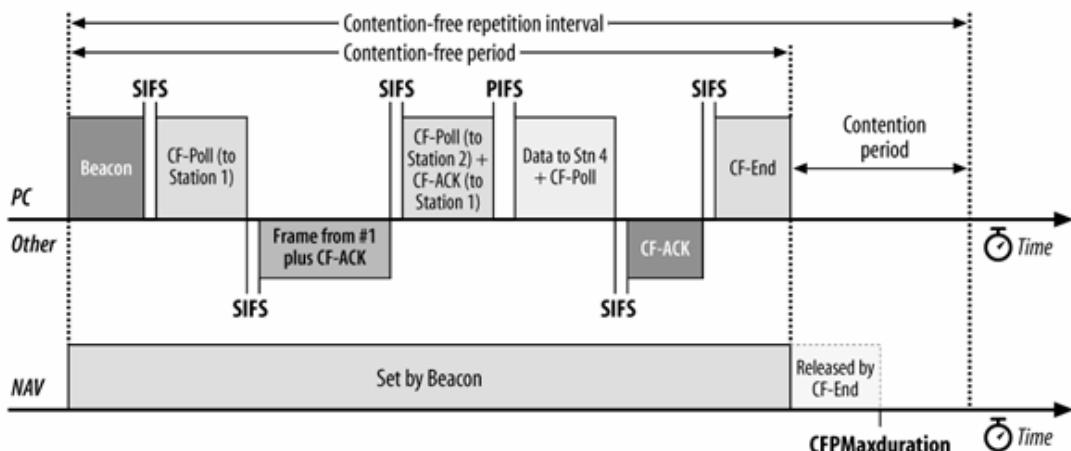


图 9-1: PCF 的运用

9.1.1.1 于免竞争期间保留介质使用权

免竞争期间一开始，基站就会送出一个 Beacon 帧。该 Beacon 帧中的 CFPMaxDuration（免竞争最大持续期间）栏位，用来标明免竞争期间最长持续多久。所有收到此 Beacon 的工作站，会将 NAV 设置为此时间值，并将 DCF 介质访问，排除在这段期间之外。

为了避免干扰，所有免竞争传输，会另外以 SIFS（短帧间隔）与 PIFS（PCF 帧间隔）加以区隔防护，这两者均较 DCF 帧间隔为短，因此在 DCF 期间，没有其他 DCF 工作站可以访问介质。

9.1.1.2 轮询表

基站接管无线介质之后，会根据轮询表(polling list)分别探询与之连接的工作站是否有数据待传。在免竞争期间，除非基站以轮询帧提出要求，否则工作站不得进行传输数据。免竞争轮询帧通常简写为 CF-Poll，一个 CF-Poll 帧代表授权传送一个帧，除非基站送出多次轮询要求，否则每次只能传送一个帧。

轮询表所列出者，乃是免竞争期间受邀传送帧的特权工作站。工作站一旦连上基站，就会被列在轮询表中，Association Request（连接要求）包含了一个栏位，用来标明该工作站能否在免竞争期间回覆轮询。

9.1.2 基站的传输

通常在免竞争期间，所有传输都只以 SIFS（短帧间隔）加以区隔。为了确保中枢协调单元掌握介质控制权，如果经过一段 PIFS（PCF 帧间隔）未得到回覆，就会继续探询表中下一部工作站。如图 9-1 所示，基站探询第二部工作站，但是没有得到回应，等候一段 PIFS（PCF 帧间隔）后，基站会继续探询表中第三部工作站，利用 PIES（PCF 帧间隔），基站得以确保本身持续掌控介质访问权。

在免竞争期间，基站也可以使用不同类型的帧。在此期间，中枢协调单元有四项主要任务。除了传送暂存帧以及接收工作站回应之类「正常的」任务，中枢协调单元可以征询轮询表中的工作站，允许它们传送帧；此外，中枢协调单元尚须传送管理帧。

在免竞争期间，时间十分宝贵，因此可以将正面回应讯息、轮询及数据传输组合在一起，以增进效率。当这三种功能结合成单一帧时，所得到的结果有点诡异。举例而言，单一帧就可以同时回应之前所收到的帧、征询其他工作站是否有暂存数据以及送出本身的数据给轮询表所列的工作站。

在免竞争期间，可以使用下列帧：

- **Data** (数据)

当基站要送出一个帧给工作站，但是不必回应之前所传送的讯息时。就会使用标准的数据帧，标准的数据帧并不会征询对方是否有数据待传，因此不允许接收端传送任何数据。免竞争期间所使用的纯数据 (**Data-Only**) 帧和竞争期间所使用的数据帧完全相同。

- **CF-Ack** (免竞争期间的回应)

如果没有数据待传，工作站会以此帧回应之前所收到的帧。免竞争期间的回应讯息比标准控制帧的回应讯息长，因此实际上可能不会使用此帧。

- **CF-Poll** (免竞争期间的轮询)

CF-Poll 帧是由基站发送给行动式工作站的，用来赋予行动式工作站传送一个暂存帧的权力。只有当基站没有数据要传给行动式工作站时，才会使用这个帧。如果尚有数据要传给行动工作站，基站会改用 **Data+CF-Poll** 帧类型。

- **Data+CF-Ack**

此帧结合了数据传送以及回应讯息。数据是针对帧接收者发送的；回应讯息则是针对之前传送的帧，通常和数据接收者无关。

- **Data+CF-Poll**

基站使用此帧传送数据给某个行动式工作站，然后要求对方传送一个待传帧。**Data+CF-Poll** 只能够在免竞争期间由基站发送。

- **CF-ACK+CF-Poll**

此帧除了会回应最近基站从某部个工作站所收到的帧，同时会要求轮询表中下一个工作站传送一个暂存帧，虽然所回应的对象可能是任何一个连上此基站的行动式工作站。

- **Data+CF-ACK+CF-Poll**

此帧将数据传送轮询功能以及回应讯息结合成单一帧，为的是达到最高效率。

- **CF-End**

此帧用来终止免竞争期间，以及将介质控制权交回 DCF 竞争机制。

- **CF-End+CF-Ack**

此帧与 **CF-End** 帧相同，不过它同时回应了之前所收到的数据帧。

- **任何管理帧**

802.11 标准并未限制免竞争期间不能使用哪些管理帧。任何特殊类型的帧只要合乎传送规则，基站都会加以传送。

9.1.3 免竞争期间的长短

CP（竞争期间）再短，至少也要能传送一个最大的帧，以及得到相对的回应。不过，竞争式服务也有可能超出竞争期间。若竞争式服务逾越 CFP（免竞争期间）预定开始时间，CFP 就会被压缩，如图 9-2 所示。

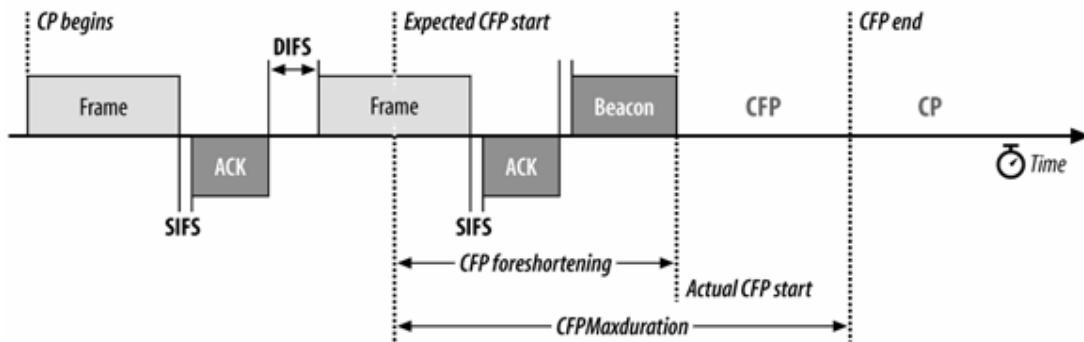


图 9-2: Data+CF-Ack 与 Data+CF-Poll 的用法

如果 CFP（免竞争期间）被压缩，在以 Beacon（信标）讯息宣告免竞争作业开始之前，还是允许正在进行中的帧交换完成现有作业。CFP 被压缩多少时间，取决于延迟多久。免竞争服务结束时间，不能晚于预定启始点之后所允许的最长时间，该时点称为信标预定传送时间(Target Beacon Transmission Time, 简称 TBTT)

中枢协调单元（point coordinator）也可以送出一个 CF-End 帧，在超过最大持续期间（maximum duration）之前中止免竞争期间（CFP）。它可以根据轮询表的长短。流量的负载或其他基站认为重要的因素，做出中止决定。实际产品有时候可以选择性地使用 PCF（中枢协调功能）来交换特定的帧，启用免竞争服务后开始进行传输，然后予以中止。

9.2 PCF 帧的封装细节

某些类型的帧只能在免竞争期间（CFP）使用。数据、回应与输询帧可以组合成单一帧。本节主要在描述何时使用哪种组合帧，以及在帧交换过程中，不同功能之间如何互动。换言之，免竞争帧在单一帧里结合了数种功能。

- Data+CF-Ack

Data+CF-Ack 帧结合了两种不同的功能以增进传输效率。此帧除了内含所要传送的数据，也同时回应了 SIFS（短帧间隔）之前所收到的数据。通常，此帧内含的数据与回应讯息是分别针对两部不同的工作站。图 9-3 中，工作站回覆之前帧的 CF-ACK（免竞争回应）讯息，结合了打算传给基站的数据，不过数据本身可能是要传给 802.11 网络中其他的工作站。

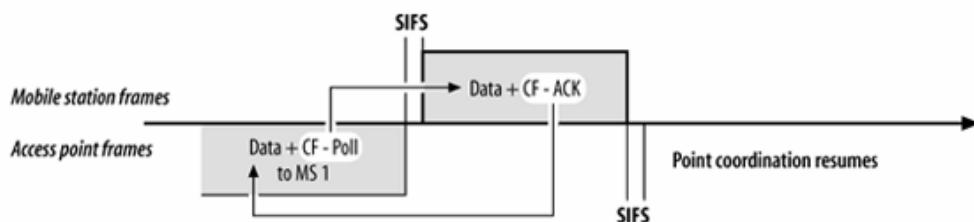


图 9-3: Data+CF-Ack 的用法

此帧只用于 **infrastructure**（基础型）网络，因为它只能在免竞争期间传送。基站或行动式工作站均可发送此类型的帧。不过在免竞争期间，基站必须负责轮询，因此似乎不太可能传送此类型的帧，因为其中并未包含输询（poll）。

- **Data+CF-Poll**

在免竞争期间，基站可以在 **infrastructure** 网络中使用 **Data+CF-Poll** 帧，当基站不需要回应任何帧时，就会以 **Data+CF-Poll** 传送数据给接收端，同时允许对方传送一个暂存帧以做为回应。帧主体所包含的数据必须是给轮询的接收者；这两种功能不能「分别」针对不同的接收者。图 9-3 中，基站使用 **Data+CF-Poll** 帧传送一个数据帧给工作站，同时要求对方（传回一个暂存帧以做为）回应。

- **Data+CF-Ack+CF-Poll**

在免竞争期间，基站可在 **infrastructure** 网络中使用 **Data+CF-Ack+CF-Poll** 帧。如果基站必须同时传送数据、回应帧以及探询轮询表中的工作站，则可以将这些功能组合在一个帧中。图 9-4 显示了 **Data+CF-Ack+CF-Poll** 的用法，如同 **Data+CF-Ack**，**Data+CF-Ack+CF-Poll** 中的组件通常是对不同的工作站。数据传输与轮询必须针对相同的工作站，而回应讯息则是针对前次的数据传输。图 9-4 中，第一部行动式工作站（MS1）传送了一个 **Data+CF-Ack** 帧。**Data** 部分必须送至基站，不过 **CF-Ack** 却是回应之前基站所传送的数据帧。（本图并未显示该帧）。依轮询表，基站随后探询第二部行动式工作站（MS2）是否有暂存帧。然而，此时基站必须回应来自 MS1 的数据帧，因此基站在帧中加入了 **CF-Ack** 讯息。当时基站正好有数据要传送，所以将这三者结合成一个多用途的帧。**Data** 与 **CF-Poll** 组件是给帧的接收者，而 **CF-Ack** 则是给前一个帧的传送者。MS1 必须聆听基站所发出的帧，才有办法接收到 该回应。



图 9-4: **Data+CF-Ack+CF-Poll** 的用法

- **CF-Ack**（不含数据）

如果只需要回应讯息，可以传送一个仅含标头及 **CF-Ack** 功能的帧。图 9-4 中，如果 MS2 没有数据待传，就仅会以一个 **CF-Ack** 帧做为回应。

- **CF-Poll**（不含数据）

CF-Poll 也可以独自传送。当然，只有基站才会使用这项功能、因此 **CF-Poll** 帧只有在免竞争期间，才会由 **infrastructure** 网络中的基站传送。如果基站已经没有其他暂存数据要传给接收者，而且不必回应之前所收到的帧，就只会传送 **CF-Poll**。一种常见的原因是，基站传送了一个 **CF-Poll** 进行轮询，但工作站方面并无数据亦无回应，这时候便不需要回应讯息。如果基站没有数据要传给轮询表中的下一个工作站，就只会传出 **CF-Poll**，如图 9-5 所示。

图 9-5 中，基站尝试传送数据给 MS1，不过并未收到回覆。等候一段 PIFS (PCF 信道间间隔) 后，基站便开始探询轮询表中下一个项目 MS2。由于没有来自 MS1 的帧需要回应，而且基站也没有数据送给 MS2，因此可以只发送 CF-Poll 给 MS2，允许对方传送暂存数据。

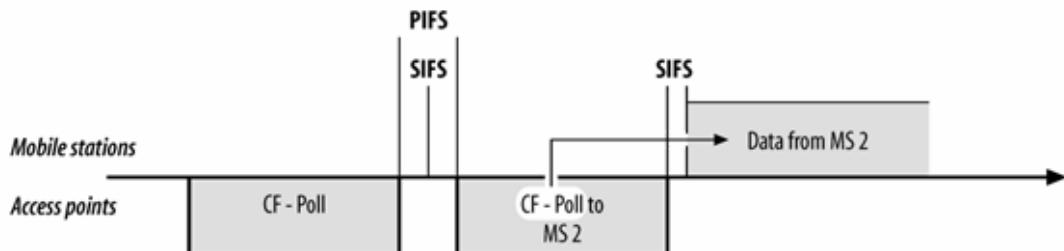


图 9-5: CF-Poll 帧的用法

CF-Ask+CF-Poll (不含数据)

最后一种数据帧类型为 CF-Ack+CF-Poll，也是由基站发送的。和所有 CF-Poll 帧一样，此帧只用于免竞争期间，而且只能给基站使用。其中包含了回应以及轮询功能，但是不含任何数据。图 9-6 显示了此帧的用法。

此处的情况和之前的设置稍有不同。图 9-6 中，MS1 回复了一个帧，而没有让基站等候逾时。当基站取得介质控制权，就会以 CF-Ack+CF-Poll 回应之前 MS1 所传送的帧，同时通知 MS2，允许它传送暂存数据。

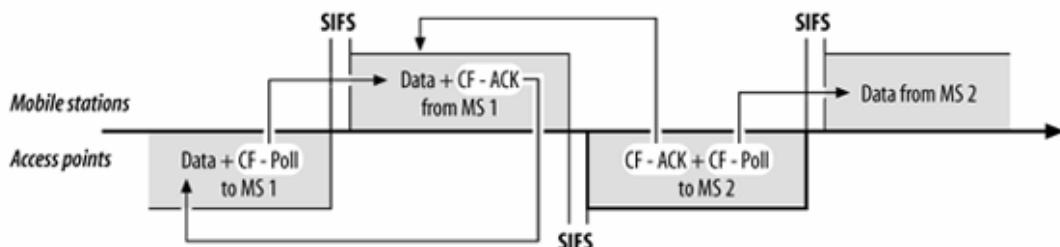


图 9-6: CF-Ack+CF-Poll 帧的用法

9.2.1 免竞争期间结束 (CF-End)

免竞争期间结束时，基站会送出一个 CF-End 帧，让工作站脱离 PCF 访问规则，然后开始采用竞争式服务。CF-End 帧的格式如图 9-7 所示。CF-End 帧的 MAC 标头，系由四个栏位组成：

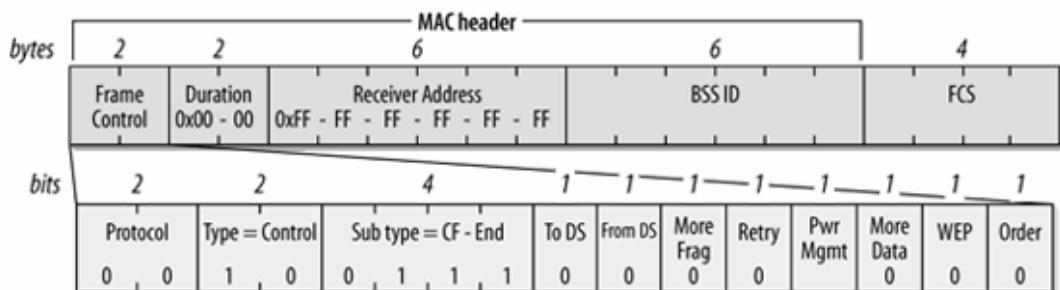


图 9-7: CF-End 帧

Frame Control (帧控制)

帧的次类型 (subtype) 设置为 1110，代表 CF-End 帧。

Duration (持续时闲)

CF-End 用来宣告免竞争期间的结束，因此不须延长虚拟载波检测时间。 Duration 会被设置为 0。收到 CF-End 帧的工作站，会将虚拟载波检测截短，以便重新启用竞争式访问。

第一个地址栏位: Receiver Address (接收端地址)

CF-End 攸关所有行动式工作站的作业，因此接收端地址会被设为广播地址。

第二个地址栏位: BSSID

基站会将 CF-End 发布给其 BBS 当中与之连接的所有工作站，因此第二个地址栏位必须填入 BSSID。在 infrastructure 网络中，BSSID 乃是基站的无线界面地址，因此 BSSID 也就是传送端地址。

9.2.2 CF-End+CF-Ack

当免竞争期间结束，基站会送出一个 CF-End 帧，让工作站脱离 PCF 访问规则，同时以 DCF 开始进行竞争式服务。如果基站同时必须回应之前所收到的数据，则可用 CF-End+CF-Ack 帧，于结束免竞争期间的同时顺便加以回应。CF-End+CF-Ack 帧的格式，如图 9-8 所示。CF-End+CF-Ack 帧的 MAC 标头，系由四个栏位组成：

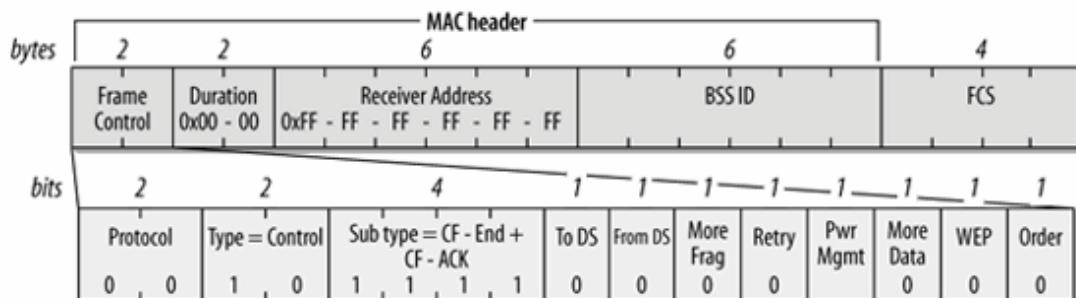


图 9-8: CF-End+CF-Ack 帧

Frame Control (帧控制)

帧的次类型 (subtype) 设置为 1111，代表 CF-End+CF-Ack 帧。

Duration (持续时间)

CF-End+CF-Ack 用来宣告免竞争期间的结束，因此不须延长虚拟载波检测时间

Duration 栏位会被设为 0。

第一个地址栏位: Receiver Address (接收端地址)

CF-End+CF-Ack 攸关所有行动式工作站的作业，因此接收端地址会被设为广播地址。

第二个地址栏位: BSSID

基站会将 CF-End+CF-Ack 发布给其 BBS 当中与之连接的所有工作站，因此第二个地址栏位必须填入 BSSID‘在 infrastructure 网络中，BSSID 乃是基站的无线界面地址，因此 BSSID 也就是传送端地址。’

9.2.2.1 CF 参数组合

支持免竞争作业的基站，可能会在帧中使用 CF 参数组合 (CF Parameter Set) 信息元素，如图 9-9 所示。CF 参数组合元素若被包含在 Beacon 帧中，可通知所有行动式工作站，开始进行免竞争作业。这些参数组合元素若被包含在 ProbeResponse 帧中，则可以让工作站明白该 BSS 支持哪些免竞争选项。CF 参数组合信息元素，系由四个栏位组成：

CFP Count (CFP 言十数器)

此栏位占用一个位元组，用以告知下个免竞争期间开始前，尚会传送几个 DTIM 帧。如果为 0，那么目前的帧代表免竞争服务的开始。

CFP Period (CFP 周期)

此栏位亦占用一个位元组，用来指示两个免竞争期间，相距多少个 DTIM 间隔。

CFP MaxDuration

这个值是以时间单位(time units，简称 TUs) 做为计量单位，用来指示免竞争期间最长可以延续多久时间。行动式工作站会以这个值来设置 NAA，表示整个免竞争期间，介质均处于忙碌状态。

CFP DurRemaining

这个值也是以 TUs 做为计量单位，用来指示目前的免竞争期间尚余多久时间。在整个免竞争期间，行动式工作站会藉助这个数值来更新 NAV。当使用 DCF 服务时，这个值会被设为 0。

bytes	1	1	1	1	2	2
	Element ID 4	Length 6	CFP Count	CFP Period	CFP MaxDuration	CFP DurRemaining

图 9-9: CF 参数组合信息元素

9.3 电源管理与 PCF

免竞争期间节省电源的方式与竞争期间类似，不过有些小小的例外。两者主要的差异为，免竞争期间的帧传递必须遵循 PCF 规则，因此只有在基站轮询时，才可以传送暂存帧。不支持 PCF 作业的工作站，必须等到竞争式服务重新启用时，才可以取回暂存帧。

在免竞争期间，不允许列于轮询表中的工作站进入休眠状态。基站使用其「中枢协调功能」(PCF) 时，可能在任何时间探询任何一部工作站。在免竞争期间，传送给工作站的帧无须暂存，因为这些列名于轮询表中的工作站，不可能处于休眠状态。

不论是在免竞争或在竞争式服务中。帧暂存的方式都一样。基站负责维护每部工作站的省电状态，并且为处于低电源模式的工作站暂存帧。如果与之连接的工作站处于低电源模式，也会为其保留广播与组播帧。

除了与免竞争服务相关的暂存状态，基站也会针对试图探询的工作站，设置 TIM 中几个位元旗标。之所以要设置这些位元旗标，与如何传递暂存帧有关。和竞争式服务一样，广播与组播帧的传送，系由 DTIM 帧所触发。如果传送广播与组播帧所需时间超过 Beacon interval (信标间隔)，基站只会传输相当于 Beacon interval 的时间，之后就会予以中止。由于尚有残留帧，因此基站会继续保留与 AID 0 相应的位元旗标。

传送了暂存的广播与组播帧之后，基站会重新检视一次 AID (连接识别码) 列表，只要其 TIM 位元旗标未被取消，就会继续传送残馀数据。帧的传送完全依循 PCF 规则，因此传送前不必加上缓冲时间。轮询表中的工作站会被加到 TIM 中，因此会参与整个过程。虽然可以传送多个暂存帧，实际状况得视提供免竞争服务的基站如何实作，行动式工作站只有在得到基站允许时，才可以进行传输。接收完所有帧之前，工作站不能进入休眠状态，除非 More Data (尚有数据) 位元为 0，代表已无后续数据。当一部工作站空闲下来进入休眠状态，就会沉睡到下一次 DTIM 传送时。DTIM 帧用来宣告免竞争期间开始，因此实际具备 PCF 功能的工作站，必须往每次 DTIM 传送之前醒来。

在免竞争期间，如果工作站自低电源模式醒来，所有为之暂存的帧，都会被转移给中枢协调功能，以便进行传送，数据移转后并不会立即传送，不过如果中枢协调功能允许，基站可以将这些帧置于伫列 (queue) 准备传送。

第10 章 物理层概观

只要呆呆伫立着，每个女人都可以魅力非凡。

— Hedy Lamarr

通讯协议的分层概念（protocol layering），让我们得以针对协议堆叠（protocol stack）的各个部分进行研究、实验或改良。802.11 架构的第二个要件为物理层（physical layer），通常简写为 PHY。本章主要在介绍无线物理层所涵盖的主题与常见的技术，以及描述所有无线物理层的共同问题；之后会就 802.11 所包含的标准物理层，分别加以详细说明。

10.1 物理层架构

物理层被分成两个附属层（sublayer）：物理层收敛程序（Physical Layer Convergence Procedure，简称 PLCP）附属层，以及实际搭配介质（Physical Medium Dependent，简称 PMD）附属层。PLCP（图 10-1）的功能在于结合来自 MAC 的帧与空中所传输的无线电波。PLCP 同时会为帧加上自己的标头。通常，帧中会包含同步信号（preamble）。以协助接收数据的同步作业。不过，每种调制方式所采用的同步信号均不相同，因此 PLCP 会为准备传送的所有帧加上自己的标头。接著由 PMD 负责将 PLCP 所传来的每个位元，利用天线传送至空中。物理层还包含了频道净空评估（clear channel assessment，简称 CCA）功能，用来指示 MAC 是否检测到了信号。

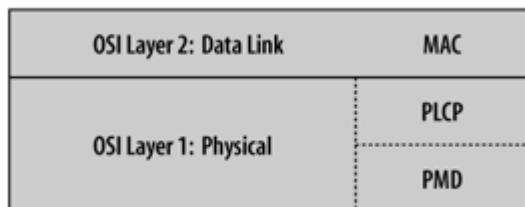


图 10-1：物理层逻辑架构

10.2 无线链路

802.11 最初的版本颁布于 1997 年，其中包含了三种物理层标准：

- . 跳频（Frequency-hopping 简称 FH）展频（spread-spectrum）无线电波物理层（radio PHY）
 - . 直接序列（Direct-sequence，简称 DS）展频无线电波物理层
 - . 红外线（Infrared light，简称 IR）物理层

后来，进一步开发了三种以无线电波技术为基础的物理层：

- . 802.11a：正交分频多工（Orthogonal Frequency Division Multiplexing，简称 OFDM）物理层

 . 802.11b：高速直接序列（High-Rate Direct Sequence，简称 HR/DS 或 HR/DSSS）物理层。

- . 802.11g：延伸速率物理层（Extended Rate PHY，简称 ERP）
- . 未来的 802.11n，俗称多进多出（MIMO）或高传输量（High-Throughput）物理层。

本书只会深入探讨其中四种以无线电波为基础的物理层；由于并未广泛使用，因此红外线物理层会略过不谈。就我所知，红外线物理层从来不曾运用在任何商业化的产品中。

10.2.1 使用执照与管制

以往无线通讯的做法，是将承载信息的信号限制在某个较窄频段，然后尽可能加大信号功率（只要合法即可）。在频段中，杂讯不可避免会造成某种程度的失真。在有杂讯的情况下，传送信号必须采取强制手段一只要能确保信号的功率远大于杂讯即可。

IR 物理层

802.11 包含了红外线 (IR) 物理层的规格。使用红外线代替无线电波，似乎有许多优点。红外线连接埠比电波收发器来得便宜—实际上，价格低到每部膝上型电脑都将红外线连接埠列为标准配备。

IR 相当能够抗拒无线电频率或射 *RF* (radio frequency, 简称 RF) 的干扰，因为无线电波运作在完全不同的频率上。这带来第二项优点：IR 不受管制。产品开发人员无须费神探究如何让产品符合世界上许多管制机构的规范。

和 802.11 故关的安全考量，大多围绕在未经授权的使用者可能盗连网络的威胁，由于光线只能够局限在某个会议室或办公室，只要将门带上即可。以红外线为塞础的局域网络，具备弹性与移动性等优点，而且安全顾虑较小。不过这并非没有代价，尚于红外线局域网络仰赖的是随处四散的光线，因此传输距离较短。

不过，以上纯属学术上的讨论。实际上并没有红外线物理层的相关产品。膝上型电脑配备的红外线埠，其所符合的标准，是由红外线数据协会 (*Infrared Data Association*, 简称 IrDA) 而非 802.11 所制定，由于无线电波可以长距离传输，而且可以穿透固体，因此弹性较大，移动性也较高。弹性与移动性既然是一般所以采用 802.11 的最大驱力，所以就算开发出红外线物理层的相关产品，也无法与之相提并论。

在古典的通讯模型中，如何避免干扰其实是属于政治（而非物理）层面的议题，对于窄频高功率的传输，管制当局必须制定一套规则，以规范如何使用 RF 频谱。在美国，由联邦通讯委员会 (*Federal Communications Commission*, 简称 FCC) 负责管制 RF 频谱的使用。美洲其他国家，也采用 FCC 所制定的一些规范。在欧洲，频谱配置是由欧洲无线电通讯管理局 (*European Radiocommunications Office*, 简称 ERO) 以及欧洲电信标准协会 (*European Telecommunications Standards Institute*, 简称 ETSI) 负责。在日本，无线电的使用受总务省 (*Ministry of Internal Communications*, 简称 MIC) 管制规范。全球“一致” (*harmonization*) 的规范作业，则由国际电信联盟 (*International Telecommunications Union*, 简称 ITU) 管辖。ITU 的建议书得到许多国家的管制单位所采用。

通常，要以特定频率传送电波，必须事先取得使用执照。使用执照限制可以使用哪些频率与传输功率，以及可以传送到哪些地区。举例而言，无线广播电台必须取得 FCC 的使用执照。同样地，移动电话网络也必须取得执照，方能在某个特定地区与市场使用无线频谱。使用执照可

以保证特定频率的独家使用权。当信号受到干扰，执照持有者可以要求管制当局介入，通常是通过关闭干扰源来解决问题。故意干扰是一种侵权行为，可能遭受刑事或民事上的处罚。

10.2.1.1 频率配置与无须使用执照的频段

无线频谱可以被划分为许多频段，每个频段针对特定的使用目的。每个频段定义了特定应用可以使用的频率。其中，防护频段（guard band）用来防止传送信号的溢散影响到其他频段。

有些频段系保留给不必使用执照的用途・举例而言，微波炉使用 2.45GHz 频段，在

自己家里使用微波炉还得获得 FCC 批准并无太大的意义。为了让厂商得以在消费性市场上开发家用产品，FCC（以及其他各国类似的管理机构）指定了一些特定频段给「产业、科学与医疗」设备使用。这些频段通常称为 ISM 频段，2.4-GHz 频段在全世界均可不经授权使用。【注】不过，无须使用执照与无须销售执照不同，建构、生产与设计 802.11 设备不必取得执照；在美国所有合法销售的 802.11 网卡，必须取得一个 FCC 识别码。在申请过程中，厂商必须提供相当多的信息给 FCC。这些信息主要是做为公开纪录之用，各位可通过 FCC 识别码上网搜寻。

使用 ISM 频段的设备，通常不必取得使用执照，只要这些设备不会散发过量的辐射。微波炉属高功率设备，不过通常会加上层层防护，以防止电磁辐射。随著新通讯技术的发展，这些不必使用执照的频段，近三年来相当受到关注。使用者无须通过执照申请程序，即可使用运作在 ISM 频段的设备，厂商也无须费神熟悉授权的程序与要求。写作本书当时，2.4-GHz ISM 频段已经充斥了不少新开发的通讯系统：

各式 802.11 系统（跳频、直接序列与 OFDM 系统）。

Bluetooth（蓝芽），一种短距离的无线通讯协议，由 Ericsson 所领军的产业联盟所开发。

水对微波的吸收峰 (Absorption Peak) 并不存在

据说微波炉之所以采用 2.45GHz，是因为水分子在此频段特别活跃。有时候，这种说法甚至被当成 802.11 无法长距离传输的理尚。如果下雨或者气候十分潮湿时，微波信号会因为大气中的水份蒸发而严重衰减 (attenuate)，那么 802.11 能不适合用于长距离传输。

微波中存在能够让水分子特别活跃的频率，这种说法纯属神话。若是这样，水份必然会吸收相当多的微波能量。如果这些能量被水有效吸收，微波炉说无法加热任何东西，因为都会被食物表面的水份给吸收殆尽，既然表面的水份会吸收掉所有能源。食物中央就无法加热变熟。所谓吸收峰 (absorption peak)。同时意味著大气中的水份蒸腾会中断卫星通讯，不过情况并非如此。NASA 的参考文献 1108(02) 〈Propagation Effects on Satellite Systems at Frequencies Below 10 GHz〉，论及大气效应预期会造成多少信号的损失，结论是通常频率在 10 GHz 以上的信号损失较为严重・举例而言，最容易被水份吸收的微波频率为 22.2 GHz。

微波炉的运作方式，并不是将水分子堆至激态 (excited state)，而是利用水分子非比寻常的强偶极矩 (strong dipole moment)。虽然本身属电中性，偶极矩使得水分子就像是两端各带细微正负电荷的小棒子・在微波炉中，不断改变的电磁场会来回扭转水分子。来回扭转之下，连带增加了整个分子的动能，水分子也因此更为活跃，但并未改变水分子的激态或者成份。

- 由一些无线电话（cordless phone）厂商所生产的展频无线电话。
- X10，家庭自动化设备所使用的一种协议，可以通过 ISM 频段进行影像（video）传输。

遗憾的是，「免照」（unlicensed）不尽然意味设备可以「与其他设备融洽相处」（plays well with others），所有不必使用执照的设备，都必须遵守传输功率的限制。既然没有编码或调制上的管制，因此不同厂商使用频谱的方式，可能彼此不相容。站在使用者的角度，解决这个问题的惟一方式，就是从中择一使用。因为设备不必取得执照，因此管理当局不会介入。

10.2.1.2 其他不必使用执照的频段

其他无须使用执照的频谱范围位于 5-GHz，美国是第一个允许在 5 GHz 频段使用免照设备的国家，不过日本与欧洲也随后跟进。【注】以下全世界各国允许使用的一系列频带：

4.92-4.98 GHz (日本)
5.04-5.08 GHz (日本)
5.15-5.25 GHz (美国・日本)
5.25-5.35GHz (美国)
5.47-5725 GHz (美国、欧洲)
5.725-5.825 GHz (美国)

除了频宽与辐射功率，使用 5 GHz 频段的设备无须遵循其他限制，相较于美国或欧洲，日本规范使用较窄的频宽。

10.2.2 展频

展频（spread-spectrum）技术是使用 ISM 频段传送数据的基础。传统无线电通讯的焦点在于，如何尽可能地在最窄的频段中塞入最多信号。展频的运作原理，是利用数学函数将信号功率分散至较大的频率范围。只要在接收端进行反向作业，就可以将这些信号重组为窄频信号。更重要的是，所有窄频杂讯都会被过滤掉，因此信号可以清楚重现。

对于无须使用执照的设备而言，使用展频技术是必要的。有时候，这是因为管制当局的要求；有时候，这是符合管制要求的惟一方式。举例而言，FCC 要求使用 ISM 频段的设备必须使用展频传输，并在一些参数上加以限制。

对传统的窄频接收器而言，传输信号展开至较宽频段之后，就和杂讯没有两样。有些展频设备厂商宣称展频可以增加安全性，因为窄频接收器无法拾起完整信号。问题是，将之更换为标准展频接收器只是举手之劳，因此必须强制使用其他安全功能。

这并不意味著，展频是可以解决干扰问题的「万灵丹」（magic bullet）。展频设备甚至可能与其他通讯系统彼此干扰；传统的窄频 RF 设备亦然。虽然展频在处理干扰上比其他调制技术

高明，但问题并未因此而消失。当更多 RF 设备（不论属于展频与否）占据无线网络的覆盖范围，杂讯就会增多，讯噪比（signal-to-noise ratio）就会因而降低，可靠的通讯范围也会跟著缩小。

为了将（无须使用执照的）设备间干扰降至最少，FCC 限制了展频传输所能使用的功率，法律上明文限制发射器的输出功率（output power）为一瓦（watt），有效辐射功率（effective radiated power，简称 ERP）为四瓦。有效辐射功率四瓦，对增益 gain 为 6 dB【编注： $10\log 4$ 】的天线而言，相当于一瓦的输出功率，对增益为 10dB【编注： $10\log 10$ 】的天线而言，则相当于 400 毫瓦的输出功率。【注】PC 无线网卡的发射器与天线显然符合此一限制，就算使用商用天线，也不会比较接近。不过，若使用外部的放大器或增益较高的天线，PC 无线网卡即可涵盖较大的区域。对于这个问题法律并未明文禁止，不过可以确定的是，无论如何还是必须符合 FCC 的功率标准。

无意间发明的展频

奥地利出生的女演员 Hedy Lamarr (海蒂拉吗) 于 1940 年代 X77 期取得了展频专利。不过，她之所以举世闻名，却是因为其他缘故除了在一部名为 Ecstasy 的捷克电影中破天荒全裸演出，好莱坞名人 Louis Mayer (路易士梅耶) 更称她为「全世界最美的女人」。她同时也是蝙蝠侠漫画【猫女】一角的灵感来源。

在德国纳粹入侵之前，Hedy Lamarr 原本是一位奥地利军火商的妻子。她认识到以无线电波遥控鱼雷是当时军火制造商的主要研究领域。遗憾的是，窄频无线电通讯容易遭受人为干扰，从而抵销无线制导武器的优劣。她从这些讨论中得到一种想法，可以使用一种复杂但预先设置好的跳频样式，随时改变控制信号的频率。只要在某个频率稍作停留，就可能遭到干扰。因此频率的变换速度必须够快，才可以避免信号被完全阻绝 Lamarr 完成所有细部设计，但不包括如何精确地控制跳频。

移居美国之后，Hedy Lamarr 遇到了 George Antheil (乔治安瑟)。他是一位美国的前卫作曲家，作品充满不合谐风格（dissonant style），人称「音乐顽童」（bad boy of music）。在著名的 Ballet Mécanique (机械芭蕾) 中，他在一处控制 16 部自动弹奏的钢琴，身旁还安排一些人毫无节制地制造噪音。要演奏这个作品，必须能够精确掌控每项元素的时间，这正是 Lamarr 在控制跳频样式时所遭遇的困难。1942 年，他们共同取得该项美国专利，编号为

2,292,387。该专利于 1959 年失效，没有为他们赚进半毛钱。这个贡献一直默默无闻，因为专利上所列的是她结婚当时所使用的名字 Hedy Kiesler Markey。无线局域网络市场在 1990 年末期逐渐浮现之后，她的发明也被重新发掘出来，并被广之现为奠定当代电信基础的先锋之作。

在古巴飞弹危机期间，美国首次将跳频技术应用在封锁古巴的舰队之上。电子展频技术具备商业可行性，已经是多年之后的事。如今，展频技术不但应用在无线与移动电话，也运用在宽频无线局域网络设备，以及使用 ISM 频段的每一种设备 n Hedy Lamarr 于 2000 年初去世，而无线局域网络正好在该年得到市场主流的一青睐。

10.2.2.1 展频的类型

802.11 所采用的无线电波物理层，使用了三种不同的展频技术：

跳频（Frequency hopping，简称 FH 或 FHSS）

跳频系统系以某种随机样式在频率间不断跳换，每个子频道只作瞬间的传输。2-Mbps FH PHY 规范于规格书第 14 款。

直接序列 (Direct sequence, 简称 DS 或 DSSS)

直接序列系统利用数学编码函数将功率分散于较宽的频段。标准中规范了两种直接序列物理层 • 最初的规格书在第 1 款所提出的是 2-Mbps PHY 标准，而 802.11b 则加入了第 18 款 HR/DSSS PHY。

正交分频多工(Orthogonal Frequency Division Multiplexing, 简称 OFDM)

OFDM 将可用频道划分为一些子频道，然后对每个子频道所要传送的部分信号进行平行编码 • 这种技术类似某些 DSL 数据机所使用的离散多音频调制 (Discrete Multi-Tone, 简称 DMT) 技术。802.11a 所加入的第 17 款，用来规范 OFDM PHY。而 802.11g 所增加的第 18 款，则是用来规范 ERP PHY。基本上 ERP PHY 跟 OPDM PHY 没有两样，只不过运作在较低的频率。

这三者中，以跳频系统的价钱最为低廉，虽然跳频的控制必须精确计时，但不必经过复杂的信号处理，即可从无线电波信号中取出位元串流。直接序列系统需要较复杂的信号处理，亦即需要消耗更多的电力以及特殊的硬件。直接序列技术所能使用的数据传输率，也较跳频系统为高。

10.3 RF 传播与 802.11

在固定式网络中，信号只能在缆线所限定的路径中移动，因此网络工程师不必知道电子信号传播的物理特性。只要依循一些规则计算出每个网段所允许的最大缆线长度，就很少会出现什么问题。RF 传播可没那么简单。

10.3.1 信号接收与效能

空气中到处都是随机的电磁波，只要将收音机调整到没有电台的频率就可以轻易听见，无线电通讯必须从背景的杂讯中分辨出信号。一旦接收条件变差，信号就愈容易被杂讯淹没，效能绝大部分取决于讯噪比 (signal-to-noise ratio • 简称 SNR) 这个决定性因素。图 10-2 以信号峰值 (the peak of the signal) 与杂讯基准 (noise floor) 之间的差异值来表示讯噪比。

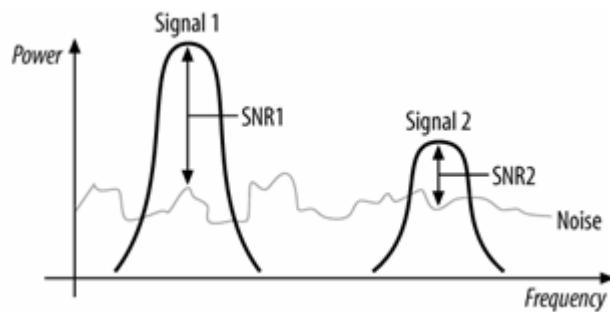


图 10-2: 讯噪比与杂讯基准

信号强度十分重要，但不代表一切。在充满杂讯的环境中，反而难以拾取过强的信号，在某些状况下，可以通过加大功率做为杂讯基准太高的补偿。免照网络很难采用提高功率的手段，

因为受到严格的管制所限制。因此，业界通常将比较多的心力放在如何降低杂讯，亦即在解读电波信号之前，尽量避免产生额外的杂讯。

10.3.1.1 Shannon 极限

值得注意的是，无线电频道能够承载多少数据，理论上并没有极限。1948 年，贝尔实验室的研究员 Claude Shannon 提出 Shannon-Hartley 定理，用来证明与计算传输频道的性能（capacity）^① 此一定理陈述了传输频道性能在数理上的极限，一般通称此定理为 Shannon 极限或 Shannon 性能。原始的 Shannon 定理把最大性能 C（每秒可传输位元数）定义成频宽 W（以 Hertz 表示）与信号功率之绝对讯噪比的函数。如果以分贝为量测单位，只要在等式中以分贝取代功率比即可。

$$C = W \log_2 (1 + S/N) \quad (\text{S/N 以功率比表示})$$

$$C = W \log_2 (1 + 10^{(0.1 \cdot \text{SNR})}) \quad (\text{SNR 以分贝表示})$$

图 10-3 显示了 Shannon 极限与讯噪比的函数关系。Shannon 定理反映出无限位元率 (unlimited bit rate) 在理论上的实际状况。要达到无限位元率，在设计编码方式时可以任意取用数量够大的信号位准来区别位元，不过这些邻近信号位准间的细微差异，将被杂讯所吞蚀。802.11 物理层设计人员的主要目的之一，就是设计出尽可能趋近 Shannon 极限的编码率。

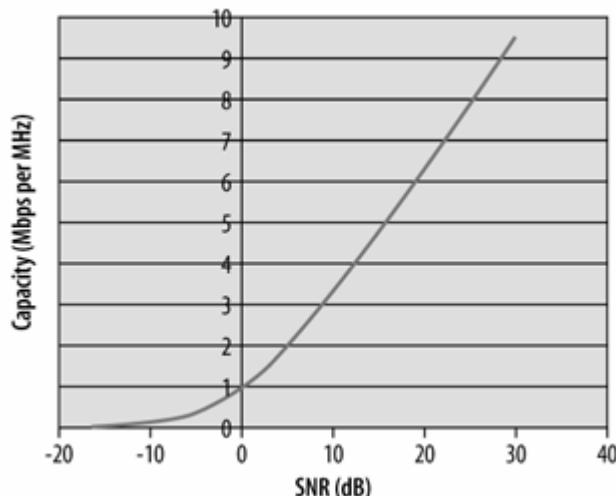


图 10-3: Shannon 极限与讯噪比 (SNR) 的关系

此外，Shannon 定理可以用来推算欲达特定数据率的理论最小讯噪比。上述方程序可求解出讯噪比：

$$S/N = 2^*(C/W) - 1$$

$$\text{SNR} = 10 \cdot \log_{10}(2^*(C/W) - 1)$$

举一个 802.11 a 的例子。以频宽为 20 MHz 的单一频道传送信号，数据率最高可达 54Mbps，代入上述方程序，可以求出讯噪比为 7.4 dB，远低于市面上大多数产品的需要，这反映出现实世界的产品只能以远糟于理想的效能运作。【注】

分贝与信号强度

放大器是以能量的数量级 (*orders of magnitude*) 放大信号。放大功率以分贝 (*decibel*, 简称 *dB*) 来计算, 以便舍弃不必要的 0。

$$dB = 10 \times \log_{10} (\text{输出功率} / \text{输入功率})$$

当输出功率大于输入功率, 此数值为正; 如果输出功率小于输入功率则为负。每 10 dB 的变化量相当提升 10 倍, 而每 dB 的变化量相当提升 2 倍。因此 33dB 的变化量相当提升 2000 倍。

$$33 \text{ dB} = 10 \text{ dB} + 10 \text{ dB} + 10 \text{ dB} +$$

功率有时候会以 *dBm* 计量, 亦即每毫瓦的 *dB* 值。要计算 *dBm* 值, 只要以 1mW 代入第一个方程式的输入功率即可。

$$dB = 10 \times 10 \times 10 \times 2 = 2000$$

记住提升两倍功率相当增加 3 dB, 这很有用。增加 1 dB, 粗略等同于功率提升 1.25 倍。记得这些数字, 将可以在脑海中快速计算出大概的增益。

10.3.2 路径损耗、传输距离与传输量

在 802.11 中, 网络的速度受到距离远近的影响。不同的 802.11 标准定义出了不同的调制方式, 速度范围从 1 Mbps 到 54 Mbps。接收器电路必须能够分辨不同的状态, 方能将位元数据从电波信号中取出。较高速的调制方式在特定时间内可以封装更多的位元, 因此需要比较乾净的信号 (以及更高的讯噪比) 方能成功解码。

电波信号行经空间时便会衰减。在 802.11 网络的有限范围内, 杂讯基准还不至于有太大的波动。不过距离一长, 信号的衰减就会影响接收端的讯噪比。当工作站逐渐远离基站, 信号准位就会不断下滑; 既然杂讯基准不变, 信号的衰减就会造成讯噪比的下滑。这种情况可以通过图 10-4 加以说明。与基站间的距离增加, 接收到的信号就愈趋近杂讯基准。距基站较近的工作站有较高的讯噪比。以网络工程而言, 当讯噪比过低以至于无法使用较高的速率, 工作站就会降速, 以便使用讯噪比要求较低的数据率。

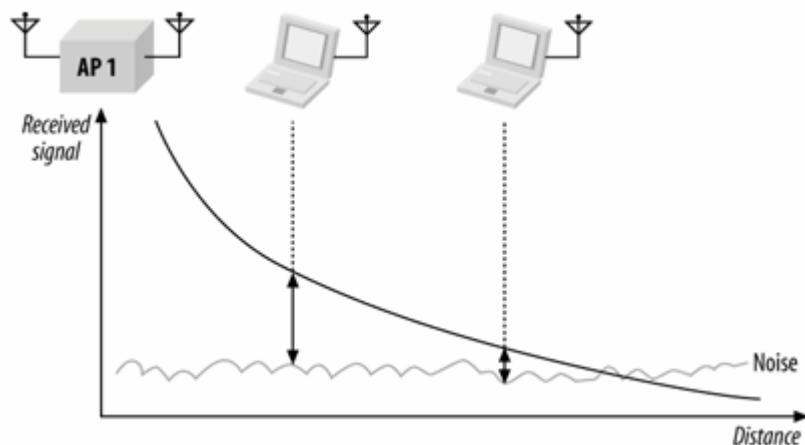


图 10-4: 传输量与距离之间的关系

如果当中没有障碍物阻隔, 信号的衰减就可以用下列公式加以计算。开放空间的损耗有时也称为路径损耗 (*path loss*), 因为它是预期中行经特定长度之路径的最小损耗。路径损耗受到

距离与电波频率的影响。距离愈远或频率愈高，则路径损耗愈大。**802.11a** 的传输距离之所以比**802.11b** 与**802.11g** 短，因为**802.11a** 所使用的**5 GHz** 路径损耗较大。开放空间的路径损耗可以表示成如下等式：

$$\text{路径损耗 (dB)} = 32.5 + 20 \log F + \log d$$

其中频率 **F** 以 **GHz** 表示，距离 **d** 以公尺为单位。不过，路径损耗不只受距离的影响，墙面或窗户等障碍物也会影响信号，至于天线或放大器则可用来加强信号，补偿传输时的损耗。计算距离时通常会加计一种称为链路边际(**link margin**)的虚构因素，代表无法预料的损耗。

$$\text{总损耗} = \text{传输功率} + \text{传输天线增益} - \text{路径损耗} - \text{障碍物损耗} - \text{链路边际} + \text{接收天线增益}$$

10.3.3 多重路径干扰

虽然有相当简单的公式可以预测电波的传播，但也只是针对**802.11** 网络的粗略估计。除了直线的路径损耗，还有其他现象会影响**802.11** 信号的接收。困扰无线网络的一个主要问题是多重路径衰落(**multipath fading**)。波与波之间具有叠加性(**superposition**)。当多个波聚集于某一点时，所产生的波即是所有波的加总。图 10-5 显示了一些波与波的叠加范例。

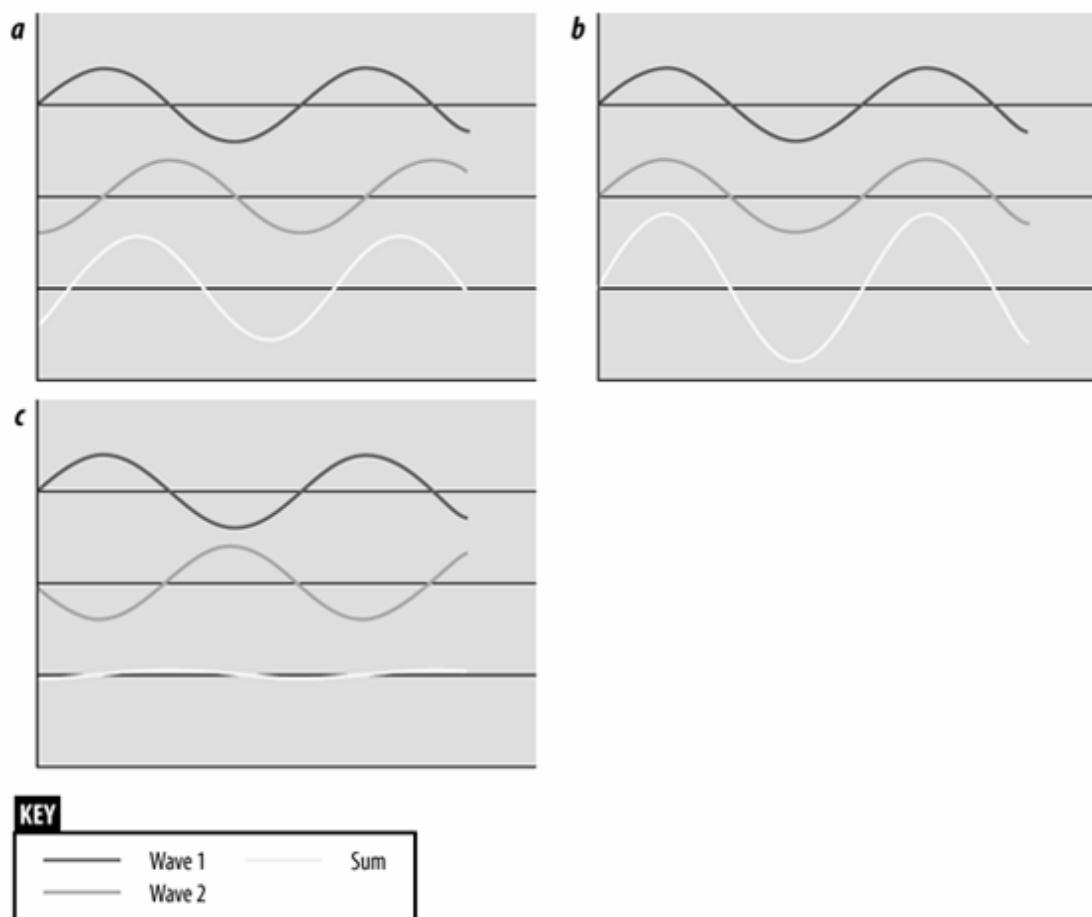


图 10-5：波的叠加组合

图 10-5<c> 所显示的两个波几乎完全相反，加总之后，相当于什么也没有。遗憾的是，这种情况出现在无线网络的次数，绝对出乎大家所料，802.11 设备大部分采用全向型天线，因此 RF 能量会往所有方向辐射。电波从天线向四方扩展，该区中各种物体表面则会加以反射。图 10-6 显示了一个经过高度简化的范例，其中有两部工作站位于完全没有阻隔的长方形区域内。

此图显示了从传送端到接收端的三种路径。接收端收到的电波为所各种电波的总合。图 10-6 所显示的路径加总起来的净值可能为。在这种情况下，接收端就无法察觉讯号的传输，因为根本没有收到任何信号。

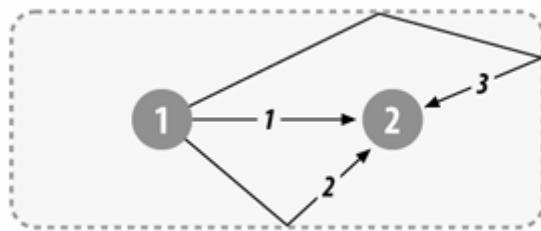


图 10-6：多重路径

由于干扰是相同的传输行走不同路径的迟延结果，这个现象就称为多重路径衰落(multipath fading) 或者多重路径干扰(multipath interference)。有时候，调整接收端的方向或摆设位置，即可解决多重干扰问题。

10.3.4 讯符间干扰 (ISI)

多重路径衰落属于讯符间干扰 (Inter-symbol interference, 简称 ISI) 的特例，从传送端至接收端，行经不同路径的电波，其路程不尽相同，因此彼此之间会有迟延落差，如图 10-7 所示。再次强调，波与波之间具有叠加性，因此造成整个波形的混淆扭曲。在实际情况下，来自不同路径的波前(wavefront)会彼此叠加。最先到达的波前与最后到达的多重路径回音，两者之间的时间差称为延迟范围 (delay spread)。延迟范围较长，就必须采用比较稳当的编码机制。802.11b 网络可以处理 500 ns 以下的延迟范围，如果延迟范围较短，效能就会更好。如果延迟范围实在太长，有些网络就会降低传输速率以为因应。有些厂商宣称，若要以 11 Mbps 全速运作而且保有合理的帧错误率 (frame error rate)，则迟延范围必须在 65 ns 以内。（如何解读产品规格表，将于第十六章探讨。）有些无线局域网络分析工具可以直接量测延迟范围。

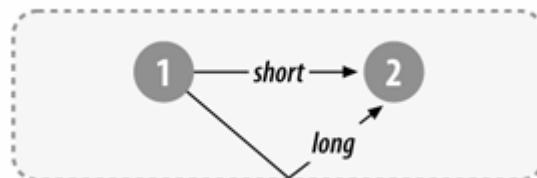


图 10-7：讯符间干扰

10.4 802.11 的 RF 工程

802.11 一直以惊人的速度被人们所采用。过去（习惯性地认为信号必然沿著定义明确之缆线而行）的网络工程师，如今所面对的局域网络，则是在充满杂讯。容易出错而且变化多端的无线链路上运行。802.11 之所以能够在数据网络领域获得成功，与 RF 工程脱离不了关系。真要介绍 RF 工程，起码得用上一本书的篇幅，也许还不止。就本书目的而言，我将会粗略地把篇幅浩瀚的 RF 工程议题分为两个部分：如何产生无线电波，以及如何传送无线电波。

10.4.1 RF 零件

RF 系统不但延伸了有线网络的范围，也和有线网络形成互补关系。虽然 RF 系统的零件，会因所使用的频率及信号的传送距离而异，不过所有系统基本上是相同的。其所使用的零件也不多。802.11 的使用者可能会对两种 RF 零件特别感兴趣：天线与放大器。之所以会对天线感兴趣，是因为在 RF 系统中，天线是有形的实体。而放大器和天线彼此互补，可以让天线输出更大的功率，在建构不同类型的 802.11 网络时，使用者或许也会感到兴趣。

10.4.1.1 天线

天线（antenna）是 RF 系统中最关键的零件，因为由它们负责将线路中的信号转换为电波，以及将电波反转为电路信号。在方块图中，天线通常是以倒三角形来表示，如图 10-8 所示。

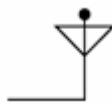


图 10-8：天线示意图

天线必须以导电材料制造方能运作，无线电波遇到天线时，电子就会流入导体而产生电流。同样地，在天线施加电流就会在天线周围产生电场，施加在天线上的电流不同，电场也会随著改变。变动的电场会产生磁场，因此形成电波。天线的长短取决于频率：频率愈高，天线愈短。每种频率可以使用的简易型最短天线长度为波长的一半（虽然天线工程师可以运用一些技巧进一步缩短天线）。这个经验法则同时适用于大型无线广播天线，以及移动电话所使用的小型天线。使用 830 kHz 频段的调幅广播电台，其电波的波长约为 360 公尺，因此必须使用大型天线。至于使用 2.4 GHz 频段的 802.11 网络界面，波长只有 12.5 公分。利用一些工程技巧，即可将天线整合到 PC 无线网卡里，或是笔记型电脑的 LCD 萤幕中。至于效能更高的外部天线，也可以让各位轻易放进背包或者电脑包随身携带。在设计上，天线也可以将方向性纳入考量。有些天线属于全向型（omnidirectional），亦即可以收发所有方向的信号。有些应用则受惠于指向型（directional）天线，这种类型的天线可以针对某个较窄的范围进行收发。图 10-9 比较了全向型与指向型天线的辐射功率。

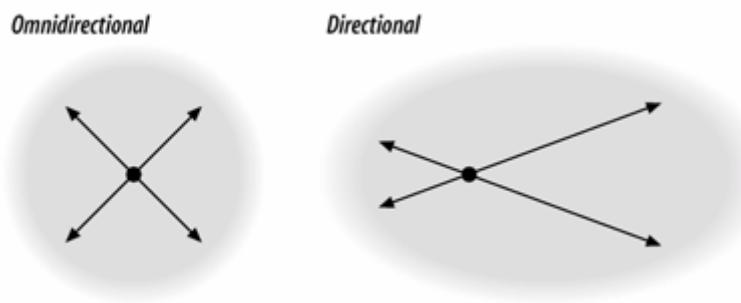


图 10-9：全向型与指向型天线的辐射功率

给予等量的输入功率，指向型天线可以传得较远，信号也比较清楚。对于所指的方向，其具备较高的无线信号敏感度。以无线链路取代有线网络时，通常会使用指向型天线。行动通讯业者划分细胞台(cell)时，通常会使用全向型天线，虽然也有例外—特别是希望网络可以延伸更远的距离时。同时，应该谨记在心的是，根本没有真正的全向型天线。我们通常习惯性认为，那些垂直悬挂的天线属于全向型，因为当你在天线的水平面移动时，信号并不会有太大的改变。不过如果你以垂直角度(亦即由上往下或由下往上)观察信号的辐射情况，就会发现这根本是两回事。如果你正为学校校区或公司园区组建网络，并且希望将天线置于大楼屋顶，就必须注意此现象。

本节所介绍的所有零件中，以天线最有可能和其他电子零件分隔两地。在这种情况下，你就得使用一条传输线(某种缆线)连接天线与收发器。传输线通常具备 50 欧姆的阻抗(impedance)。

就使用 2.4 GHz 频段的 802.11 设备而言，通常 PC 无线网卡会采用内建天线。这种

内建天线虽然堪用，但表现平平，顶多只能算是中上。天线愈大，效能愈佳。有些 802.11 网卡附有外部天线接头。外接天线可以让网卡有更好的效能，不过外观质感就会因此而大打折扣。为了满足改善天线效能的需求，同时不让丑丑的外接天线占用空间，许多笔记型电脑厂商便将天线内建在萤幕周遭的边框里。

10.4.1.2 放大器

放大器可以增强信号，信号的放大或增益程度系以分贝(decibels，简称 dB)做为量测单位。放大器大致上可以分为三种：低杂讯、高功率与其他种类、低杂讯放大器(Low-Noise amplifier，简称 LNA)通常与天线连接，用来将所收到的信号放大到与 RF 系统连结的电子零件可辨识的程度。LNA 同时也可以就杂讯系数(noise factor)区分等级，杂讯系数可用来评量放大器本身所带来的不相干信息。杂讯系数愈小，接收器就可以辨识愈细微的信号，因此可以涵盖较长的距离。

至于高功率放大器(High-power amplifier，简称 HPA)，则是用来将信号提升至最大功率而后传送。输出功率是以 dBm 做为量测单位，其与 watt 有关(参见本章对 f 分贝与信号强度所做的说明)。放大器依循的是热力学定律，因此在放大信号的同时会产生热量。802.11 PC Card 只能使用低功率传送器，因为如果安装在膝上型电脑，很快就会耗尽电池的电力。不过，基站可以外接放大器，另以电力较为充沛的电力设施(Power grid)供电。

放大器与天线关系到如何符合管制规定的微妙之处。802.11 设备限定使用 1 瓦输出功率以及 4 瓦有效辐射功率(effective radiated power，简称 ERP)。ERP 藉由天线增益(gain)减去传输线的损耗(loss)，让传送器的输出功率倍增。假设你手上有个 1 瓦的放大器，所使用的



天线可带来 8 dB 的增益，而传输线的损耗则是 2 dB。那么 ERP 即为 4 瓦；整个系统的增益为 6 dB，相当于提升传送器功率 4 倍。

第11 章 跳频物理层

1977 年 802.11 初稿所提出的物理层标准中，跳频展频 (frequency-hopping spread-spectrum，简称 FH 或 FHSS) 是最先得到广泛运用的物理层。支持跳频调制 (FH-modulation) 的电子零件相对比较便宜，而且无须用到多大的功率。起初，采用跳频网络的主要优点在于，相同区域内可以同时容纳好几个网络，而且这些网络的总和频宽或传输量相当高。不过到目前为止，跳频网络多半已经沦为 802.11 历史的注脚。虽然好歹也是一种标准 1 不过目前只剩一家厂商仍在生产与销售跳频系统，而且这些产品也渐渐淡出市场。随著更高速规格的发展，跳频系统的优勢已经逐渐消逝，何况新型芯片组更为省电，功耗更低。

本章描述了 FH PHY (跳频物理层) 的基本概念，以及其所使用的调制技术。此外，还会交待物理层收敛程序 (physical layer convergence procedure) 如何打造传送至无线链路的帧，以及稍微提到无线介质本身的一些细节。到目前为止，PH PHY 已经成为 802.11 历史的注脚，所以各位可以跳过本章，直接阅读下一章所讨论的 DSPHY (直接序列物理层)。然而，若能掌握 802.11 的技术演进，则可让你更清楚整体全貌。

11.1 11.1 跳频传输

所谓跳频，乃是以一种预设的准随机样式 (predetermined, pseudorandom pattern) 快速变换传输频率，如图 11-1 所示。图中的纵轴将可用频率划分为几个频槽 (frequency slot)。同样地，时间轴也被划分为一系列时槽 (time slot)。这些槽位 (slot) 的使用方式，系由跳频样式来控制。本图所使用的跳频样式为(2,8,4,7)。正确掌握跳频时机是主要关键；传送端与接收端必须同步，这样接收端才有办法随时与传输端的频率保持一致。

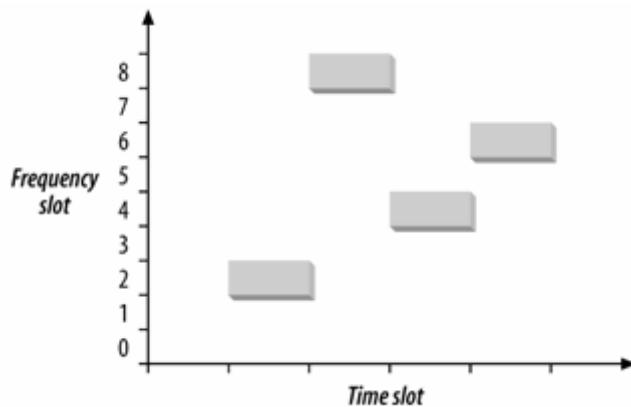


图 11-1：跳频

跳频有点类似分频多工 (frequency division multiple access，简称 FDMA)，不过有 4v 重要差异。FDMA 系统会为每个设备配置固定的频率。这些设备共同分享可用的无线频谱，各自使用不同频率。跳频系统所使用的频率会依时间而有所不同，并非一成不变。每个频率只使用一小段时间，称为停驻时间 (dwell time)。

最重要的是，调频可以避免设备干扰某个频段 (frequency band 简称 band) 的主要用户，这种做法之所以可行，是因为各个杂频段的主要用户有权使用较高的功率，传送足以覆盖无线局

域网络的信号。跳频用户对主要用户只会造成瞬间干扰，因为跳频将能量分散至较宽的频段。

[注] 同样地，主要用户只会影响展频设备的某个频槽，就像是瞬间的杂讯一般。图 11-2 显示了某个主要用户使用第 7 个频槽时所造成的影响。虽然第 4 个时槽的传输受干扰损毁，但前三个时槽还是可以成功传送。

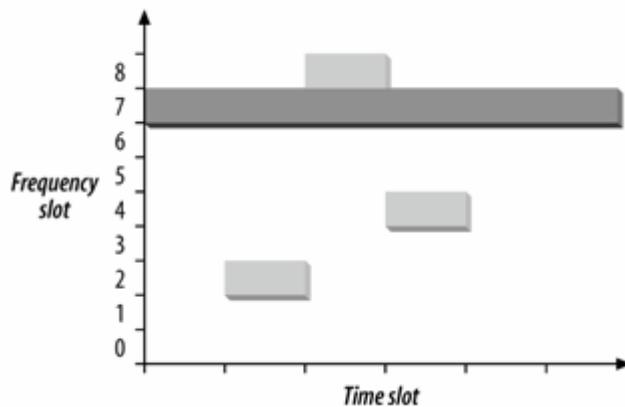


图 11-2：以跳频避免干扰

如果两个跳频系统需要共用相同频段，可以指定不同的跳频顺序，如此便不会互相干扰。在同一时间，每个跳频系统必须使用不同的频槽。只要两个系统使用不同的频槽，就不会互相干扰，如图 11-3 所示，和之前的图形一样，灰色方块的跳频序列为 (2,8,4,7)。其中加入了跳频序列为 (6,3,7,2) 的第二个跳频系统。彼此不相重叠的跳频序列称为正交 (orthogonal)。在同一区域使用多个 802.11 网络时，正交跳频序列可以使总传输量达到最高。

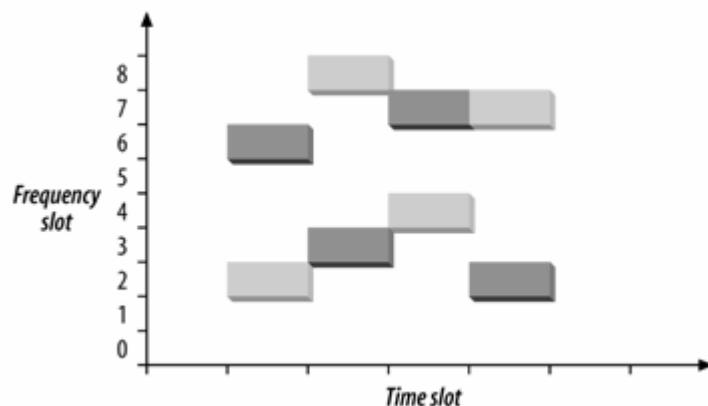


图 11-3：正交跳频顺序

11.1.1 802.11 FH 的细节

802.11 将 ISM 微波频段划分为一系列 1-MHz 的频道 (channel)。几乎 99% 的微波能量都限制在频道当中。802.11 所使用的调制方式 • 会将数据位元编码成频道中央所传送频率的偏移量 • 频道是以中心频率 (center frequency) 来定义，频道的中心频率为 2.400 GHz。之后每个频道会依序加上 1-MHz：频道 1 的中心频率为 2.401，频道 2 的中心频率为 2.402，一直到中心频率为 2.495 GHz 的第 95 频道 • 能够使用 ISM 频段哪些部分，依管制当局的规定而有所不同；主要的管制区 (regulatory domain) 及其可用频道均列于表 11-1。

表 11-1：不同管制区所使用的频道

管制区	可用频道
美国 (FCC)	2 至 79 (2.402-2.479 GHz)
加拿大 (IC)	2 至 79 (2.402-2.479 GHz)
欧洲 (不含法国与西班牙) (ETSI)	2 至 79 (2.402-2.479 GHz)
法国	48 至 82 (2.448-2.482 GHz)
西班牙	47 至 73 (2.447-2.473 GHz)
日本 (MKK)	73 至 95 (2.473-2.495 GHz)

802.11 FH 系统所使用的停驻时间为 390 个单位时间(time units), 相当于 0.4 秒, 当 802.11 FH PHY 在频道间进行切换时, 整个跳频程序不能超过 224 微秒。跳频本身必须符合额外的管制规定, 不论是跳频数的多寡, 或跳频的发生率皆然。

11.1.2 802.11 跳频序列

用以推演跳频组合 (hop set) 的数学函数, 属于 PH PHY 规格的一部分, 记载方 802.11 规格书第 14.6.8 款。举例而言, 北美与欧洲大部分地区所使用的跳频序列(hop sequence) 1, 其跳频顺序为 {13, 26, 65, 11, 46, 19, 74, 50, 22, 二}。802.11 a 一步将跳频序列区分为彼此不相重叠的组合, 同一组合的成员 (即跳频序列) 间彼此正交。在欧洲与北美, 每种组合包含 26 个成员。有些地区的管制当局会限制可跳频的频道数, 因此每个组合将包含较少的成员。详见表 11-2。

表 11-2：每个管制区跳频组合所包含的序列数量

美国 (FCC)	26
加拿大 (IC)	26
欧洲(不含法国与西班牙) (ETSI)	26
法国	27
西班牙	35
日本 (MKK)	23

11.1.3 加入 802.11 跳频网络

跳频序列的标准化, 使加入跳频网络成为可能。FH 网络的 Beacon 帧包含时戳(timestamp) 以及 FH 参数组合元素{FH Parameter Set element}。FH 参数组合元素包含跳频样式编号(hop pattern number) 以及跳频索引(hop index)。收到 Beacon 帧后, 工作站就会知道如何同步本身的跳频样式。

工作站可根据跳频序列编号(hop sequence number)得知道自己的跳频次序。举例而言, 假定有个工作站收到 Beacon 帧, 表示该 BSS 使用了编号为 1 的北美/欧洲跳频序列, 而且目前的跳频索引为 2。只要查询跳频序列, 该工作站就可以判定下个频道为 65。跳跃时间也有明确的定义。每个 Beacon 帧均包含一个 Timestamp (时戳) 栏位, 当以时戳对「Beacon 帧中之停驻时间」取模数 (modulo) 而结果为 0 时, 就会发生跳频。

11.1.4 ISM幅射量规定与最大传输量

802.11 跳频系统受到频谱配置政策所规范。举例而言，以下是美国 FCC 所提出的三项主要规定：【注】

1. 频段至少必须包含 75 个可供跳频的频道，占用 83.5-MHz 的频宽。

2 跳频频道所使用的频宽不得大于 1 MHz。

3. 设备必须平等对待每个可用频道。30 秒的周期内，每个频道不能停驻超过 0.4 秒。在这些规定当中，以第二项最为重要。不论使用多么神奇的编码机制，任何时刻都只能使用 1 MHz：频宽。虽然因为另两项规定，频道会不断变动，但第二项规定无疑限制了用来编码数据的信号变化量。

如果采用双阶编码，每个周期可以编码一个位元。以每周期 1 位元而言，1 MHz 可以提供 1 Mbps 的数据传输率。较复杂的调制与解调制机制可以提高传输率，四阶编码可以在一个周期内包装两个位元，因此 1-MHz 频宽可以提供 2 Mbps 的传输率。欧洲电信标准协会（European Telecommunications Standards Institute，简称 ETSI）同时也为使用 ISM 频段的展频设备制定了一组规范，记载于欧洲电信标准（European Telecommunications Standard，简称 ETS）300-328。ETSI 允许使用较少的频道；只需要 20 个就够了。不过，ETSI 对于辐射功率的管制就严格得多。实际上，为了同时符合 FCC 与 ETSI 的规定，设备通常会使用 FCC 所要求的频道数，搭配 ETSI 所规定的辐射功率。

11.1.5 干扰效应

802.11 是第二个使用 2.4-GHz ISM 频段的标准，因此不得不接受来自其他传输的干扰，这些传输通常具备较高的优先性。严重的干扰可能导致某个频道不堪使用，不过其他频道却不受影响。以美国和欧洲大约 80 个可用频道来讲，一个频道受到干扰，最多会使介质的原始位元率（raw bit rate）降低 1.25%。（在 IP 层通常必须付出较高的代价，因为还要将帧间隔。回应讯息、帧标头以及物理层收敛协议标头计算在内）有愈多频道受到干扰，传输量就愈低。参见图 11-4

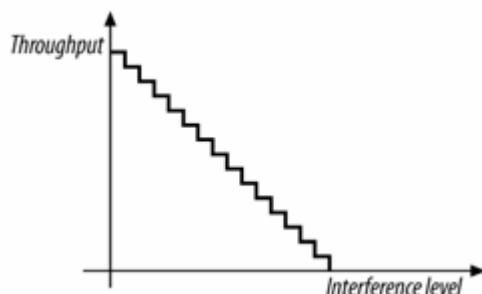


图 11-4：干扰对 FHSS 系统之传输量的影响

11.2 高斯频移键控 (GFSK)

FH PHY 采用了高斯频移键控 (Gaussian frequency shift keying, 简称 GFSK)。[注] 频移键控就是将数据编码成载波 (carrier) 中一系列的频率变动，将数据编码成频率的好处是，杂讯通常会随信号的振幅而改变；与振幅无关的调制系统（例如，调频广播）通常比较能够免于杂讯的干扰。GFSK 当中的 Gaussian 意指电波脉冲的形状 [编注：即钟形曲线 (bell shaped curve)：钟形曲线又称高斯曲线 (Gaussian curve)]；GFSK 将能量的发散限定在相对较窄的频段当中，因此适合做为频段的再利用 (secondary use) 工具。防止 RF 能量溢散的信号处理技术著实不错，对某个频段的再利用者 (secondary user) 而言尤其如此。藉由降低干扰的可能性，GFSK 让 802.11 无线局域网络得以组建在某个频段已经有更高优先用途的地区。

11.2.1 二阶式 GFSK

最基本的 GFSK 实作称为二阶式 GFSK (2-level GFSK, 简称 2GFSK)。其中使用了两种频率，分别代表。或 1。要传送 1，就会将载波频率提高一特定量。至于 0，则是将载波频率减少一特定量。图 11-5 显示了一般的编码程序。实际系统上所使用的载波频移量较小，为了说明编码的运作方式，本图刻意画得比较夸张。

通过系统所传输的数据率称为讯符率 (symbol rate)。由于必须经过几个周期以后，才有办法判定所使用的载波频率，以及其所传送的信号究竟为 1 或 0，通常讯符率只是载波频率的零头。虽然载波频率约有每秒 24 亿个周期，但讯符率通常每秒只有一或两百万个讯符。

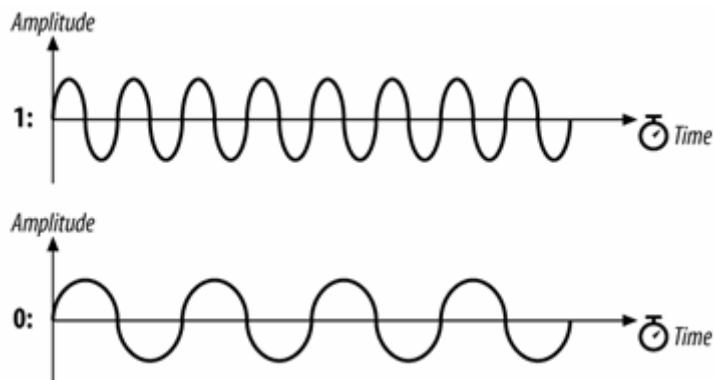


图 11-5: 二阶式 GFSK

GFSK 的频率变动并不剧烈。瞬间频率变动较大则需要使用较贵的电子零件，以及较高的功率。较和缓的频率变动可以降低设备的成本，RF 溢散 (leakage) 也较低。图 11-6 说明了以 2GFSK 为字母 M (二进制码为 1001101) 进行编码时的频率变动状况，需特别注意的是，图中纵轴代表传输频率。传送 1 时，频率会提升至中心频率以上，相当于中心频率加上特定偏移量，传送 0 时，频率则以相同偏移量下降。代表时间的水平轴被切割为许多讯符周期 (symbol period)。在每个周期中点，接收器会对传输频率进行量测，同时将该频率转换为讯符 (symbol)。（在 802.11 跳频系统中，较高级的数据在传送前会经过搅码 (scrambled)，因此要传送给对方的位元顺序不见得和空气中的位元顺序相符。本图纯粹在说明 2GFSK 的运作原理，不涉及实际的编码。）

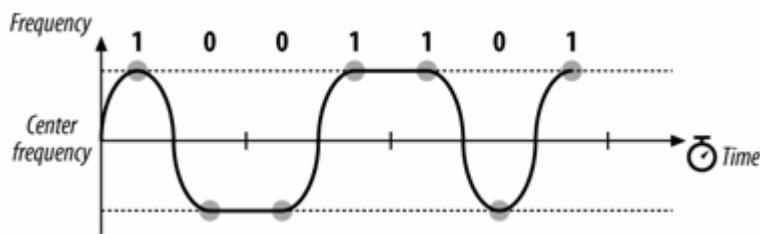


图 11-6: 以 2GFSK 对字母 M 进行编码

11.2.2 四阶式 GFSK

利用此机制，你可以有两种传递更多数据的方式：使用较高的讯符率，或者在每个讯符中编码更多位元信息。四阶式 GFSK (4-level GFSK，简称 4GFSK) 基本上和 2GFSK 采用相同的方式，不过使用四种讯符。这四种讯符(00、01、10 与 11)会分别对映到特定的离散频率 (discrete frequency)，因此在符号率相同的条件下，4GFSK 可以传送两倍的数据。显然，这并非毫无代价：4GFSK 必须使用较复杂的发射器与接收器。讯符与频率之间的对应关系如图 11-7 所示。

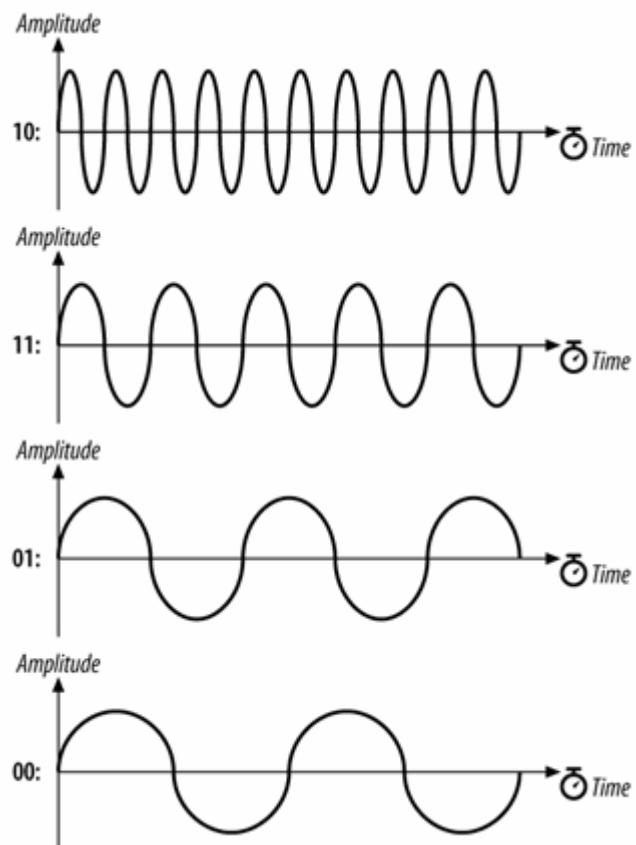


图 11-7: 4GFSK 之讯符与频率的对映关系

采用比较复杂的信号处理方式，4GFSK 可以在单一讯符中包装更多位元。图 11-8 说明了如何对字母 M 进行编码。再次强调，纵轴代表频率，横轴切割为许多讯符时间。讯符的传输是通过频率的变动；每个讯符的频率如虚线所示。本图其实暗示了 GFSK 编码方式在提高位元率

时必须面对的问题。区分两种信号准位十分简单，四种就比较困难。位元率每提高两倍，信号准位也就变为两倍，RF 元件就必须区分更细微的频率变动。实际上，这些限制使得 FH PHY 局限于 2 Mbps。

11.3 FH PLCP

在帧被调制至 RF 载波之前，来自 MAC 的帧必须先经过物理层收敛程序(Physical Layer Convergence Procedure，简称 PLCP)加以处理。不同的物理层可能有不同的需求，因

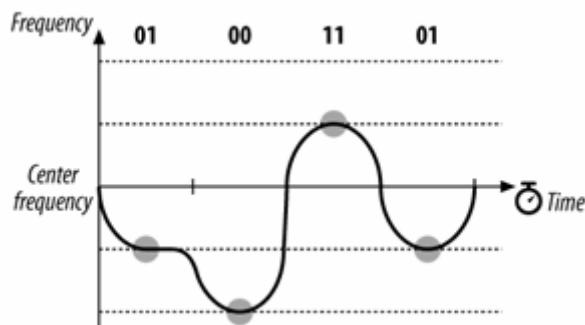


图 11-8 以 4GFSK 对字母 M 进行编码

此 802.11 允许物理层在处理即将传送至空气的 MAC 帧时，可以有某种程度的自由。

11.3.1 分封 (Framing) 与白化 (whitening)

FH PHY 所使用的 PLCP 会在 MAC 传来的帧前面加上标头，其中包含五个栏位 PLCP 是位于 MAC 以及 PMD (实际搭配介质) 无线界面之间的中继站，以 ISO 参考模型的术语来讲，从 MAC 传来的帧属于 PLCP 服务数据单元 (PLCP service data unit，简称 PSDU)。PLOP 的分封格式如图 11-9 所示。

Preamble (同步信号)

和有线 Ethernet 一样，Preamble 同步信号) 系用来同步发射器与接收器，以维系两者之间的计时关系。在 802.11 FH PHY 中，同步信号是由 Sync (同步) 以及 Start Frame Delimiter (帧界定符号，简称 SFD) 两个栏位所组成。

Sync (同步)

Sync 栏位的长度为 80 个位元，由一系列 01 交替的序列 (010101...01) 所组成。工作站会找寻此同步样式 (sync pattern)，准备接收数据。除了同步传送端与接收端，Sync 栏位还有其他三种目的。首先，同步信号的出现，代表帧即将到来。其次，有些工作站的天线不只一支，如此可防范多重路径衰落 (multipath fading)，或其他环境所造成的接收问题。这些工作站可以选用收到最强信号的天线。最后，接收端可以衡量所收到信号的频率是否偏离正常值，如有必要则加以校正。

SFD (讯框界定符号)

和 Ethernet 一样，SFD 用来指示同步信号的结束，以及帧的开始。FH PHY 采用的是 16 位元的 SFD: 0000 1100 1000 1101。

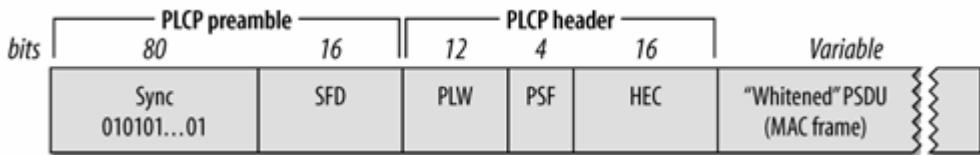


图 11-9 : PH PHY 所使用的 PLCP 帧分封格式

Header (标头)

同步信号之后紧跟著是 PLCP 标头。此标头包含 PLCP 所使用的媒体层专属参数。此标头由三个栏位组成：一个长度栏位 (PLW)、一个速度栏位 (PSF) 以及一个帧检查码 (HEC)。

PLW (PSDIT Length Word)

PLOP 标头的第一个栏位是 PLW。PLCP 帧的承载数据 (payload) 为长度可达 4,095 个位元组的 MAC 帧，这个栏位的长度有 12 个位元，用以通知接收器 PLCP 标头之后的 MAC 帧长度。

PSF (PLOP Signaling)

位元 0，即第 1 个被传送出去的位元，目前保留不用，设置为 0。位元 1-3 是所承载之 MAC 帧的传输率编码。由于有几种速度可供选择，因此这个栏位可供接收器调整适合的解调制机制。虽然 802.11 标准允许你使用速度介于 1.0 Mbps 与 4.5 Mbps 之间。增量为 500kps 的数据传输率，但目前只为 1.0 Mbps 与 2.0 Mbps 两种速度定义调制机制。【注】参见表 11-3。

表 11-3: PSF 的意义

位元 (1-2-3)	数据传输率
000	1.0 Mbps
001	1.5 Mbps
010	2.0 Mbps
011	2.5 Mbps
100	3.0 Mbps
101	3.5 Mbps
110	4.0 Mbps
111	4.5 Mbps

HEC (Header Error Check)

为了防止 PLCP 标头错误，因此使用长度为 16 个位元的 CRC 来检验整个标头的内容，并将其置于此栏位。不过此标头并未防范帧其他部分的错误。对于 Data 栏位所放置的内容并无任何限制。任何数据均包含一长串连续的 0 或 1，这使得数据看起来不是那么随机。为了让所要传送的数据比较像是随机的白噪音 (white noise)，FH PHY 将会以一种白化演算法 (whitening algorithm) 对 MAC 帧进行处理。此演算法会在电波传送之前对数据进行搅码 6 接收器则是通过逆向处理来还原数据。

11.4 FH PMD

虽然 PLCP 标头里有一个记载 MAC 帧传输率的栏位，不过其中只有两种符合 PMD 附属层标准。这两种 PMD 之间具有许多共通特性，例如：支持天线分集（即多重天线），允许启用或关闭天线内建的功率放大器，以及使用高斯脉冲调整器（Gaussian Pulse shaper）尽量将 RF 能量限制在狭窄的跳频频段。图 11-10 显示了 802.11 跳频网络所使用之收发器的一般设计。802.11 标准规定，以 1 Mbps 或 2 Mbps 传送时，收发器起码必须具备一 80 dBm 的灵敏度。

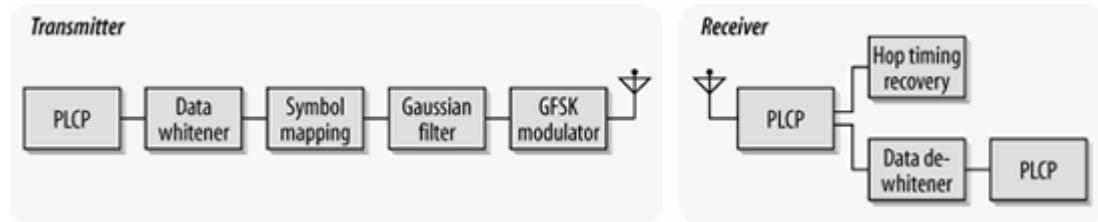


图 11-10：跳频收发器

11.4.1 传输率 1Mbps 之 FH PHY 所使用的 PMD

基本的跳频 PMD（实际搭配介质）允许 1.0 Mbps 的数据传输率。来自 MAC 的帧已经附加上了 PLOP 标头，所产生的位元序列，会从无线电波界面传送出去。为了符合 1-MHz 的频宽管制，每秒只能传输一百万个讯符。由于所采用的调制机制为 2GFSK，因此每个讯符可以编码一个位元。802.11 规定所使用的最小功率为 10 毫瓦，同时要求使用功率控制，必要时将幅射功率限定在 100 毫瓦。

11.4.2 传输率 2 -Mbps 之 FH PHY 所使用的 PMD

FH PHY 还有另外一种较高速的 PMD 可以使用，和 1.0-Mbps 之 PMD 一样，附加上 PLCP 标头之后，再利用 2GFSK 以 1.0 Mbps 的速率进行传输。在 PLCP 标头中，PSF 栏位所代表的是帧主体（frame body）的传输率。采用较高的数据传输率时，帧主体则会使用不同于物理层标头的编码方式。管制上要求所有 PMD 只能使用 1MHz 的讯符率，因此 4GFSK 只能用于帧主体。每个讯符分别代表两个位元，因此每秒一百万个讯符可以达到 2.0 Mbps 的数据率。如果信号品质太差无法使用较高速率，支持 2.0-Mbps 之 PMD 的韧体可以降速而改用 1.0-Mbps 之 PMD。

11.4.2.1 载波检测/净空频道评估 (CS/CCA)

为了落实 802.11 的 CSMA/CA 功能，PLCP 包含了一种功能，可藉以判断目前无线介质是否正在使用。MAC 不仅使用虚拟载波检测机制，也使用了实际载波机制，而实际载波检测是由物理层所负责。802.11 并未规范如何决定信号是否存在，只要能够符合标准所要求的效能，厂商可以自由决定如何实作。802.11 规定，信号检测能力必须符合最起码的要求，至少能够检测到具一定功率且与 802.11 相容的信号。

11.5 PH PHY 的特性

表 11-4 列出了 FH PHY（跳频物理层）里的一些参数值。除了该表所列的标准化参数，FH PHY 尚有一些参数可供调整，让 802.11 跳频系统各部分的迟延得以维持均衡。其中包括 MAC、

PLCP、收发器等的迟延变数，以及收发器电子零件个别变异的相关参数。另外值得注意的是，同一区域所有跳频网络的整体传输量（total aggregate throughput）相当高。整体传输量乃是跳频组合大小的函数。在每个跳频组合中，所有序列彼此保持正交关系，不会互相干扰。在北美与欧洲大部分地区，每个区域同时可以组建 26 个跳频网络。如果每个网络的传输率为 2-Mbps，其中有一半时间是用来传递承载数据（user payload data）只要 ISM 频段没有什么干扰存在，该区的总传输量即可高达 26-Mbps.

表 11-4 FH PINY 参数

参数	值	备注
槽位时间	50 微秒	
SIFS 时间	28 微秒	SIFS 可用来推衍出其他帧间隔值（DIFS，PIFS 以及 EIFS）0
竞争时间的长短 (Contention window size)	15 至 1,023 个槽位	
同步信号持续时间 (Preamble duration)	96 微秒	同步讯符以 1 MHz 的速率进行传输，因此传输每讯符需时 1 微秒：96 个位元则需要 96 个讯符时间。
PLCP 标头持续时间 (PLCP Header duration)	32 微秒	PLCP 标头有 32 个位元，因此需要用到 32 个讯符时间。
最大 MAC 帧 (Maximum MAC frame)	4,095 个位元组	802.11 建议最多使用 400 个讯符（1 Mbps 使用 400 个位元组，2 Mbps 使用 800 个位元组），以便在不同环境下维持效能的一致性。
最低灵敏度 (Minimum sensitivity)	-80 dBm	

第12 章 直接序列序列物理层： DSSS 与 HR/DSSS (802.11b)

首次修订的 802.11 规格书，规范了采用直接序列展频（direct sequence spectrum，简称 DSSS）技术的第二种物理层。802.11 直接序列展频物理层的数据率为 1 与 2Mbps。虽然速度与跳频物理层相同，不过人们很快就发现，直接序列技术有潜力达到比跳频技术更高的速度。因此就算当时两者速度相当，直接序列还是成为了物理层的首选。1999 年，802.11b 规范了数据率可达 5.5 与 11Mbps 的物理层。之前 1 与 2Mbps 的物理层通常与后来的 5.5 与 11Mbps 物理层合并为单一界面，即使它们的规格并不相同。（它通常被称为 802.11b，虽然这两个较低的速率并不属于 802.11b）。本章将会介绍直接序列物理层（DS PHY）的基本概念，以及所采用的调制技术。除了说明 PLCP 如何处理即将通过电波链路的帧，还会简短交待实体介质本身的一些细节。

12.1 直接序列传输

直接序列传输是一种不同的展频技术，可以通过较宽的频段传送信号。直接序列技术的基本运作方式，是通过精确的控制将 RF 能量分散至某个宽频频段。当无线电载波的变动被分散至较宽的频段时，接收器可以通过相关处理（corelation process）找出变动何在。图 12-1 以比较抽象的观点说明了直接序列的基本运作方式。

位于图左的是传统的窄频电波信号。信号经过展频器的处理，以数学转换公式将窄频输入信号的振幅平坦化，分布至相对较宽的频段。对窄频接收器而言，经过直接序列展频处理的信号就像一些低准位杂讯，因为 RF 能量已被扩展至较宽的频段。直接序列传输的关键是，RF 载波的任何调制也同时被扩展至整个频段。接收器可以监视某个宽频频段，找寻影响整个频段的变动何在。原始信号可以通过相关器（correlator）还原，只要逆转整个展频程序即可。

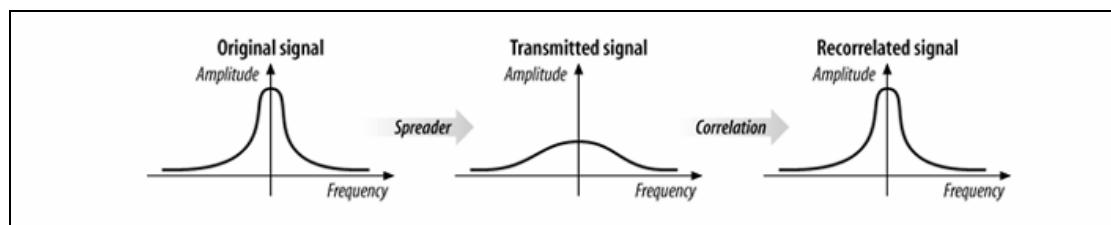


图 12-1：基本的 DSSS 运作方式

从高价的观点来看，相关器只是在找寻影响整个频段的 RF 信号变动。相关性（Correlation）所提供的防护，使得直接序列传输可以抗拒相当多的干扰。? 讯通常是以突波或脉动形式出现，相对而言所占的频段较窄。在定义上，这类? 动并不会影响整个频段。因此，相关函数（correlation function）会将杂讯扩展至整个频段，所以经过相关处理的信号完全不受影响，如图 12-2 所示。

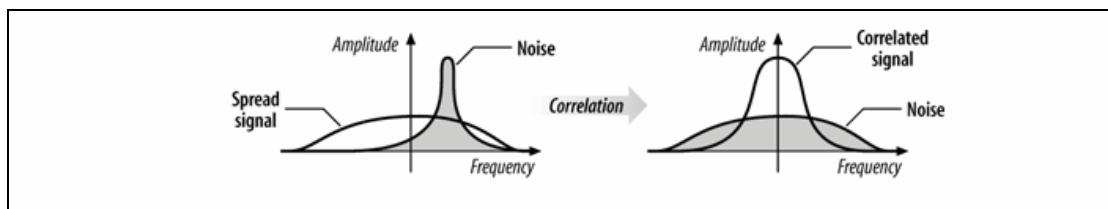


图 12-2：以相关处理扩展杂讯

直接序列调制的运作方式，乃是以展频码（chipping sequence，或译为缀片序列）对数据串流作处理。chip（缀片）乃是展频程序中所使用的二进制数字。bit（位元）属于比较高价的数据，chip（缀片）则是编码程序中使用的二进制数字。bit 与 chip 之间并不存在任何数学上的差异。展频开发人员之所以采用这个术语，是为了表明 chip 虽属编码与传输程序的一部分，然而本身并未携带任何数据。展频码亦称为准随机杂讯码（PN code），其传输率必须高于数据。（直接序列物理层的主要功耗，在于使用高频振荡器来产生缀片串流或者还原数据）图 12-3 显示了直接序列调制的数据传输过程中，展频码所扮演的角色。位于图左的是单一的数据位元，其值为 1 或 0。每个数据位元都会用到好几个缀片。图中，缀片串流由 11 个位元所组成展频码，展频码与数据位元组合后，产生携带数据位元的 11 个缀片。这 11 个缀片/单一数据位元序列，是通过电波链路来传送。在接收端，会以同样的缀片串流（即展频码）来比较这 11 个缀片区块。如果与展频码相符，所还原的数据位元为 0；如果不符，所还原的数据位元为 1。

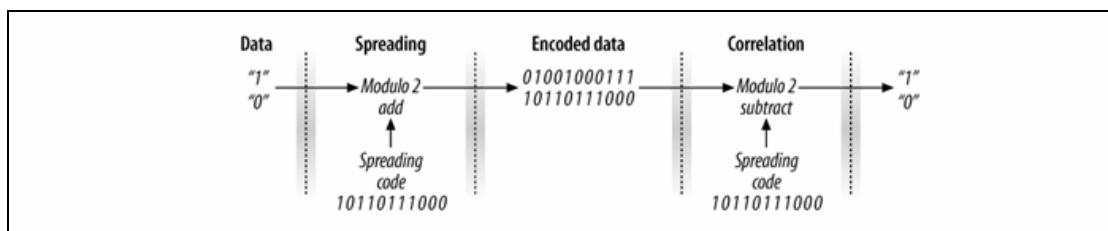


图 12-3：加入展频码

以较高的缀片率（chip rate）对较低的位元率（bit rate）信号进行编码，会产生信号功率被扩展至较大频宽的副作用。直接序列系统最重要的特性之一即是展频率（spreading ratio），代表传输单位元（bit）必须使用多少个缀片（chips）。【注】较高的展频率可以提高信号的还原能力，不过需要使用较高的缀片率及较大的频宽。将展频率提高两倍，需要用到两倍的缀片率，也需要用到两倍的频宽。增加缀片率需要付出两种成本。直接成本就是必须使用价格比较昂贵，可以在较高频率运作的 RF 零件，而间接成本则是所需要的频宽。因此在设计直接序列系统时，应该尽量将展频率压低，这样在符合设计需要的同时还可以避免浪费频宽。

直接序列调制是以频宽交换传输量。相较于传统的窄频传输，直接序列调制显然需要更多电波频谱，速度也比较慢。不过，它通常可以跟其它干扰源共存，因为接收器的相关函数（correlation function）有效地排除了窄频？讯。相较于跳频，直接序列技术也比较容易提升传输量。管制当局并未限制频谱的使用量，，通常限制的反而是处理增益的最低下限。使用较宽的频段可以达到较高的传输率，不过较宽的频段需要使用较高的缀片率。

12.1.1 802.11 直接序列网络的编码方式

802.11 采用 11 个位元 Barker word 做为展频码 (PN code)。每个位元均以 Barker word 进行编码。Barker word 及其属性的详细探讨已超出本书的范围。对 802.11 网络而言，Barker word 的关键属性就是具备良好的自动相关展频率 (spreading ratio) 关系到所谓的处理增益 (processing gain)。有时候这两个名记彼此通用，不过处理增益必须将系统的实际损耗纳入考量，因此其值稍微低于理想中展频率。(autocorrelation) 性质，亦即接收器所使用的相关函数在绝大多数环境中的表现均合乎预期，而且相对比较能够容忍多重路径衰落。Barker word 之所以使用 11 个位元，是因为管制当局通常要求直接序列系统必须具有 10 dB 的处理增益 (processing gain)。每一个位元配置 11 个位元的展频码，可让 802.11 符合管制要求，而且还留有一点安全边际。以 11 个位元做为展频码并不算多，因此可以容纳更多更多的重叠网络。较长的展频码可以得到较高的处理增益，不过需要使用较大的频宽。802.11 使用 Barker 序列 {+1, -1, +1, +1, -1, +1, +1, -1, -1, -1} 做为展频码。用在 802.11 时，+1 更换为 1，而-1 更换为 0。因此 Barker 序列就变成了 10110111000。模 2 的加法器 (modulo-2 adder) 会将之运用到数据串的每个位元。

【注】如果编码对象为 1，展频码所有位元均会改变；如果编码对象为 0，就会保持不变。图 12.4 说明了整个编码程序。

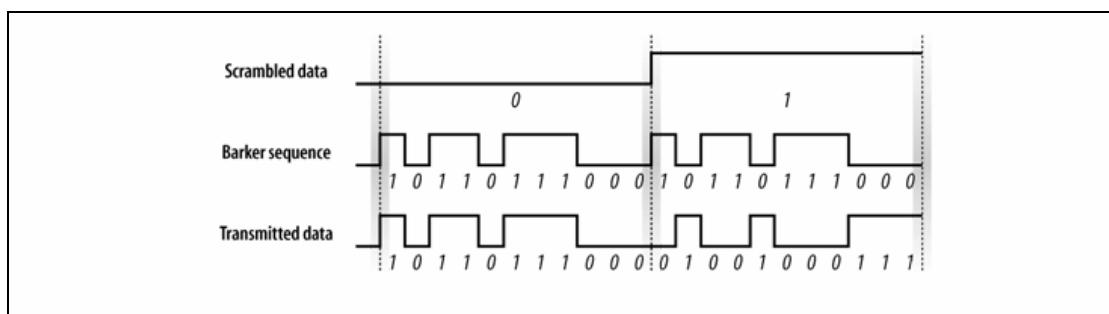


图 12-4：以 Barker word 进行编码

接收器可以定期检视所收到的位元当中包含多少个 1。Barker 序列本身有六个 1 和五个 0，则代表所要传送的是 1。除了计算 1 与 0 的数目，接收器也可以藉由位元样式的分析，推论出所传送位元的实际值。

注 以 Barker 序列进行编码的技术，和一些无线电话系统所使用的分码多工 (code division Multiple access，简称 CDMA) 技术类似。此技术让多部工作站 (手机) 行以同时访问无线介质。CDMA 采用相当复杂的数学运算，以确保每部手机的传输，对其他位于同一细胞台的手机而言，就像是随机的杂讯。其所涉及的数学运算，远比固定的准随机杂讯码复杂许多。

12.1.2 802.11 直接序列网络所使用的无线电频谱

相较于 FH PHY，DS PHY 所有用的频道较宽。DS PHY 在 2.4-GHz 频段使用了 14 个频道，每个频道的频宽为 5 MHz。频道 1 位于 2.412 GHz，频道 2 位于 2.417 GHz，依此类推至位于 2.472 GHz 的频道 13。频道 14 是特别针对日本所定义的，其中心频率与频道 13 的中心

频率相差 12 MHz。表 12-1 显示了每个管制当局允许使用哪些频道。北美与欧洲均允许使用频道 10，这也就是为什么大部分产品均以频道 10 作为预设频道。

表 12-1：各管制区所使用的频道

管制区	可用频道
美国(FCC)/加拿大(IC)	1-11 (2.412-2.462 GHz)
欧洲，不含西班牙(ETSI)	1-13 (2.412-2.472 GHz)
西班牙	10-11 (2.457-2.462 GHz)
日本(MIC)	1-13 (2.412-2.462 GHz) 与 14 (2.484 GHz)

12.1.2.1 频道能量的分布

每个频道中，大部分的能量会散布在 22-MHz 的频段。因为 DS PHY 使用的是 11-MHz 的芯片时脉，能量会从频道中心以 11MHz 的位数分散出去，如图 12-5 所示。为了避免干扰相邻的频道，第一个旁波瓣（side lobe）会经过处理，使之小于频道中心频率能量 30 dB。第二个旁波瓣经过处理，使之小于频道中心频率能量 50dB。这相当于分别将能量降低 1000 位与 100000 位。这些限制在图 12-5 当中是以 dBr 标记，亦即与频道中心能量的相对 dB 值。图 12-5 使用的是对数刻度量表（logarithmic scale）：-30 dBr 其代表一千，而 -50dBr 则代表十万。

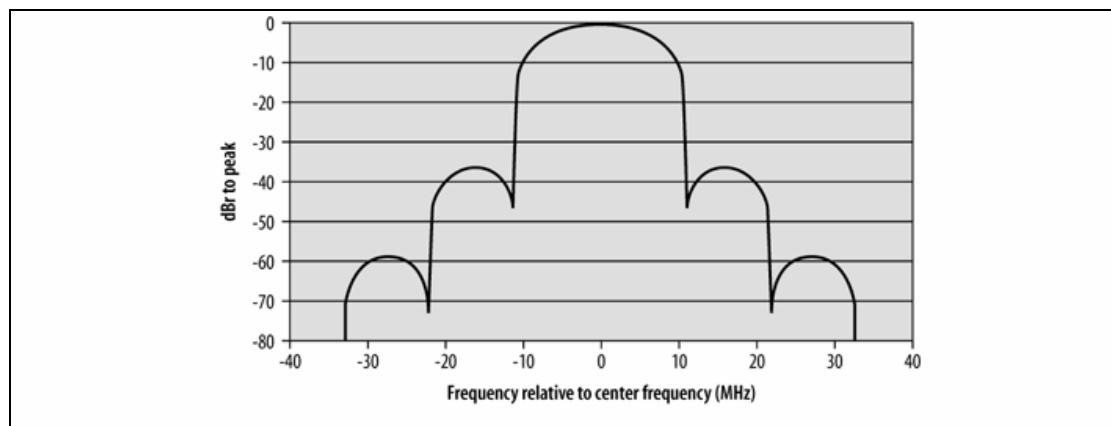


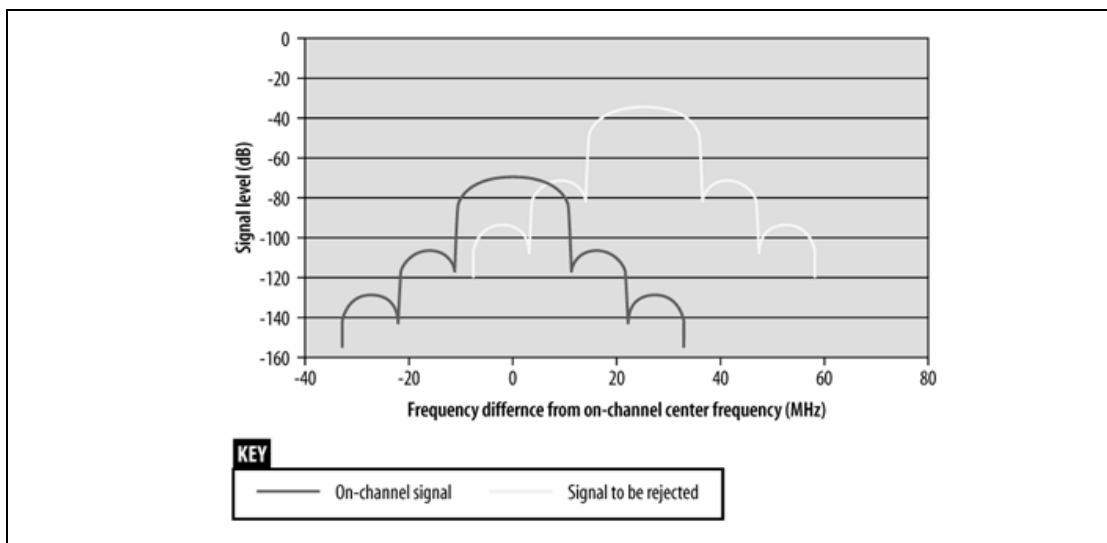
图 12-5：802.11 DS 之各个传输频道的能量分布

通过传送滤波器（transmit filters），可将大部分的 RF 能量限制在 22-MHz 频段。欧洲的管制单位限定最高的辐射功率只能为 100 毫瓦；美国的 FCC 则允许使用 1000 毫瓦的辐射功率。如果使用指向型天线，甚至可以将能量集中为更高的辐射功率。

12.1.2.2 邻频拒斥 (adjacent channel rejection) 与频道分隔 (channel separation)

为了避免干扰，必须在频域中对 802.11 设备加以区隔。最初的规格书要求相距 30MHz 的两个邻近信号必须有 35dB 的拒斥值，可以频道的中心频率输入一个极速信号（maximum-speed signal），如图 12-6 左边的曲线。它的功率比规定的最低灵敏度高 6dB；对 802.11b 接收器而言为 -70dBm。在相距 25MHz 以上之处输入第二个 11 Mbps 的 802.11b 信号，强度提高 35dB。右边曲线代表干扰测试信号。只要帧错误率低于 8%，接收器就算通过测试。请注意，干扰信号

的第一个旁瓣（first lobe）与主频（on-channel）信号的中心主瓣（main center lobe）间存在明显的重叠。



图：12-6：邻频拒斥

邻频拒斥也会影响同一时间可用的频道数。虽然 ISM 频段的 802.11 网络定义了 14 个频道，不过频道间相当接近。真实信号必须加以区隔以避免干扰。802.11b 标准认为 25MHz（5 个频道）的间隔即已足够。图 12-7 显示了在所谓的非重叠频道（1、6 与 11）上进行传输时的频谱遮罩（spectral mask）。相较于之前的图形，比较容易看出若使用非重叠的频道组合，所有系统元件都必须以最高效率运作。不过在真实世界里，并非所有无线电系统都能够以近乎极限的方式拒斥信号很强的邻频传输。虽然可以使用重叠较多的四频配置方式（例图 1.4.7 与 11），不过这种部署策略并不常见。频道间的重叠部分愈多，相邻频道的电波作业就愈容易受到干扰。干扰太高会导致载波检测制回报介质处于忙碌状态，或者导致传送中的帧损毁。不论如何，个别频道的最高传输量都会因此变少。以少许传输量换来全区频宽看似划得来，事实上并非如此。

不论称之为 1、6 与 11；A、B 与 C 或者 Tom、Dick 与 Harry，在 2.4 GHz 无线局域网络中，最多只能有三个非重叠频道。

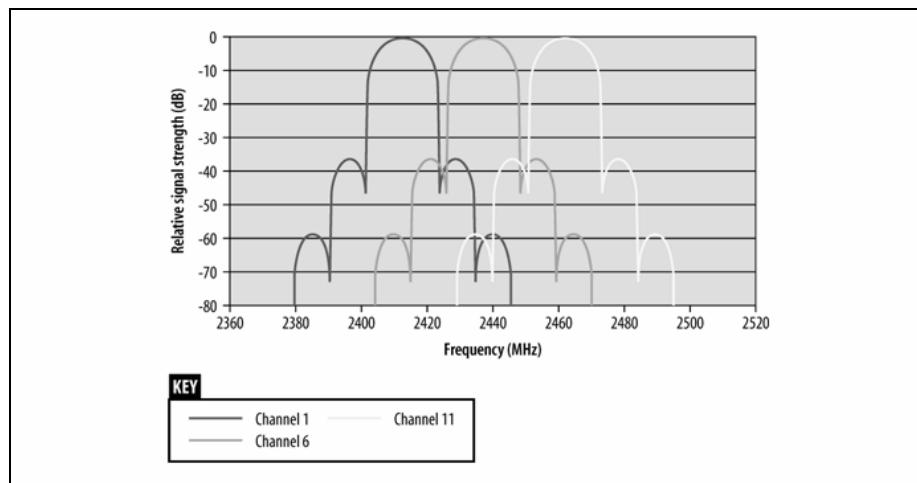


图 12-7: 802.11 DS 网络中频道的分隔

12.1.2.3 最大传输量（理论值）

如果使用 DS PHY 的信号处理技术，那么最大传输量将是所使用频率空间的函数。粗略而言，ISM 频段的频宽为 80-MHz。若展频率为 11，则最大位元率大概比 7Mbps 稍微多一些。不过，这是指使用一个频道的状况，而且产品必须使用时 77MHz 的振荡器来产生展频码。高频设备相当耗费电池的电力，而且使用这么高的编码率必须用掉整个频段，对可用频谱而言这简直是最糟的浪费。要达到较高的传输量，必须使用较复杂的技术。802.11b 只是稍微增加了讯符率，但它使用较复杂的编码技术，在传输量方面将可获得更大的进展。

12.1.2.4 干扰反应

比起跳频信号，经过直接序列调制的信号比较能够抵抗干扰。相关程序（correlation Process）让直接序列系统得以更有效率地解决窄频干扰的问题。每个位元（bit）使用 11 个缀片（chips），可以容许漏失或损毁几个缀片而不损及数据。至于直接序列系统的缺点，在于回应杂讯的能力并不会增加。相关器（correlator）在某种程度可以除去杂讯，但是如果干扰对频段的遮蔽率过高，将无法还原任何信号。图 12-8 显示了直接序列系统对干扰程度的响应。

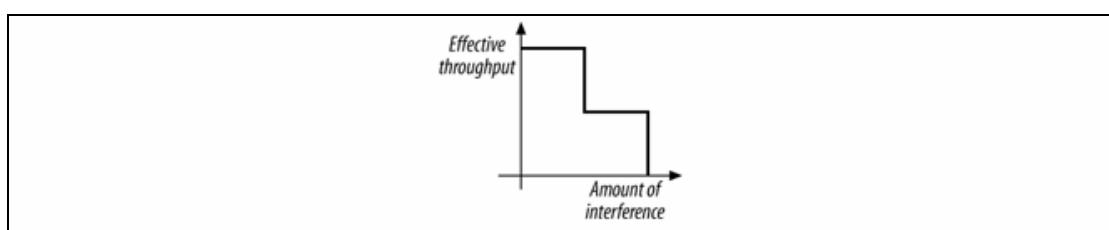


图 12-8 : DSSS 系统中传输量对干扰的响应

比起跳频系统，直接序列系统比较能够有效避免妨碍到频段优先用户（primary User）。经过直接序列处理后，信号比较宽，振幅也比较小，对传统窄频接收器而言有随机背景杂讯。如果同地区两位使用者所选用的直接序列频道相隔太近，使用上就会产生问题。一般而言，不待频段优先用户察觉，直接序列设备彼此干扰的问题已事先浮出水面。

12.2 差分相移键控 (DPSK)

差分相移键控 (Differential phase shift keying, 简称 DPSK) 是 802.11 直接序列系统的基础。正如其名，它是以传输信号的相位差对数据进行编码。在 PSK 中，波型的绝对相位并不重要，重要的是相位的相对变动。和频移键控（调频）一样，PSK 也可以抗拒干扰，因为干扰通常只会影响振幅。图 12-9 显示了两个相同的正弦波，彼此之间沿时间轴相互偏移。两个波形之相同点的偏移量即为相位差。

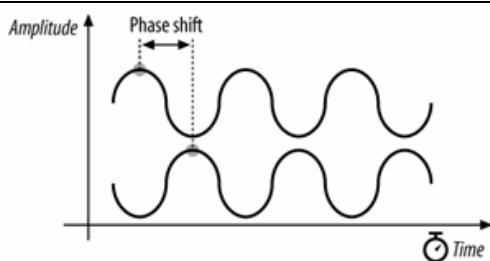


图 12-9：两个正弦波之间的相位差

12.2.1 差分二进制相移键控 (DBPSK)

形式最简单的 PSK 使用两种载波，它们彼此偏移半个周期。其中一个波称为参考波 (reference wave)，所对应的编码为 0。偏移半个周期的波，所对应的编码为 1。表 12-2 列出了可能的相位偏移。图 12-10 说明了如何藉助正弦波的相位差进行编码。

表 12-2：DBPSK 的相位偏移

讯符	相移
0	0
1	180 度 (π ?)

举个相同的例子，对字母 M (以二进制数值表为 1001101) 进行编码，相当于将时间轴区分为七个讯符时间，然后在每个讯符范围传送适当的偏移相位。图 12-11 说明了如何进行编码。首先，时间被切割为一系列讯符周期，每个周期由几个载波周期所构成。当讯符为 0，波形如同上一个讯符。如果讯符为 1，就会偏移半个周期。因此，传送 1 时载波会被「截断」，传送 0 时载波则会平顺地过滤到下一个讯符时间。

12.2.2 差分正交相移键控 (DQPSK)

和 2GFSK 一样，DBPSK 也受限于每个讯符只能编码一个位元。较先进的接收器与传送器可以使用一种称为差分正交相移键控（亦称四相位差调制，简称 DQPSK）的技术，以每个讯符编码数个位元。DQPSK 并非使用基准波与相位差为半个周期的偏移波，而是采用一个基准波与三个偏移波，每个波偏移四分之一周期，如图 12-12 所示，表 12-3 列出了所有可能的相位偏移。

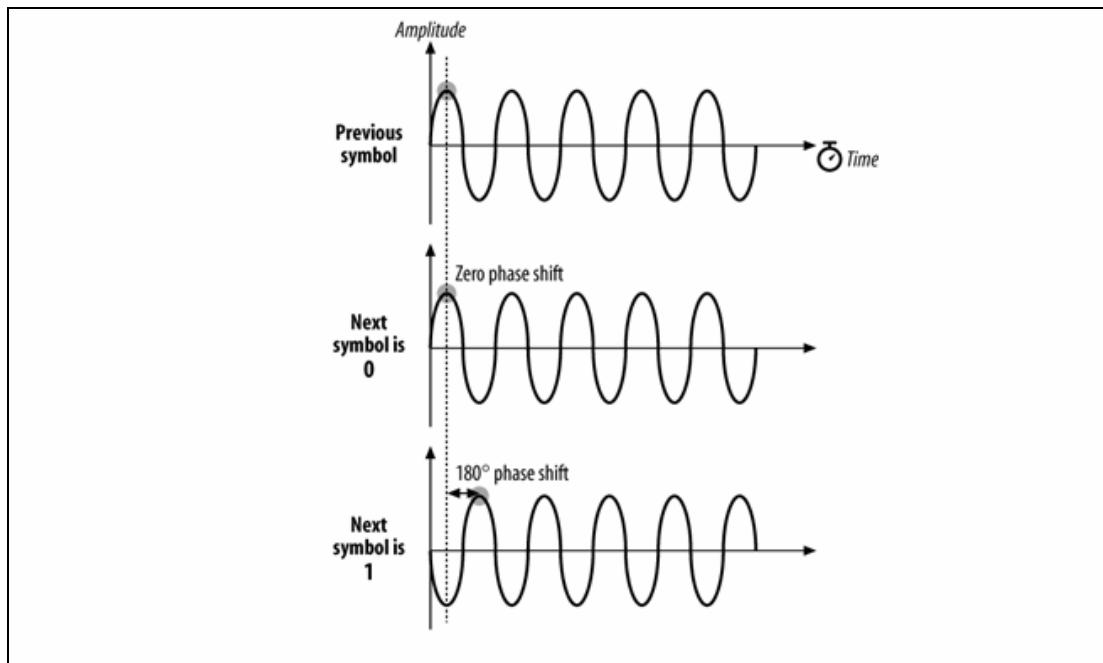


图 12-10: DBPSK 的编码方式

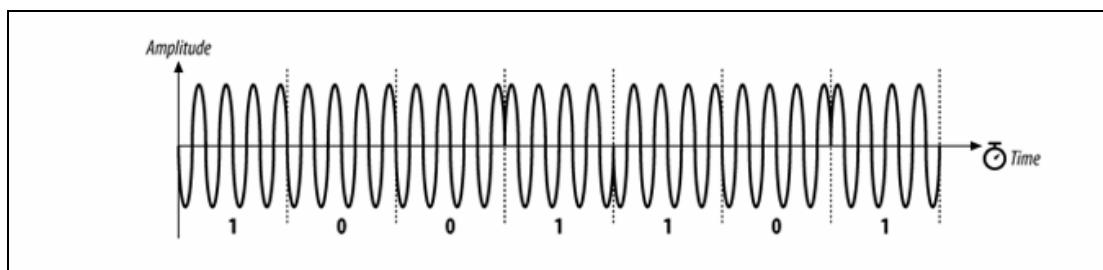


图 12-11: 以 DBPSK 对字母 M 进行编码

表 12-3: DQPSK 相位偏移

讯符	相相移 (相位差)
00	0
01	90 度 ($\pi/2$?)
11	180 度 (π ?)
10	270 度 ($\pi 3/2$ 或 $-\pi/2$?)

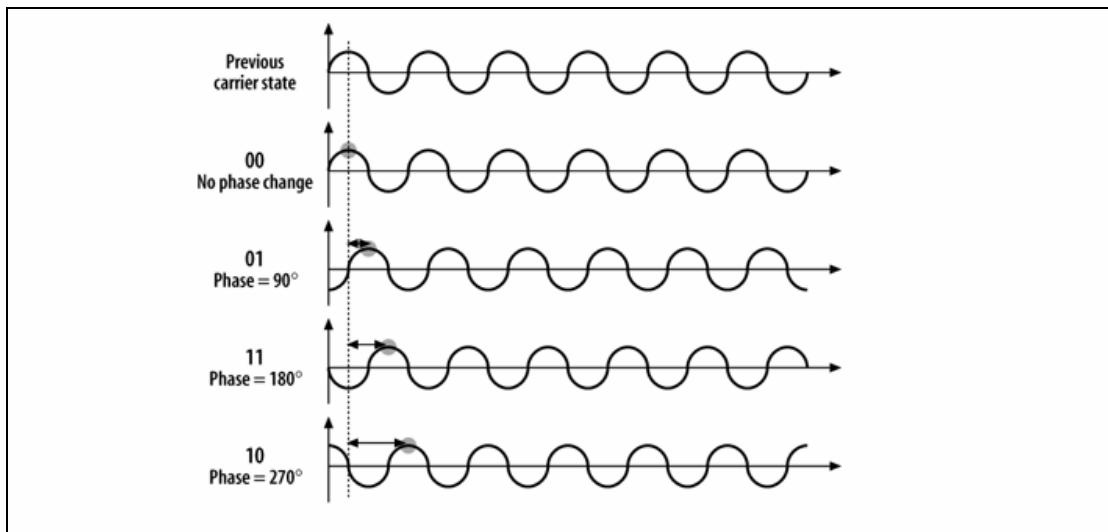


图 12-12: DQPSK 的编码方式

现在以 DQPSK 对 M 进行编码(图 12-13)。在 UTF-8 字集中, M 是以二进制字串 01001101 表示, 或者可以将它切割为四个等分, 每个等分由两位元的讯符组成, 亦即 01-00-11-01。在第一个讯符周期内, 相位偏移为 90 度; 为了清楚起见, 图所显示的偏移量是以纯粹的正弦波为基准。第二个讯符不会造成任何相位偏移, 因此波形并无任何改变。第三个讯符导致 180 度相位偏移, 因此在最高振幅与最低振幅之间造成剧烈落差。最后一个讯符导致相位偏移 90 度。

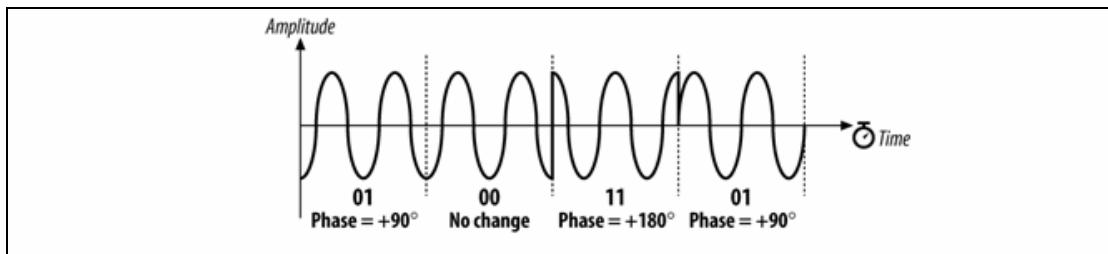


图 12-13: 以 DQPSK 对字母 M 进行编码

相较于 DBPSK (二阶编码机制), DQPSK 所具备的明显优势为, 四阶编码机制可以提供较高的传输量。采用 DQPSK 的代价则是, 如果多重路径干扰十分严重, 可能会导致无法使用。多重路径之所以发生, 是因为信号从传送端分路抵达接由端。每个路径的距离不同, 因此从每个路径所接收到的信号相对于其他路径彼此有时间差。时间差所造成的迟延是相位差编码机制的天敌。波前 (wavefront) 并未附上标签或者以不同颜色标示, 因此某个波前可能因为路径太长而迟到, 或者太晚传送而产生相位偏移。在多重路径干扰十分严重的环境下, DQPSK 会比 DBPSK 更早崩溃。

12.3 “原本的”直接序列物理层

物理层本身包含了两个元件。物理层收敛程序 (PLCP) 会在传送之前进行与物理层有关 (PHY-dependent) 的分封作业, 而实际搭配介质 (PMD) 则负责帧的实际传送。

12.3.1 PLCP 的分封 (framing) 与处理

DS PHY 所使用的 PLCP 会在 MAC 传来的帧之前加上标头，其中包含了六个栏位。以 ISO 参考模型的术语来讲，从 MAC 传来的帧属于 PLCP 服务数据单元（PLCP service data units，简称 PSDUs）。PLCP 的分封格式如图 12-14 所示。

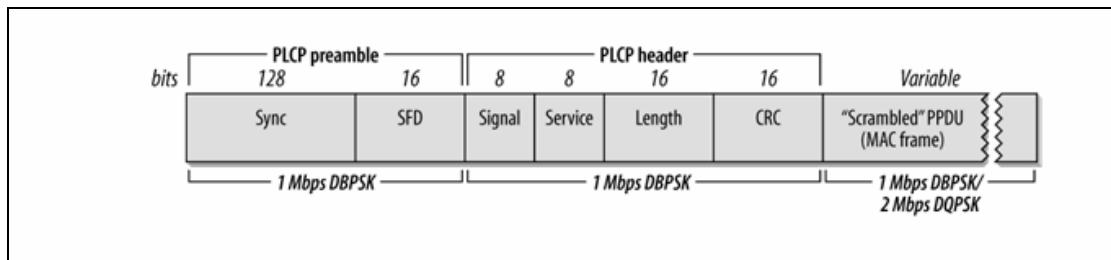


图 12-14：DS PLCP 帧的分封

FH PHY 使用数据白化器（data whitener）在数据传送之前进行随机化处理，不过白化对象只限于 PLCP 标头之后的 MAC 帧。DS PHY（直接序列物理层）也有类似的功能，称为搅码器（scrambler），只是其所搅码的范围，遍及整个直接序列帧，包括 PLCP 标头与同步信号。

同步信号 (preamble)

同步信号用来同步发射器与接收器，以维? 两者之间的计时关系。同步信号是由 Sync 以及 SFD 两个栏位组成。传送之前，同步信号会经过（直接序列搅码程序的）搅码。

Sync (同步)

Sync 栏位的长度有 128 个位元，每个位元值均为 1。和 FH PHY 不同的是，Sync 栏位传送之前会经过搅码。

Start Frame Delimiter (帧界定符号，简称 SFD)

SFD 可让接收器得知帧从何开始，就算同步位元在传送过程中有所遗漏。此栏被设置为 0000 0101 1100 1111，和 FH PHY 所使用的 SFD 有所不同。

标头 (Header)

同步信号之后紧跟着是 PLCP 标头。此标头包含了 PLCP 所使用的物理层专属参数，由五个栏位组成：一个用编码代表速度的信号栏位，一个服务识别码栏位（Service），一个长度栏位（Length）以及一个帧检查码（CRC）。

Signal (信号)

接收器可用 Signal 栏位来辨识所封装之 MAC 帧使用何种传输率。其值若不是设为 0000 1010 (0x0A)，代表 (1-Mbps) 作业，就是设为 0001 0100 (0x14)，代表 2-Mbps 作业。

Service (服务)

此栏位保留供示来使用，每个位元均设置为 0。

Length (长度)

此栏位设置为传送一个帧所需要的微秒数，以 16 位元的无号整数来表示。由最低效位元开始传送至最高效位元。

CRC (帧检查码)

为了防止标头经过无线链路时受损，传送端会根据前面四个标头栏位的内容计算出一个 16 位元的检查码。接收端在对帧做进一步处理之前，会先验证检查码。

Data 栏位所放置的内容并无任何限制。任何数据均包含了一长串连续的 0 或 1，这使得数据看起来不是那么随机。为了让所要传送的数据比较像是随机的背景杂讯，**DS PHY** 会以一种多项式搅码机制，将成串的 1 或 0 从所传送的数据串流中移除。

12.3.2 DS PMD 附属层

PMD（实际搭配介质）是相当复杂与冗长的规格，其中包含两种数据率（1.0 与 2.0 Mbps）相关规定。图 12-15 显示了 802.11 直接序列网络收发器的一般设计。

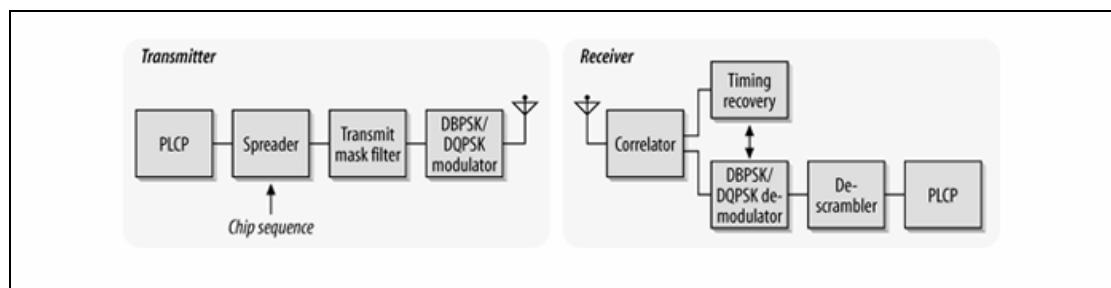


图 12-15：直接序列收发器

12.3.2.1 以 1 Mbps 进行传输

就低数据率而言，DS PMD 可用 1.0Mbps 的速率传送数据。来自 MAC 的帧加上 PLCP 标头后，即会对整个单元进行搅码。所产生的位元序列使用 DBPSK 以每秒一百万个讯符的速度进行编码，然后通过实体界面传送。和 FH PMD 一样，DS PMD 有最低功率的限制。如果要符合管制要求，可将功率设置为 100mW。

12.3.2.2 以 2.0 Mbps 进行传输

和 FH PHY 一样，2.0Mbps 传输使用了两种编码机制。PLCP 同步信号和标头使用 DBPSK 以 1.0Mbps 速度进行传送。虽然使用较低速率传送标头会降低有效传输量，不过 DBPSK 却比较能够容忍杂讯与多重路径干扰。同步信号与标头传送完毕后，PMD 就会切换为 DQPSK 调制，开始提供 2.0-Mbps 的服务。和 FH PHY 一样，大多数实作 2.0-Mbps 传输率的产品，可以在检测到干扰时切换回低速的 1.0-Mbps 服务。

12.3.3 DS PHY 的 CS/CCA

802.11 允许 CS/CCA（载波检测/亲朋好淨空频道评估）功能以下列其中一种模式运作：

Mode 1

当能量超过能量检测（energy detection，简称 ED）门槛，就会回报介质处于忙碌状态。ED 门槛因传输功率而异。

Mode 2

采用 Mode 2 的实作产品必须搜寻真正的 DSSS 信号。如果检测到，就算信号 低于 ED 门槛，亦会回报该频道处于忙碌状态。

Mode 3

Mode 3 结合 Mode 1 与 Mode 2。所检测到的信号必须具备足能量，才会向上一层回报频道处于忙碌状态。

一旦频道被视为忙碌，在预定传输的时间内就一直处于忙碌状态，就算信号已经遗失。传输持续时间由 Length 栏位。回报介质是否忙碌必须非常迅速。一旦在竞争期间的开始检测到信号，CCA 机制就必须报告介质处于忙碌，直到这段时间结束。之所以必须设置较高的交能要求标准，是因为一旦工作站在竞争延迟结束后开始进行传送，就得持续掌握介质，其它工作站必须暂缓访问介质，直到帧传送完毕。

12.3.4 DS PHY 的特性

表 12-4 显示了 DS PHY 中几个参数值.除了表中所列的标准参数，DH PHY 尚有一些参数可供调整，让 802.11 直接序列系统中各部分的迟延保持均衡.其中包括 MAC 、PLCP、收发器的迟延变数，以及收发器这电子零件个别变异的相关变数。另外值得注意的是，同一区域中所有直接序列网络的整体传输量（total aggregate throughput）较该区所有非重叠的跳频系统为低。整个传输量乃是彼此不相重叠频道数之函数。在北美与欧洲大部分地区，每个区域同时间只能够容纳三个直接序列网络。如果每个网络的传输率为 2-Mbps，且协议的效能可让使用者的数据传输量达到额定速率的 50%，该区的总传输量即为 3- Mbps，远低于跳频系统的整体传输量。

表 12-4：DS PHY 参数

参数	值	备注
槽位时间 (Slot time)	20us	
SIFS 时间	10us	SIFS 可用来推衍出其他的帧间隔值 (DIFS、PIFS 以及 EIFS)。
竞争期间的大小 (Contention window size)	3 至 1023 个槽位	
同步信号持续时间 (Preamble duration)	144us	同步讯符系以 1 MHz 速率传输，因此传输每个讯符需时 1us；144 个位元则需要 144 个讯符时间。
PLCP 标头持续时间 (PLCP header duration)	48us	PLCP 标头有 48 个位元，因此需要用到 48 个讯符时间。
最大 MAC 帧 (Maximum MAC duration)	4 至 8, 192 个位元组	
最低接收灵敏度 (minimum receiver sensitivity)	-80dBm	
邻频拒斥 (Adjacent channel rejection)	35dB	参见量测注意事项。

和 FH PHY 一样，DS PHY 中有些属性亦可供厂商调整，让系统各部分的迟延时间得以保持均衡。其中包括 MAC、PLCP、收发器的迟延变数，以及收发器之电子零件中个别变异的相关参数。

12.4 互补码调制（CCK）

802.11 直接序列系统采用了每秒一千一千万的缀片率（11 million chips per second）。原本 DS PHY 将缀片串割分为一系列 11 位元的 Barker words，每秒传送一百万个 Barker words。每个 word 当中，会根据所使用的是 1.0 Mbps 或 2.0 Mbps 数据率，分别编码一或两个位元。要达到更高的数据率，以及在商业上具有实用性，就必须在每个讯符当中承载更多信息，而不只是一或两个位元。

直接进行相位差编码无法在每个编码字（code word）中携带多少位元。DQPSK 所使用的接收器，必须能够分辨四种周期的相位差。要增加每个讯符所能承载的位元数，必须能够处理更细微的相位偏移，例如八种或十六种周期偏移（cycle shift）。遇到多重路径干扰时，检测更细微的相位偏移更是困难，而且还必须使用更复杂（因此也更昂贵）的电子零件。

IEEE802.11 工作小组并未继续采用直接相位差编码，转而使用不同的编码方式。互补码调制（Complementary code keying，简称 CCK）将缀片串流（chip stream）割分为一系列以 8 位元构成的编码讯符（code symbol），因此底层所使用的传输率乃是每秒传送 1.375 百万个编码讯符。CCK 采用了复杂的数学转换函数，可以使用若干 8-bit 序列，在每个编码字中编码 4 或 8 个位元，因此数据总传输量 5.5 Mbp 或 11 Mbps。此外，CCK 所使用的数学转换函数，可以让接收器轻易辨别不同的编码，就算遇上干扰或多重路径衰落的情况。图 12-16 显示了 CCK 所使用的编码讯符。它十分类似低速直接序列物理层所使用的 chipping process（缀体程序），差别在于编码字部分是由数据本身推衍而来，并未使用类似 Barker word 之类静态而具重复性的编码字。

用于低速直接序列物理层的 Barker 展频方式，是使用静态编码将信号于可用频段展开。CCK 使用编码字（code word）来承载信息以及展开信号。准备这些复杂的 8 位元为一组的编码字，必须使用一些不同的相位角（phase angles）。

12.5 高速直接序列物理层（HR/DSSS PHY）

为了与原本的直接序列物理层有所区别，以 11Mbps 运行的高速物理层被简称为 HR/DSSS。和前者一样，HR/RSSS 分成两个部分。PLCP 负责准备传送所需要的帧，PMD 则负责将之转换为无线电波。

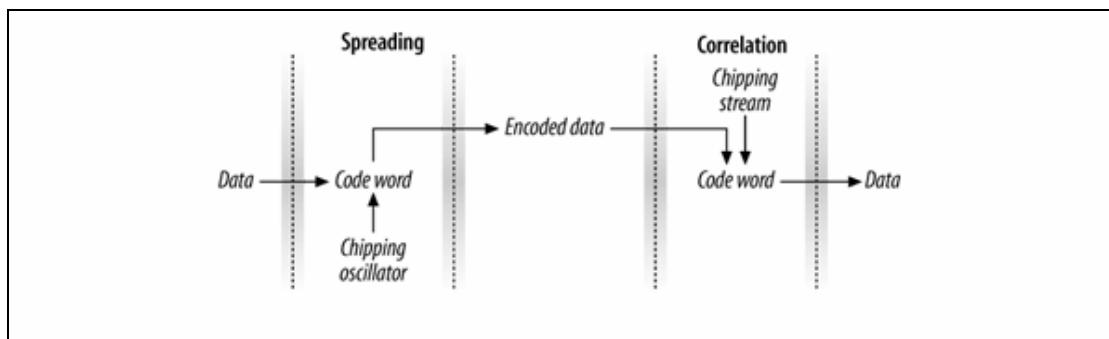


图 12-16: CCK 所使用的编码讯符

12.5.1 PLCP 分封 (Framinf) 与搅码 (scrambling)

原本的直接序列物理层所使用的长标头会大幅降低效能。802.11 MAC 要求每个数据帧均得到正面回应，而 192 微秒的同步信号远远大于 MAC 的回应信号。以 11 Mbps 的数据率而言，传送一个大小为 1500 位元组的帧并得到 MAC 正面回应，同步信号与 PLCP 封装标头就占用了其中 25% 的时间。开发新的物理层时，802.11b 的设计人员采用一种新的“短”帧格式，因此在改善协议效能的同时也提升了传输量。使用短标头可将同步信号与 PLCP 分封所造成的负担削减至 14%。虽然负担仍在，但已有大幅改善。图 12-17 显示了 802.11 所规范的 PLCP 帧格式，802.11b 刚问世时，并非所有设备均支持短标头，因为当时 2 Mbps 直接序列设备的设备量相当大。目前，几乎所有网络卡均已支持短同步信号，大多数基站也以它为预设值。

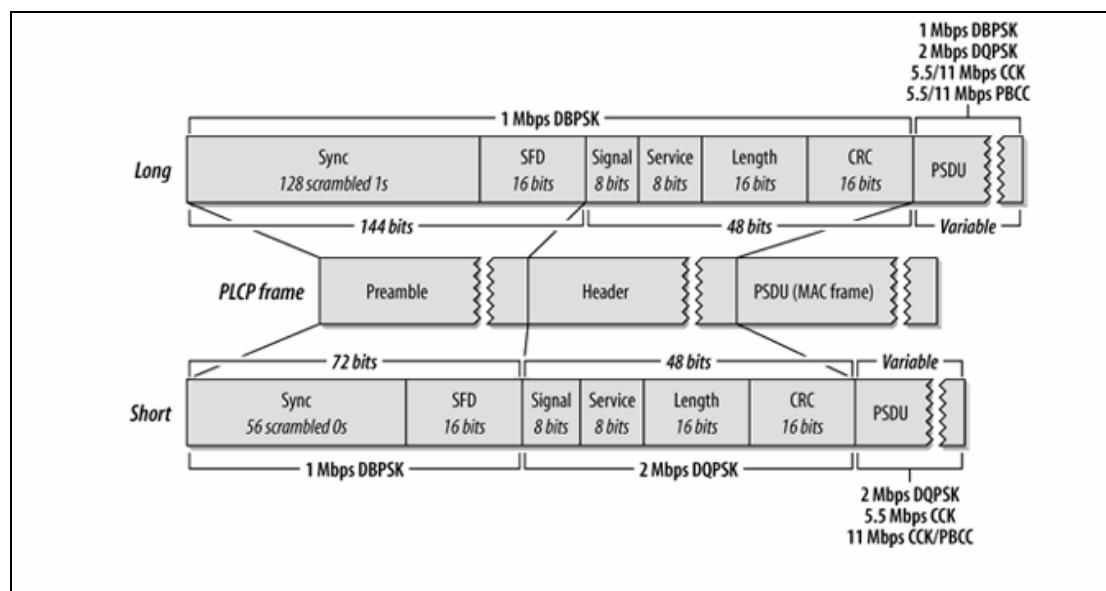


图 12-17: HR/DSSS PLCP 的帧格式

当然，除非所有工作站均提供支持，否则短帧就无法使用。为了避免支持短帧的网络消失，802.11b 规定，回覆 Probe Request (探查要求) 主动扫描的工作站，必须使用相同的 PLCP 标头。如果某部只支持长 PLCP 标头的工作站送出 Probe Request，基站就必须以长标头加以回应，就算该 BSS 设置上使用的是短标头。

Preamble (同步信号)

帧始终同步信号，同步信号由 sync 与 SFD 栏位组成。此同步信号会使用 DBPSK 并以 1.0 Mbps 的速率进行传送。

LongSync

Long Sync 栏位由 128 个内容为 1 的位元所组成。不过在传送之前，此栏位会先经过搅码器处理，因此数据内容会有所不同。高速系统使用特定值做为搅码函数的乱数基准 (seed)，不过也可以回溯相容，支持不指定乱数基准的旧式系统。

ShortSync

Short Sync 栏位由 56 个内容为 0 的位元所组成。和 Long Sync 一样，这个栏位会先经过搅码器处理。

Long SFD

Long Preamble 以 SFD 来宣告 Sync 标位的结束。在 Long PLCP 中，SFD 序列为 1111 0011 1010 0000。和所有 IEEE 规格一样，实际的传送顺序是最低效位元 (least-significant bit) 优先，因此该字串是由右至左传送。

Short SFD

为了避免与 Long SFD 混淆，Short SFD 的值正好相反，亦即 0000 0101 1100 1111。

同步信号之后为 PLCP 标头。它是由 Signal、Service、Length 以及 CRC 标位所构成。长标头会使用 DBPSK 以 1.0 Mbps 速率进行传送。不过，短标头的目的是为了减少标头传送时的负担，以及所需要的时间，因此会使用 DQPSK 以 2.0Mbps 速率进行传送。

Long Signal

Long Signal 标位用来指示被封装之 MAC 帧所使用的速度与传输方式。目前，802.11b 定义了四个数值，其所对应的 8 位元编码如表 12-5 所示。

表 12-5: Signal 标位

速度	值（最高效位元至最低效位元）	十六进位值
1 Mbps	0000 1010	0x0A
2 Mbps	0001 0100	0x14
5.5 Mbps	0011 0111	0x37
11 Mbps	0110 1110	0x6E

Short Signal

Short Signal 标位用来指示被封装之帧所使用的速度与传输方式，不过标准中只定义了三个值。Short preamble 只能用于 2.Mbps、5.5Mbps 以及 11Mbps 的网络。

Service

802.11 初版的标准原本是将如图 12-18 所示的 Service 标位留待未来使用，不过 802.11b 随即将它应用于高速延伸服务。首先，Length 标位以微秒为单位记录封装帧所需要的时间。传输速度高于 8.Mbps 时，这个值就有些暧昧不明。因此，Service 标位所使用的八个位元被用来将 Length 标位扩充为 17 个位元。其中第 3 个位元 (clock lock) 用来显示该 802.11b 产品是否使用经锁定的时脉 (locked clock) 时脉的锁定 (clock locking) 是指传输频率与讯符时脉使用同一振荡器。第 4 个位元 (Modulation) 用来显示封包所使用折编码类型，0 代表 CCK，1 代表 PBCC。其它保留位元必须设置为 0。Service 标位的传送是由左至 (b0 到 b7)，不论 PLCP 帧格式的长短，均是如此。（802.11g 做了进一步的改变，相关细节将于第十四章探讨。）

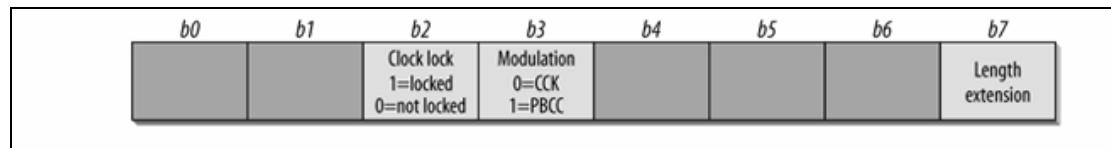


图 12-8: HR/DSSS PLCP 标头的 Service 标位

Length

Length 栏位在 PLCP 短帧与长帧格式中完全一样，代表传送经过封装的 MAC 帧所需要的微秒数。802.11b 标准以近两页的篇幅描述如何计算 **Length** 值，不过这些细节已经超出本书的范围。

CRC

CRC 栏位在 PLCP 短帧与长帧格式完全一样。传送端会以 **Signal**、**Service** 以及 **Length** 栏位计算 **CRC** 检查码。接收端可以利用 **CRC** 值来确保所收到的标头未经更动，也未在传输过程中损毁。**CRC** 的计算会在数据搅码前进行。

HR/DSSS PHY 所使用的数据搅码程序几乎与原来的 DS PHY 一样。惟一的差别，在于其所使用的搅码函数采用了特定的乱数基准值（**seed**）。PLCP 短帧与长帧分别使用了不同的乱数基准。

12.5.2 HR/DSSS PMD

与 FH PHY 不同，DS PHY 只有一种 PMD 规格。一般收发器的设计如图 12-19 所示。

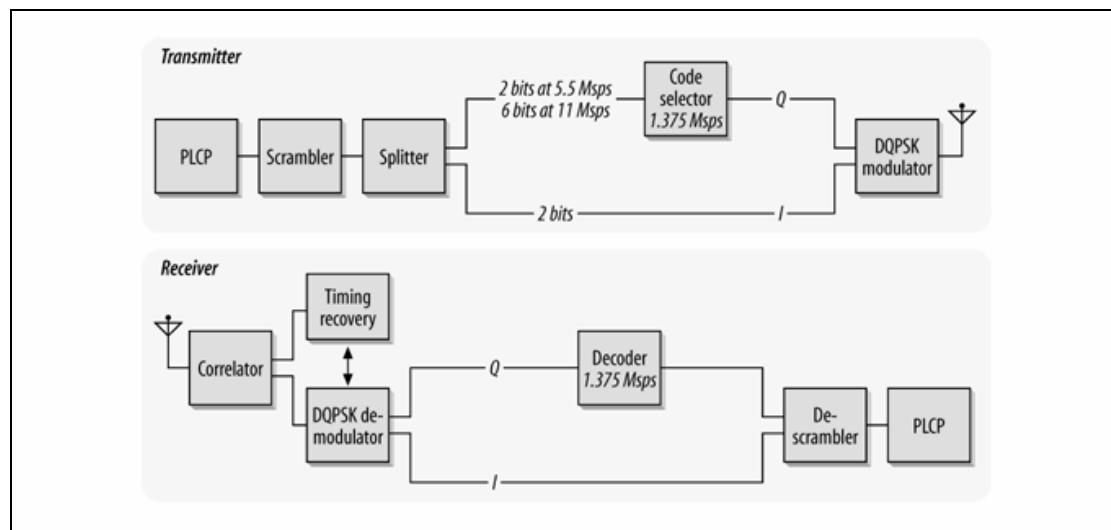


图 12-19：HR/DSSS 收发器

12.5.2.1 以 1.0 Mbps 或 2.0 Mbps 进行传输

为了确保能够和现有的 802.11 直接序列扩频体相容，HR/DSSS PHY 可用 1.0 Mbps 或 2.0 Mbps 的速率进行传输。较慢的传输方式与本章之前所描述的低速直接序列物理层没有两样。任何低速传输均须使用长标头。

12.5.2.2 以 CCK 进行 5.5 Mbps 的传输

高速传输是以 DQPSK 相移键控（相位差调制）技术达成。DQPSK 在每个讯符周期可以传送两个位元，这两个位元可编码成相应的四种相位偏移之一。如果使用 CCK，讯符字（symbol word）本身可以承载更多信息。5.5-Mbps 传输在每个导符中可编码四个数据位元。其中两个位元使用传统的 DQPSK，另外两个位元则是通过编码字（code word）的内容加以承载。图 12-20 显示了整个程序。

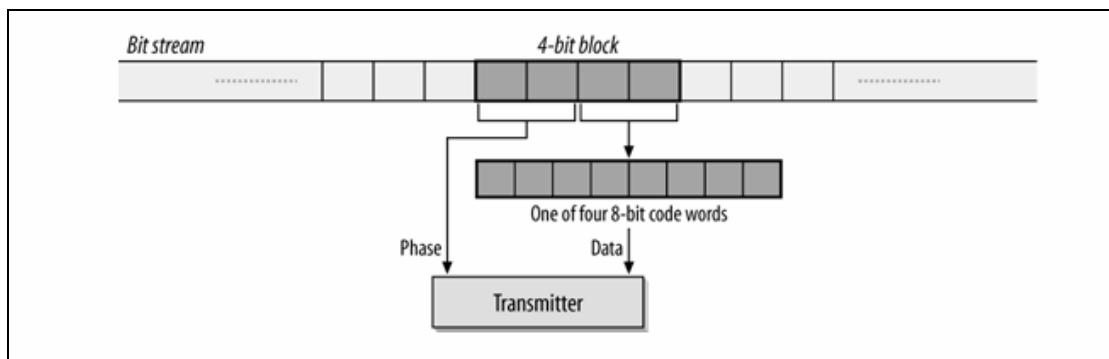


图 12-20：以 5.5Mbps 进行 802.11b 的传输

- PLCP 帧所包含的 MAC 帧，被切割成一连串 4-bit 区块（block）。每个 4-bit 区块再进一步被划分为两个 2-bit 区段（segment）。
- 第一个 2-bit 区段是以前后两个讯符之间的 DQPSK 相位差进行编码（表 12-6）。偶数与奇数讯符之所以采用不同的相位差，纯粹是为了技术上的需要。讯符编号从 0 开始，并由第一个 4-bit 区块起算。

表 12-6：讯符间的 DQPSK 相位偏移

位元样式	相位角（偶数讯符）	相位角（奇数讯符）
00	0	π
01	$\pi/2$	$3\pi/2$
11	π	0
10	$3\pi/2$	$\pi/2$

- 第二个 2-bit 区段，可用来将「目前讯符」对映到四种编码字（表 12-7）其中之一。这四种编码字可通过 802.11 标准在 18.4.6.5 款所记载的数学函数推演得知。

表 12-7：Mbps 编码字

位元样式	相位角（偶数讯符）
00	i, 1, i, -1, i, 1, -i, 1
01	-i, -1, -i, 1, 1, 1, -i, 1
10	-i, 1, -i, -1, -i, 1, i, 1
11	i, -1, i, 1, -i, 1, i, 1

12.5.2.3 以 CCK 进行 11 Mbps 的传输

为了支持 11Mbps 的传输，在每个讯符中必须编码八个位元。和其他技术一样，头二个位元是以目前所发送的讯符与前一个讯符之间的相位差来进行编码。其他六个位元则是使用 CCK。图 12-21 显示了整个程序。

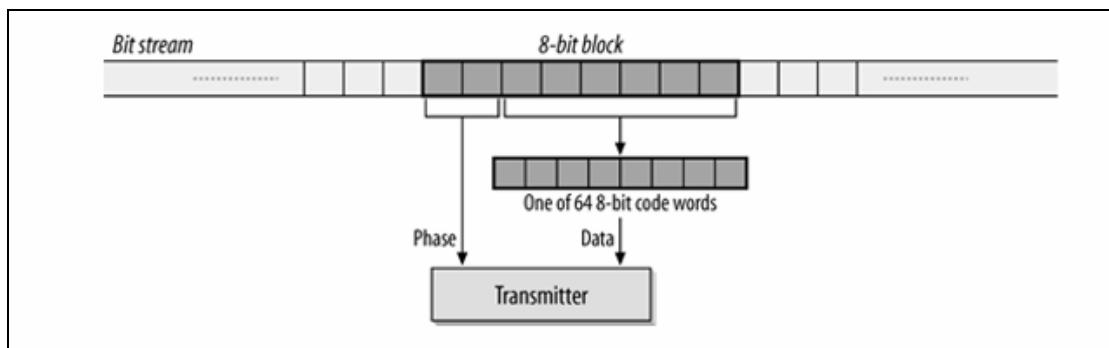


图 12-21：以 11Mbps 进行 802.11b 的传输

- PLCP 帧所包含的 MAC 帧，被切割成一连串 8-bit 区块（block）。每个 8-bit 区块再进一步划分为四个 2-bit 区段（segment）。
- 第一个 2-bit 区段是以前后两个讯符之间的 DQPSK 相位差进行编码。和 5.5-Mbps 一样，偶数与奇数讯符之所以采用不同的相位差，纯粹是为了技术上的需要。讯符编号从 0 开始，由第一个 8-bit 区块起算。此相位偏移与 5.5-Mbps 传输所使用的完全相同。
- 其余六个位元被分为三组。每一组均对应到表 12-8 所列的相位角，并据以推衍出编码字。

表 12-8：11-Mbps 传输所使用的相位角编码

位元样式	相位角
00	0
01	$\pi/2$
10	π
11	$3\pi/2$

举例而言，试问如何将位元序列 0100 1101 转换为复合码（complex code），以便在 802.11b 网络进行传输。第一对位元为 01，以目前与上一个讯符之间的相位差进行编码。在 MAC 帧中，如果该讯符为偶数讯符，相位偏移为 $\pi/2$ ，否则，偏移量为 $3\pi/2$ 。（MAC 帧中的讯符编号由 0 开始，所以帧的第一个讯符为偶数。）其余六个位元区为三组，每组包含两个位元：00、11 与 01。这三组用来对应相位角与编码字。下一个步骤是将相位角转换为用来传输的复合码。

12.5.2.4 净空频道评估

和原本的 DS PHY 一样，高速的版本在 CS/CCA 作业模式上也有三种选择。所有这些直接序列 CCA（净空频道评估）模式均来自同一份列表。Mode 1 与 DS PHY 的 CCA Mode 1 相同，Mode 2 与 Mode 3 只用于原本的 DS PHY。Mode 4 与 Mode 5 则是 HR/DSSS 专属的 CCA 模式。

Mode 1

一旦超越能量检测（ED）门槛，介质就会被视为处于忙碌状态。ED 门槛因所使用的传输功率而异。典型的直接序列系统亦会用到此模式。

Mode 4

实作上，**Mode 4** 是有来找寻直实信号。一旦被触发，实作**Mode 4 CCA** 的产品会启动一个 3.65 ms 的计时器，然后开始倒数。如果在计时器逾时之前，并未发现有效的 HR/DSSS 信号，介质就将被视为处于闲置状态。3.65ms 相当于以 5.5 Mbps 传送最大可能帧（the largest possible frame）所需要的时间。

Mode 5

Mode 5 结合了 **Mode 1** 与 **Mode 4**。所检测到的信号必须达到足够的能量，才会向上层协议回报频道处于忙碌状态。

一旦频道被视为忙碌，在预定传输的时间内，便会一直处于忙碌状态，就算信号已经遗失。该频道会被视为忙碌，直到 Length 栏位所记载的时间过去。如果检测到了第二个 PLCP 标头，找寻有效信号的产品实作，有可能会不管此项要求。

12.5.3 802.11b PHY 的非必要功能

802.11b 包含了两种非必要的物理层功能，两者均未受到广泛使用。有人提议使用二进制封包？旋编码（Packet Binary Convolutional Coding，简称 PBCC）来达到 11Mbps 的传输率，不过并未受到广泛使用。有些建议书提议在未来版本中采用 PBCC，不过这些建议书在 2001 年已被否决。

第二种称为机动跳频（channel agility），它被设计来协助网络避免干扰。机动跳频会定期变更中心频道，以此避免干扰。机动跳频从未受到广泛使用因为它并不是特别有用。接收器在干扰出现时跳至其它频道可以提升一些传输量，但是这不如找出干扰源予以移除，或者重新配置频道来得有效率。

12.5.4 HR/DSSS PHY 的特性

表 12-9 列出了若干 HR/DSSS PHY 的参数值。和 DS PHY 一样，HR/DSSS PH 尚有一些参数可供调整，以补偿实际系统各部分所产生的迟延。

表 12-9：HR/DSSS PHY 参数

参数	值	备注
最大 MAC 帧长度	4095 个位元组	
槽位时间（Slot time）	20us	
SIFS 时间	10us	SIFS 可用来推衍出其他的帧间隔值（DIFS、PIFS 以及 EIFS）。
竞争期间的大小（Contention window size）	31 至 1023 个槽位	
同步信号持续时间（Preamble duration）	144us	同步讯符系以 1 MHz 速率传输，因此传输每个讯符需时 1us；144 个位元则需要 144 个讯符时间。

参数	值	备注
PLCP 标头持续时间 (PLCP header duration)	48us	PLCP 标头有 48 个位元，因此需要用到 48 个讯符时间。
最低敏感度 (minimum receiver sensitivity)	-76Bm	
邻频拒斥 (Adjacent channel rejection)	35dB	参见量测注意事项。

另外值得注意的是，HR/DSSS 网络在某个区域所能提供的整体传输量，仍然低于非重叠的跳频网络。整体传输量是彼此不相重叠之频道数的函数。在北美与欧洲大部分地区，每个区域同时间可以容纳三个 HR/DSSS 网络。如果每个网络的最高传输率为 11Mbps，假定承载数据的传输量为 50%，该区的总传输量即为 16.5 Mbps 【编注：11x3x0.5】。

第13 章 802.11a 与 802.11j

5-GHz OFDM PHY

2.4 GHz ISM 频段十分拥挤，而且经常充斥著非 802.11 信号。为了达到更高的传输率 802.11 工作小组制定出另一种物理层标准，使用 5 GHz 附近的免照频谱。除了还有很多空间，目前也很少有设备使用这个频段。

802.11a 早在 1999 年就已经成为标准，但是经过很长一段时问产品才开始出现。802.11a 硬件最早出现在 2001 年底。目前，Atheros Communications 算是最著名的 802.11a 芯片组厂商。不论是在形式或功能方面，802.11a 和其他类型的无线网卡均十分类似。大多数网卡采用 CardBus 界面，不过目前比较常用的反而是其他造型(form factor) 的网卡。通常数据率愈高传输距离就愈短，但一般来说，802.11a 不论在数据率或传输距离，都还算能够与 802.11b 相提并论。

起初，802.11a 是专门针对美国所做的设计，使用 5-GHz 的国家免照信息基础设施 (Unlicensed National Information Infrastructure，简称 U-NIT) 频段。802.11a 成功打开美国市场后，其他管制当局便着手制定相关法规，允许使用 802.11a。在 802.11 工作小组的协助下，最后针对欧洲制定了 802.11h (参见第八章)，针对日本制定了 802.11 市。

注：拜 Horace Greeley 之赐，这句话才广为流传。

本章首先会介绍 OFDM 的基础知识。OFDM 的做法是将较大的频道切割成数个子频道道。这些子频道随后会以平行的方式加以利用，以便达到更高的传输率。我预料许多读者会跳过本章前面的部分，若不是因为这些读者对 OFDM 已经相当熟悉，就是因为他们只对如何使用频段，以及 PLCP 如何包装所要传送的帧感到兴趣。

13.1 正交分频多工 (OFDM)

802.11a 是以正交分频多工 (orthogonal frequency division multiplexing，简称 OFDM) 为基础。OFDM 的技术并不算新。此技术的基本架构完成于 1960 年代末期，而美国则在 1970 年一月批准专利，专利号码为多 3488445。近年来，DST(HDSL、VDSL 与 ADSL) 与无线数据应用对 OFDM 重新燃起兴趣，主要是出现了更好的信号处理技术，使之更为实际可行。[注] 然而，在做法上，OFDM 的确不同于其他近年来出现的编码技术，如分码多工 (code division multiple access，简称 CDMA)。CDMA 通过复杂的数学转换，以单一载波 (single carrier) 进行多路传输，OFDM 则是以多重副载波 (multiple subcarriers) 进行单一传送。CDMA 分码所使用的数学运算，远比 OFDM 复杂得多。

OFDM 设备会将一个较宽的频道 (frequency channel) 切割成几个子频道 (subchannel)。每个子频道均用来传输数据。所有这些「较慢」的子频道随后会被多工的方式组合成「较快」的频道。

13.1.1 载波多工

当网管人员请使用者对网络设备提供建议时，最常得到的反应就是希望网络的速度能够更快一些。数据传输的需求与日俱增，这带动了一些致力于提升传输速度的技术发展。在性质上，OFDM 采取类似 Multilink PPP 的做法：当一条链路不够使用，就增加几条平行的链路来处理。

OFDM 和旧式分频多工(FDM) 技术关系十分密切。两者均是将可用频宽切割为许多称为载波 (carrier) 或副载波 (subcarrier) 的片段，同时将这些载波当成个别频道进行数据传输。藉由这些副载波的平行运用，以及对这些副载波的数据进行多工处理，OFDM 可以有效提升传输量。

注：由于对 OFDM 感到兴趣的人并不多。因此参考数据也相当贫乏。对其数学背景有兴趣的读者，可以参考 Richard van Nee & Ramjee Prasad 所合著之《(OFDM for Wireless Multimedia Applications)》(Artech House, 2000) 一书。

传统的 FDM 被广泛运用于第一代移动电话，做为无线频道的配置方式。每个用户会被分配到一个专用频道，频道间使用防护频段(guard band) 以确保某个频道所溢出的信号不致干扰到相邻频道的用户。图 13-1 显示了传统 FDM 所采取的做法。

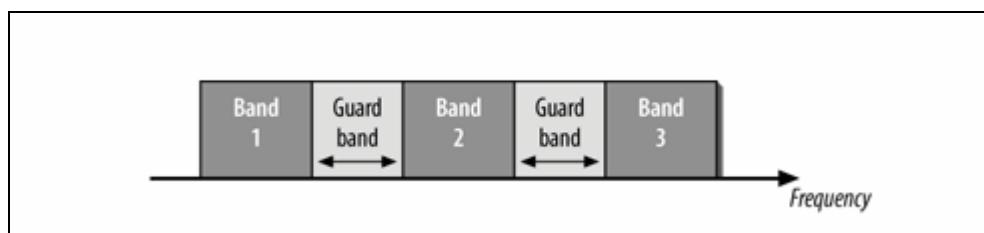


图 13-1：传统的 FDM

传统 FDM 的问题在于防护频段不仅浪费频宽，也会减少可用资源 (capacity)。为了避免无用的防护频段浪费传输资源，OFDM 使用彼此重叠，但不会互相干扰的频道。图 13-2 显示了传统 FDM 与 OFDM 之间的差异。

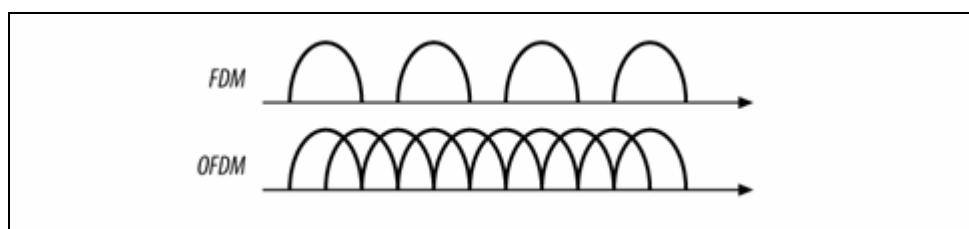


图 13-2：FDM 与 OFDM 的差异

之所以能够使用相互重叠的载波，是因为定义了副载波，因此可以轻易区分彼此。能够区别副载波，关键在于它使用了一种复杂的数学关系，称为正交性 (orthogonality)。

13.1.2 正交性的意义（不使用微积分）

正交 (orthogonal) 这个数学名词，源自 *orthos* 这个希腊文，意思是直接、正确或者真实。在数学上，*orthogonal* 这个单字则是用来描述彼此独立的项目。只要对信号进行光谱分解

(spectral breakdown)，就很容易从频域(frequency domain)当中了解正交性的意涵。OFDM之所以能够运作，是因冯所选用的副载波频率，其波形丝毫不受其他副载波影响。图 13-3 显示了一种正交性的常见观点。图 13-3 中，信号被区分为三个副载波。每个副载波的波峰均做为数据编码之用，如图 13-3 上方以圆点标示者。这些副载波之间经过刻意设计，彼此之间保持正交关系；注意每个副载波的波峰，此时其他两个副载波的振幅均为 0。

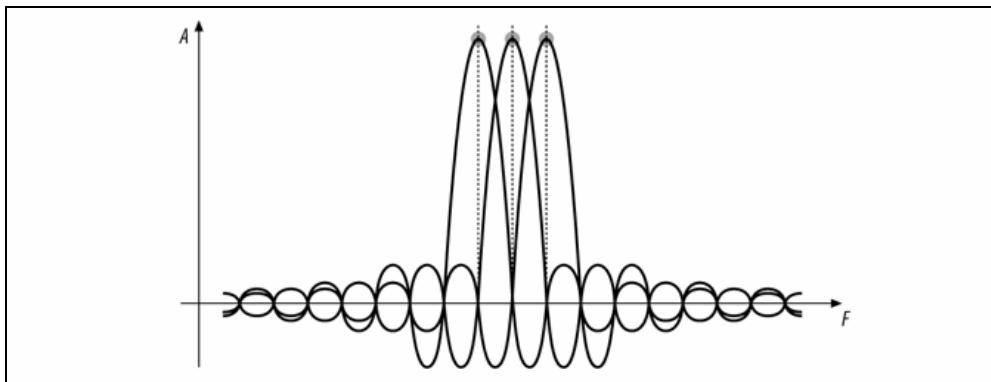


图 13-3：频域中的正交性

OFDM 会从每个子频道取得编码信号，然后使用反向快速傅利叶转换 (inverse fastFourier transform, 简称 IFFT)，利用每个子频道的振幅产生一个组合波形(composite waveform)。OFDM 接收器随后可以使用快速傅利叶转换(FFT)，从所收到的波形中取出每个副载波的振幅。

13.1.3 防护时间

第十二章讨论物理层时有提及讯符间干扰 (inter-symbol interference, 简称 ISI) 是接收器面临的主要问题 (图他斗 4)。当不同路径之间的迟延差距过大，导致后来所发送的数据副本混叠先前所收到的数据时，就会发生讯符间干扰。

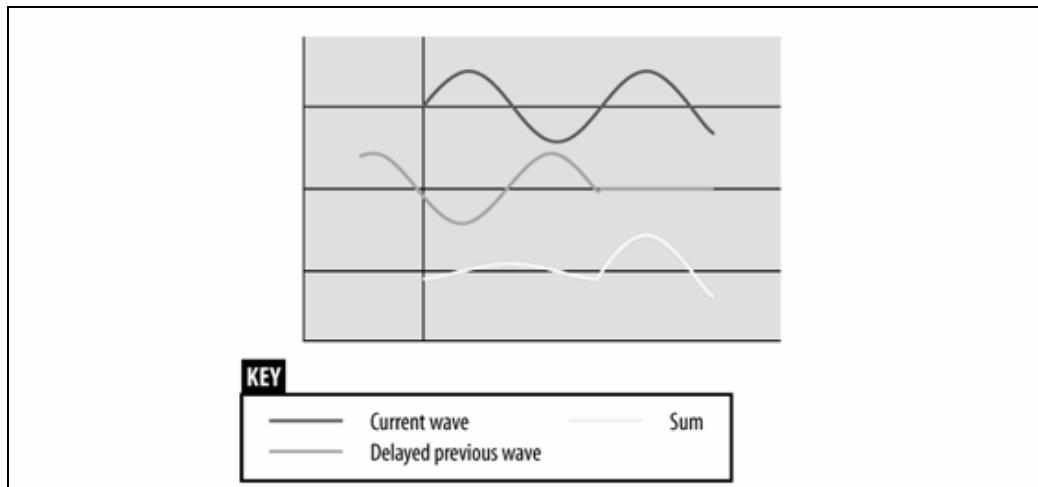


图 13-4：重新检视 ISI

Fourier 分析、Fourier 转换以及信号处理

Fourier (傅利叶) 转换通常被称为「信号处理的瑞士刀」。信号处理通常是以构成频率的元素定义行为。不过，接收器主要在处理依时间变动的信号振幅。**Fourier** 转换是一种数学运算，它会将波形折解成许多组成元件。**Fourier** 分析所处理的则是依时间变动的信号，将之转换为一组构成该信号的频域元素。

信号处理应用程序通常也需要用到反向运算式。已知一组频率元素，这些应用程序就可以利用这些频率元素重建出组合波形。从频域中的已知频率要素重建组合波形的数学运算，即为 **Fourier** 转换。

严格来讲，**Fourier** 分析被应用在类似物理学教科书中所描述的平滑曲线。运用在一组离散数据点时，必须使用 **Fourier** 转换的亲戚，称为离散 **Fourier** 转换(discrete Fourier transform，简称 DFT)。和 **Fourier** 转换一样，DFT 的反向运算称为 IDFT (反向 DFT)。

DFT 是一种运算密集的程序，其 order (复杂度) 为 N^2 ，亦即 DFT 的执行时间与数据点数目的平方成正比。不过，如果资料点的数目是 2 的偶乘方 (evenpower)，就可以利用一些速算法，将复杂度降到 order $N \log N$ 。如果要处理的资料量相当大，所降低的复杂度可以大大提升演算法的速度。因此，数量为 r 的资料点所采用的 DFT 速算法，就称为快速 **Fourier** 转换 (fast Fourier transform，简称 FFT)。FFT 的反向运算，则称为反向快速 **Fourier** 转换(inverse fast Fourier transform，简称 IFFT)。FFT 过去一直应用于超级电脑或信号处理特殊硬件的领域。不过以目前的微处理器速度，个人电脑就已经具备复杂的信号处理能力。特殊的数位信号处理器(digital signal processor) 如今变得相当便宜，几乎已经应用在所有东西之中，包括 802.11 网卡的芯片组。

如果采用 OFDM，讯符间干扰就不会造成问题。OFDM 所使用的 **Fourier** 转换，会将所收到的波形萃取为副载波的振幅，因此时间偏差就不会造成太大的问题。图 13-4 中，基本的低频载波将具有较大的振幅，而迟到的高频部分则可以忽略不计。

虽然有种种好处，但也非全无代价。OFDM 系统使用了多个频率各异的副载波。这些副载波被紧密包裹到一个作业频道中，只要副载波频率有稍许偏移，就会在载波之间造成干扰。这种现象称为载波间干扰 (inter-carrier interference，简称 ICI)。频率偏移之所以产生，可能是因为多普勒效应(Doppler effect) 射器与接收器的时脉频率稍有偏差。

为了同时解决 ISI 与 ICI 的问题，OFDM 收发器会在讯符时间 (symbol time) 开头的部分保留二段防护时间 (guard time) 必而且只在非防护时间进行 **Fourier** 转换。以讯符而言，防护时间以外的部分 f 通常称为 FFT 积分时间 integration -time)，因为 **Fourier** 转换只针对该部分进行处理。

短于防护时间的迟延并不会造成 ICI，因为频率元素并不会渗透到后续的讯符时间。慎选防护时间乃是 OFDM 系统设计人员的主要任务。防护时间显然会降低系统的整体传输量，因为它减少了可用于传输数据的时间。过短的防护时间不仅无法防止干扰，同时还会降低传输量。防护时间如果太长，则会白白浪费许多传输量。

13.1.4 周期延伸 (周期前置)

实作防护时间最直接的方式，莫过于届时不要传送任何东西，如图 13-5 所示。

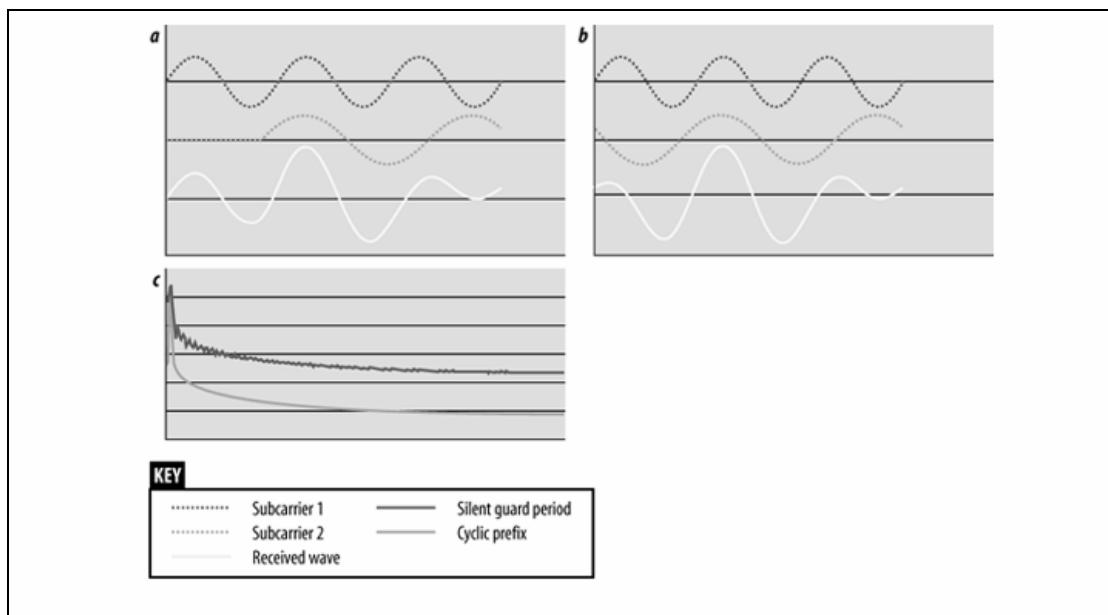


图 13-5：天真的防护时间实例（千万别这么做！）

如此实作防护时间，一旦遇到常见的迟延，就可能将正交性粉碎无遗。OFDM 要求各载波之间的波长数目必须为整数。当防护时段几乎完全静止时，迟延现象就可以轻易摧毁此一必要条件，如图 1 于 S 所示。当图中两个副载波叠加在一起，光谱分析 (spectral analysis) 显示副载波 1 (两周期/讯符) 的振幅较强，而副载波 2 (三周期/讯符) 相对较弱。此外，光谱分析也显示相当数目的高频成份，进一步使信号更加混淆。这些高频部分是突然「启动」。信号所造成的结果。

要解决静止的防护时段所造成的问题十分简单。只要将副载波的 FFT 积分时段向前延伸至防护时段即可。延长副载波 (换言之即是延长整个 OFDM 讯符) 会使 Fourier 转换只显示出该副载波频率的振幅。这种技术通称为「周期延伸」 (cyclic extension)，也可以称为 r 周期前置延伸：(cyclic prefix extension)。经过前置延伸的防护时段，称为「周期前置」 (cyclic prefix)。

图 13-6 的周期前置保有光谱分析的结果。副载波 1 并无偏差，因此不会造成问题。副载波 2 有所迟滞，不过前一个讯符只出现于防护时段，因此 Fourier 转换不会加以处理。由于周期前置延伸的作用，当副载波 2 经过 Fourier 转换处理时，它在每段积分时间 (integration time) 就是三个周期的纯波 (pure wave)。

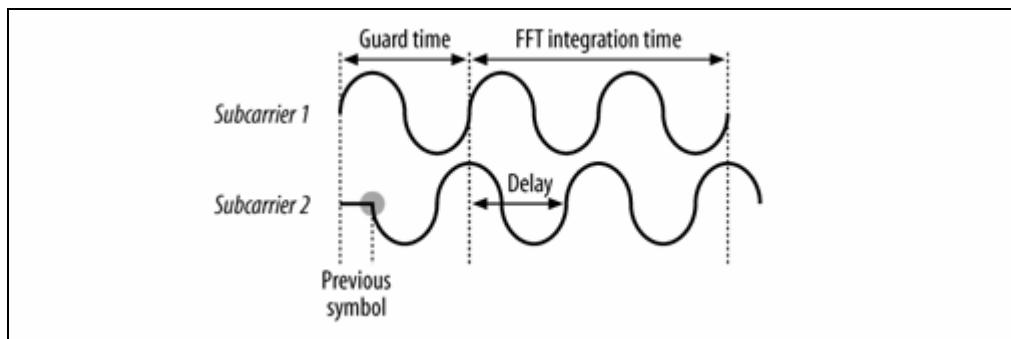


图 13-6：周期前置延伸

13.1.5 加窗法 (Windowing)

另外，OFDM 收发器可以采用一种加强技术，以便符合实际需要。在讯符的边界地带，信号的过渡 (transition) 不尽然都是相当平顺。这种突然的转换会产生一些高频成分 (杂讯)。为了使 OFDM 收发器表现良好，通常会在信号前后加上填塞位元(padding bits)。如此一来，收发器在达到完全功率或自完全功率降下的过程中。就能够以麻坡升：(ramp up) 或许坡降：(ramp down) 的方式缓缓升降。使用错误更正码时，填塞位元通常是必要的。有些文件称填塞位元为「调整序列」(training sequences)。

加窗法 (Windowing) 主要是让新的信号能够缓缓拉升至完全强度！以及让旧信号能够逐渐消逝的一种技术。图 13-7 显示了一种常见的余弦波加窗函数。在讯符周期开始阶段，新的函数系根据余弦函数逐渐拉高至完全强度。当讯符周期结束，该余弦曲线则是让讯符的结束不致过于突然。

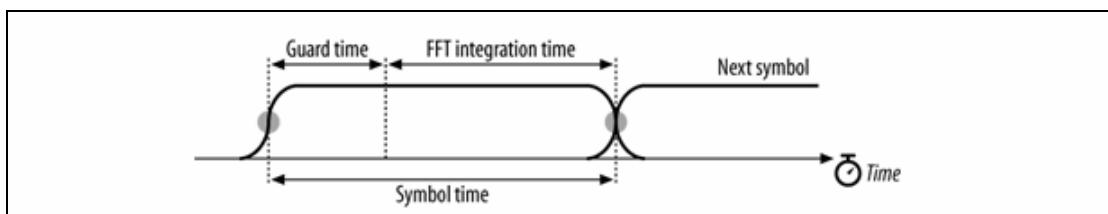


图 13-7：余弦加窗 (Cosine windowing) 技术

13.2 802.11 所采用的 OFDM

802.11a 并未彻底运用 OFDM 技术。负责 OFDM 标准化作业的任务小组运用至无线局域网络时，采取了中庸之道。

13.2.1 将 OFDM13.2.1 302.11 a 所选用的 F.M 参数

选择 OFDM 参数时，通常有三项既定的事实。频宽 (Bandwidth) 是固定的，这通常由管制当局来限制。迟延时间 (Delay) 取决于 OFDM 系统的作业环境。通常办公大楼的迟延范围 (delay spread) 为 40 至 70-ns，不过在某些环境里，迟延范围可能高达 200 ns。最后，提高位元率 (bit rate) 通常是设计上所要达到的目标，虽然这通常意味著「在其他参数之限制不变的情况下，尽量提高位元率」。

比较常见的做法是，防护时间应该为平均迟延时间的二至四倍。因此，802.11a 设计人员选用 800 ns 做为防护时间。讯符的持续时间应该比防护时间长，不过有值得斟酌之处。较长的讯符时间，代表该段时间内可以容纳更多副载波。更多副载波会增加传送端与接收端的信号处理负担，设备的成本与复杂度也会因此提高。比较实际的做法是，选择至少比防护时间多五倍的讯符时间。802.11a 以 800-ns 的防护时间搭配 4-us 的讯符时间。Subcarrier spacing (副载波间隔) 与 FFT 积分时间成反比。802.11a 的积分时间为 3.2-us，而 Subcarrier spacing 为 0.3125 MHz (1/3.2us)。

802.11a 中作业频道的频宽为 20 MHz。作业频道使用多少频宽，纯粹是设计上的决定。较宽的频道具有较高的传输量，不过可用频谱当中只能容纳较少的作业频道。采用 20-MHz 作业频道，可以为每个频道提供合理的速度 (最高为写 Mbps)，以及在所指定的频谱中提供数量合理的作业频道。802.11a 在调制与编码上提供了相当多样的选择。采用较稳定的调制方式与较保守

的编码率，可以提供较低速但较可靠的传输量，选择较细致的调制方式与较激进的编码率，则可以提供较高但不是那么可靠的传输量。

13.2.2 作业频道的结构

和 DS PHY 一样，OFDM 物理层将频谱区分为作业频道。每个频宽 20-MHz 的频道由 52 个副载波所组成。其中有 4 个副载波充当导波（pilot carrier），用以监控路径偏移与 ICI。至于其余 48 个副载波则是用来传递数据。副载波之间彼此相距 0.3125MHz 频道编号从 -26 至 26，如图 13-8 所示。由于信号处理上的需要，副载波 0 并未使用。

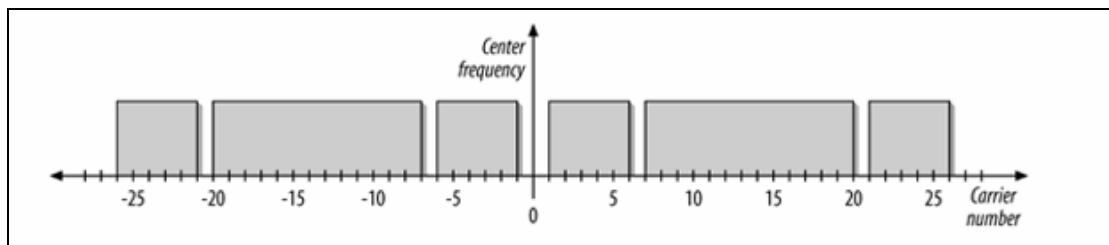


图 13-8：OFDM 频道的结构

副载波 -21、-7、7 以及 21 被指定为导波。为了避免在 Fourier 转换中出现过强的光谱线（strong spectral line），导波会以 802.11a 所规范的保守调制技术传送固定的位元序列。

13.2.2.1 子频道调制技术

802.11a 在每个子频道上使用「正交调幅」(quadrature amplitude modulation, 简称 QAM) 技术来传送数据。QAM 是在单一载波 (single carrier wave) 上编码数据，不过该载波是由「同相」(in-phase) 与下正交：(quadrature) 两种信号组成。QAM 会同时对这两种信号进行调幅；亦即根据输入信号的大小调整载波波形。主载波是以同相信号为名，简写为 I。正交信号落后四分之一周期，简写为 Q。（也可以用复数来表示其波形，建构出 QAM 的数理模型。）基本上，这个组合信号的振幅以及相位差均用来编码信息。【注】

QAM 被广泛使用于无线电传输系统。以北美电视系统而言，同相信号用来承载亮度 (luminance 或 brightness) 信息，而正交信号则用来承载彩度 (color) 信息。调幅广播也可以有立体声；一种称为 C-QUAM 的正交调幅系统，就是以正交信号来编码立体声 (stereo) 信息。

注：802.11 接序列实体 W (DS PHY) 所使用的相移调制属于 QAM 的特例。它所调制的是相位而非振幅。

电视和广播通常属于类比系统。在数位系统中，同相与正交信号经过量化 (quantized) 被限定在一组特定准位。当两种信号都被限定在一组特定准位时，结果就形成了所谓的星座图 (constellation)。星座图通常是在二维平面上描绘出同相与正交信号的可能值。星座图上的每个点代表一种讯符 (symbol)，每个讯符代表特定的位元值。提到 QAM 时，通常会在前面标记星座图中的位元数，例如 64-QAM。在每个方向，量化值的数目必须是 2 的乘幂数，因此 QAM

前面附注的数字也将是 2 的乘幂数 (power of two)。和其他建议书一样，802.11a 采用方形星座图，亦即其值必须为 2 的偶次幂 (even power of two)，此数字恰为正方形 (16-QAM, 64-QAM, 256-QAM)。

要提高数据率，只要使用点数更多的星座图即可。不过当数据率提高，接收信号品质必须够好，否则就难以区别星座图中的相邻点。如果距离太近，每个点的可接受误差范围就会缩小。802.11a 在物理层标准中规范了每个星座点的最大可接受误差范围。图 13-9 显示了 802.11a 所使用的星座图。BPSK 与 QPSK 的位元率最低，它们是直接序列物理层所使用的两种相移键控调制。

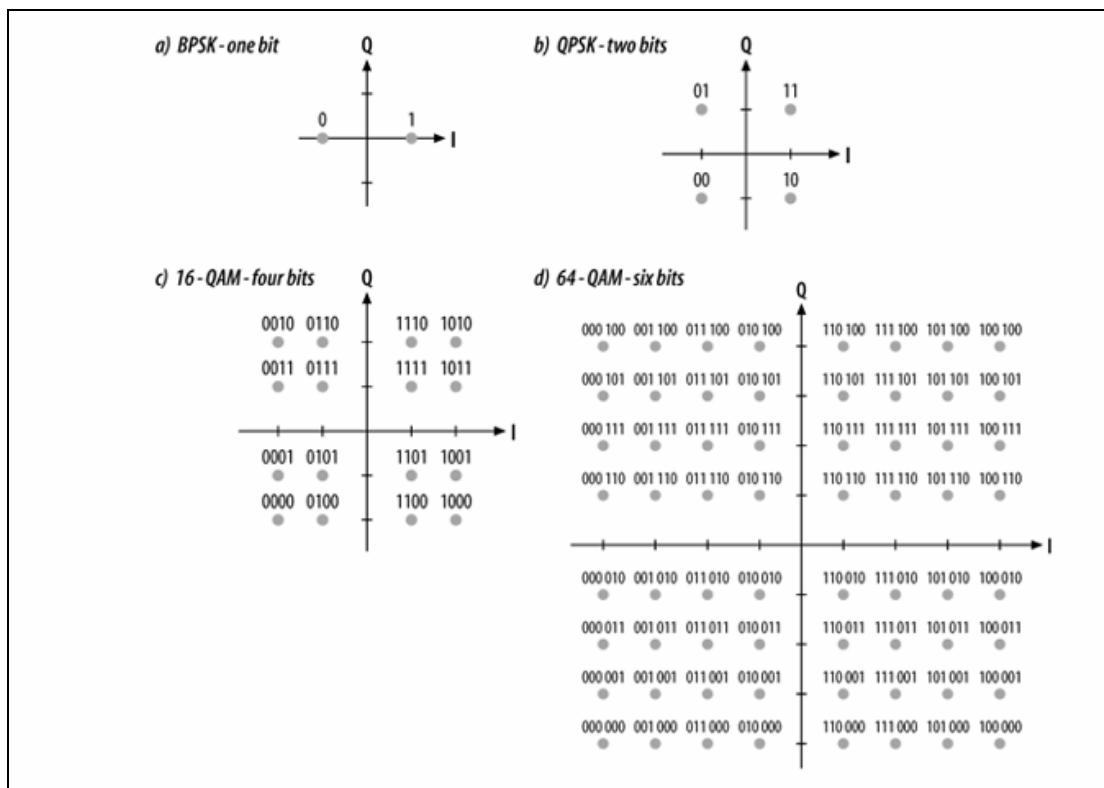


图 13-9: 802.11 a 所使用的星座图

子频道数乘以每个频道的位元数，就可以得出电波频道的总传输率。使用 64-QAM 时，每个子频道可以承载六个位元。802.11a 使用 8 个子频道，因此每个频道的传输率为 288 个位元。不过，还有另外一个属性必须说明。大多数无线电频道作业不可能没有错误出现。因此必须加入错误更正码。

13.2.2.2 前溯错误更正码与编码

严格来讲，前溯错误更正码 (forward error-correcting code) 并不属于 OFDM。不过，当信号遭受窄频干扰，或者在特定的窄频频率面临所谓的深度衰落 (deep fading) 时，也可以使用 OFDM。一旦发生衰落现象，由于所收到的振幅十分微小，因此频道就会丧失携载数据的能力。为了防止某些衰落的频道造成位元错误率 (bit error rate) 大幅上扬，实作上，可以使用 OFDM 为所有子频道加上错误更正码 (error correction code)。

搭配错误更正码的 OFDM，有时也称为加码式 OFDM（codedOFDM）。加码式 OFDM 会在各个频道使用前溯错误更正(forward error correction，简称 FEC) 码。只要遗失或受损的位元数不多，FEC 系统可以让接收器检测受损位元并加以修复。为了具备错误更正能力，必须在数据串流中加入冗馀位元（redundantbits）。FEC 码的运作方式，系根据目前所传送的数据位元来产生一个状态引擎（stateengine），并且将它们编码至多个讯符当中。以这些讯符抹平杂讯，就可以把瞬间杂讯减至某种程度，使接收器重组位元串流的能力不致受误差所影响。

可用的前溯错误更正码有两种。「区块码」（block code）采用长度固定的输入区块，而「迴旋码」（convolutional code）则可以应用于任何长度的串流。区块码主要用于以固定长度来储存。传输或处理数据的应用。DVD、CD 以及硬碟机等均使用区块码。不过对无线局域网络而言，迴旋码是比较好的选择，因为传输帧的长度通常并不固定。【注】

回旋码有两个主要参数。**constraint length** 决定了数据位元的等化时间。**constraintlength** 愈长，等化（average）数据位元（包含杂讯）就需要愈多时间，虽然解码器的复杂度会因此而增加，不过这是换取较可靠传输的代价。至于较短的 **constraint length**，则是便用 802.11a 标准建议的 Viterbi 演算法。之所以有此建议，是因州 Viterbi 解码器属于「最大相似度」（maximum likelihood）解码器。Viterbi 解码然解读出的数据位元和原始数据的相似程度最高。并非所有解码器均采用最大相似度演算法，虽然它对数位传输系统而言显然是项重要的属性。802.11a 所使用的 **constraint length** 为 7，这个数字是 Viterbi 解码器实际应用上的极限。（Viterbi 码的复杂度会随著 **constraint length** 成指数递增。）

注： 1993 年，发现两组 回旋编码可以组成所谓的「超级码」(turbo code)。超级码的威力十分惊人，不过代价是必须付出一些 回旋编码的迟延时间。如果迟延一些时间无妨，就可以使用超级码，例如外太空与卫星通信。超级码的进一步信息可以参考 *jet Propulsion Laboratory takes, (<http://zuww3,31pl.nasa.gov/public/JPLtcodes.html>)* 其中的报导比较了 Voyager 与 Cassini 两次探测所使用的超级码与错误更正码。超级码也用于 Qualcomm 的 3G 网际网络访问系统 1xEV-DO。

第二个参数是编码率（coding rate，简写为 R），用来决定加入多少冗馀位元 • 它代表每个编码位元可以传送多少数据位元。 $R=1/2$ 的迴旋编码代表每两个编码位元传你一个数据位元。比较激进的做法可能会加入较少的冗馀信息，例如使用 $3/4$ 的编潮率，亦即当中只有 25% 的冗馀位元。选用何种编码率纯粹是工程上的议题。当编码率减少，用来更正错误的编码位元就比较多，因此比较牢靠，不过必须付出传输量变少的代价。802.11a 规范了三种编码率，其中最保守的做法使用 $1/2$ 的编码率，至于最激进的做法，编码率甚至高达 $3/4$ 。【注】

迴旋编码率可以通过镂空（puncturing）程序加以改变。镂空码的做法是丢弃某些加码位元（coded bits），从而提高 回旋码的编码率。数据编码时采用较低的编码率 • 以 802.11a 为例，最低的编码率是 $1/2$ ，因此数据变为原先的两倍 • 要将编码率提高为 $2/3$ ，可以丢弃其中三分之一的加码数据，亦即将加码数据「镂空」（punctured） • 要镂空为 $2/3$ 的编码率，意即丢弃 30% 的加码数据。扣除丢弃的位元，才是真正传送的加码数据 • 在接收端，解码器会在镂空的部分填塞无关紧要的位元。图 13-10 显示了将编码率从 $1/2$ 提高为 $3/4$ 的镂空程序。使用镂空码的好处是，它可以用软件控制的 回旋编码器来实作，而且可以通过软件，使用不同的镂空样式（puncturing pattern）来变更编码率。

13.2.2.3 子频道交错

每个作业频道由 48 个频道组成。基本上，每个作业频道的传输量就是 48 个数据串流的总合。所接收到的加码位元串流必须对映到正确的副载波。**802.11a** 所使用的是一组交错规则，而不是使用简单的 **round-robin** 演算法，轮流将位元对映到副载波，例如第一个位元对映到第一个副载波，第二个位元对映到第二个副载波，依此类推。第一项规则可以确保依序传送的位元会被分散至相隔较远的副载波，第二项规则可确保依序传送的位元对映至不同的星座图点。举例而言，图 13-11 显示了用于 **16-QAM** 的交错作业，其中共有 192 个位元。承载数据的副载波总数为 48，每个位元均必须对映到其中一个副载波。图形中描绘出了每个副载波所对映的点位，并且清楚地显示出了每个副载波负责四个加码位元。

注： 802.11a 所使用的回旋码长度限制为 7 编码率为 $1/2$ 。Voyager 进行深度太空兀旅时也是使用回旋码。

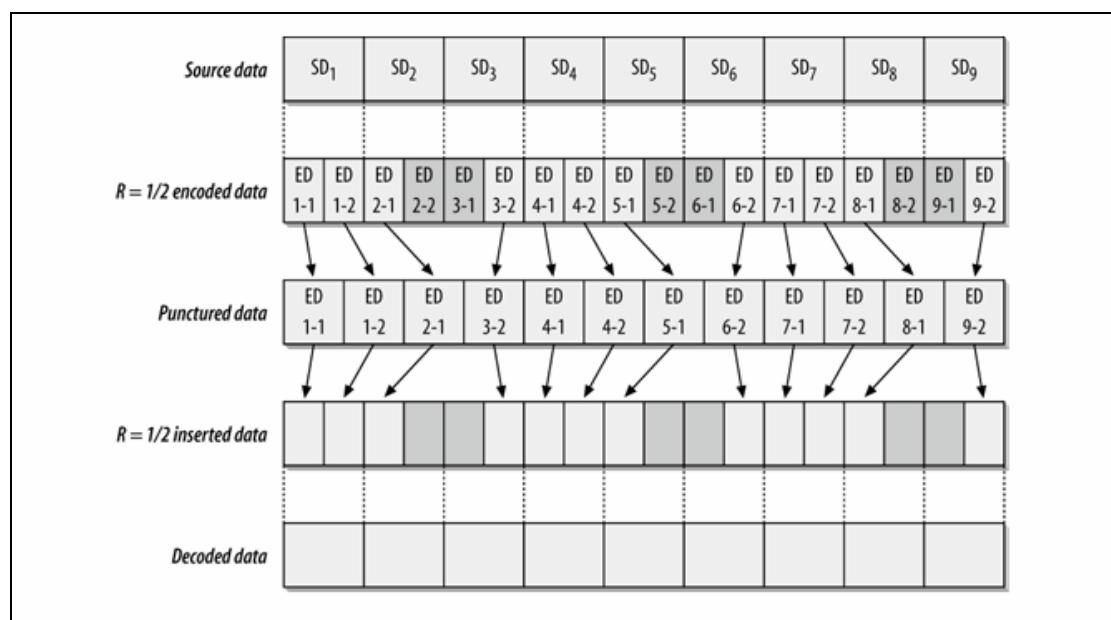


图 13-10：通过镂空程序提高编码率

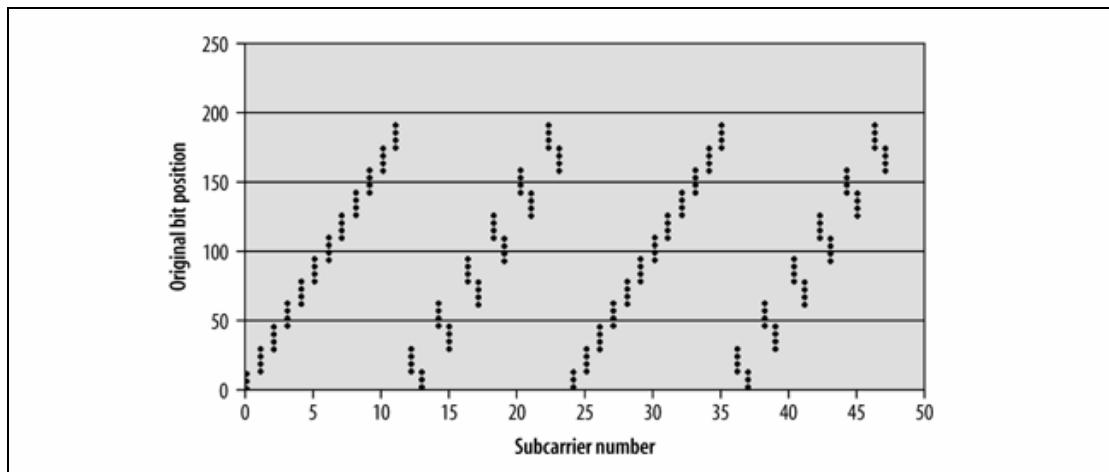


图 13-11: 16-QAM 的交错程序

13.2.3 作业频道

根据下列公式，可以为 5-GHz 频段中的频道指定编号，频道间相距 5 MHz：

$$\text{中心频率 (MHz)} = 5,000 + 5 \times n; \quad n = 0, 1, 2, \dots, 199$$

$$\text{中心频率 (MHz)} = 5,000 - 5^*(256 - n), \quad n = 240, 241, \dots, 255$$

显然，每个频宽为 20-MHz 的 802.11a 频道占用四个频道。频道的建议使用方式列于表 13-1。802.11a 原本是针对美国所做的设计。欧洲的频道划分是在 2003 年底纳入 802.11h，日本的作业频道则是在 2004 年底纳入 802.11h。【注】

表 13_1: 802.11a/j 的作业频道

频率	允许使 用地区	最大功率 限制 (注 a)	作业频 道编号	中心频率 (GHz)
4.920-4.980 GHz	日本	250 mW EIRP 且 < 1W 或者 10 mW EIRP	240 244 248 252	4.920 4.940 4.960 4.980
5.040-5.080 GHz	日本	250 mW EIRP 且 < 1W 或者 10 mW EIRP	8 12 16	5.040 5.060 5.080
5.15-5.25 GHz	日本	200mW (<10mW/MHz)	34 38 42 46	5.170 5.190 5.210 5.230
U-NII 低频段 (2.5 mW/MHz)	美国	40mW (5.15- 5.25GHz)	36 40 44 48	5.180 5.200 5.220 5.240

注：欧洲无线电波管制标准是由「欧洲邮政电信协会」(European Conference of Postal and Telecommunications Administrations, 简称CEPT)负责。相关法规是CEPT委托「欧洲无线电通讯委员会」(European Radiocommunications Office)制定的。5 GHz 无线局域网络管制规定详见ERC/DEC/(99)23(文件网址为<http://www.ero.dk/doc98/official/Pelf/DEC9923E.PDF>)。日本的主管机关是「总务省」(Ministry of Internal Communications, 网址为<http://www.soumu.go.jp/>)。相关法规详见Articles 49.20与49.21(http://www.soumu.go.jp/joho_tsusin/eng/Resources/Legislation/MRA/020226_00.htm)。

频率	允许使用地区	最大功率限制(注 a)	作业频道编号	中心频率(GHz)
U-NII 中频段 (5.25-5.35 GHz)	美国	200mW (12.5 mW/MHz)	52 56 60 64	5.260 5.280 5.300 5.320
5.470-5.725 GHz	欧洲(CEPT) (2003年11月后， 也允许在美国地区 使用，受U-NII的规 范【注 b】)	1 W EIRP	100 104 108 112 116 120 124 128 132 136 140	5.500 5.520 5.540 5.560 5.580 5.600 5.620 5.640 5.660 5.680 5.700
U-NII 高频段 (5.725-5.825 GHz)		800 mW (50 mW/MHz)	149 153 157 161	5.745 5.765 5.785 5.805

注 a 美国允许使用的功率。相当于增益为 6 dBi 之天线的最大输出功率。

注 b FCC 03-287 另外开放了这段频谱(<http://braunfoss.fcc.gov/edocs-public/attachmatch/FCC-03-287AZ.pdf>)，不过在本书即将付印时测试程序仍在开发当中。未经测试认证，任何设备均不得在美国使用此频段。

作业频段尚有一些值得注意的功能。和 DS PHY 一样，OFDM 会使用传输遮罩(transmit mask)，防止功率泄漏至左右频段。所使用的遮罩如图 13-12 所示。

图 13-13 显示了美国所使用的 802.11a 频道。在每个 U-NII 频段(band)中包含四个频道(channel)。在两个较低的频段中，允许频道彼此重叠，以及在 U-NII 低频段与中频段两旁使用予 0-MHz 的防护频段。

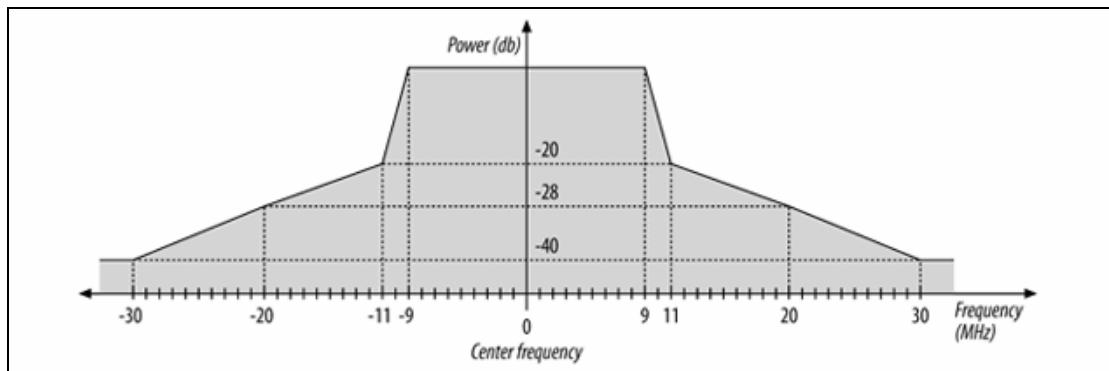


图 13-12: 802.11 的频谱传输遮罩

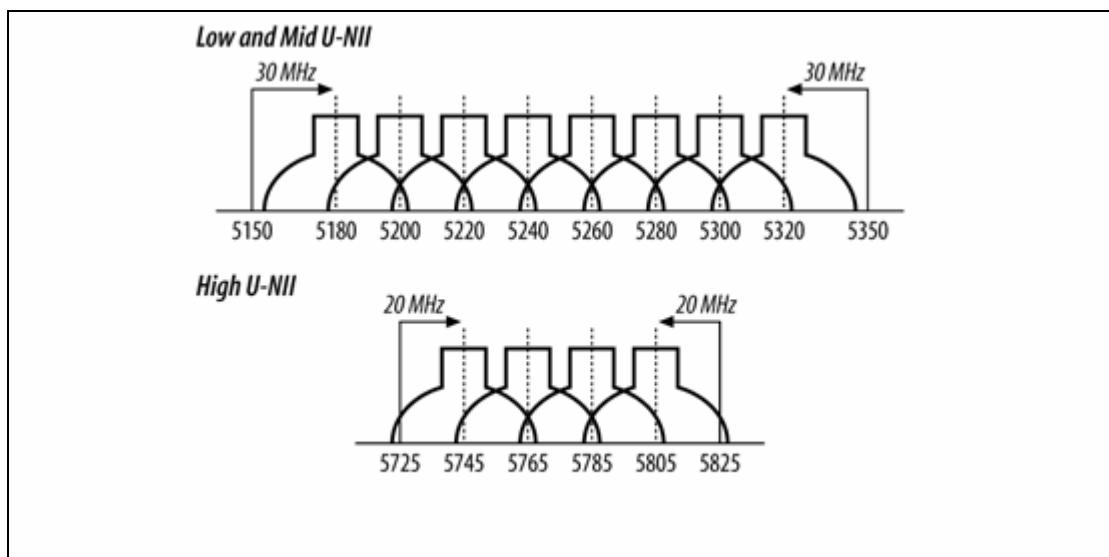


图 13-13: 表 13-1 作业频段的图示

13.3 OFDM PLCP

和其他物理层一样，OFDM PHY 具有它自己的 PLCP，其中包含了该物理层专属的帧参数。

13.3.1 帧的格式

OFDM PHY 负责添置同步信号(preamble) 以及 PLCP 标头。此外，干结尾的位元，以协助所使用的编码机制。本节是以逻辑的方式来区分不过有些组成元件涵盖协议单元中不同的栏位。图 13-14 是我们进行 OFDM 讨论的出发点。

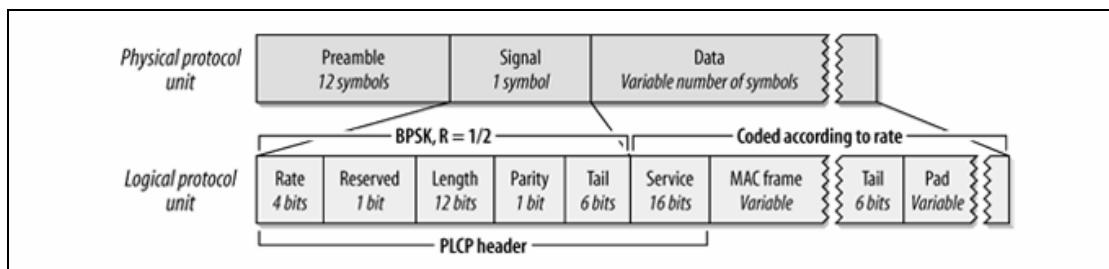


图 13-14: OFDM PLCP 帧的格式

图 13-15 显示了帧的前段，其中包含防护时段（guard interval）以及发射器所使用的加窗法（windowing）。同步信号持续了 16 μs，平均分配给短调整序列（short training sequence）与长调整序列（long training sequence）。两者之间的区别将于下节探讨。同步信号之后，由一个 OFDM 讯符携载 Signal 栏位，然后由数据讯符携载 PLCP 标头的结束栏位，最后是 MAC 原始数据（payload）以及结尾位元（trailer）。所有讯符均使用经过修饰的余弦窗（cosine window）以确保转换能够平顺。于用来同步频率的短同步信号（short preamble）之后，会使用防护时间（guardtime）来防止多重路径衰落（multipath fading）。

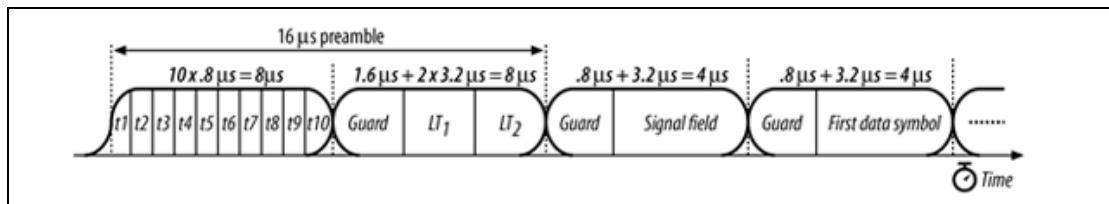


图 13-15: 同步信号与帧开始的部分

13.3.1.1 同步信号

和所有常见的 IEEE 802 网络一样（包括所有的 802.11 物理层），OFDM 实体协议单元（physical protocol unit）系以一个同步信号（preamble）开始。它是由 12 个 OFDM 讯符所组成，藉以同步传送端与接收端的计时器。前面十个讯符乃是短调整序列（short training sequence），接收器会用它来锁定信号，如果使用多组天线，也可藉它来选用天线。以及同步「开始解码后续讯符」所需之大规模时序关系。短调整序列传输时并未使用防护时段，在短调整序列后面紧跟着两个长调整序列（long training sequence）。长调整序列主要用于微调 timing acquisition，同时探用防护时段的保护。

13.3.1.2 标头

PLCP 标头就是实体协议单元的 Signal 栏位，外加实体协议单元之 Data 栏位然 Service 次栏位。Signal 栏位包含 Rate、Length 以及 Tail 等次栏位，如图 13-16 所示。

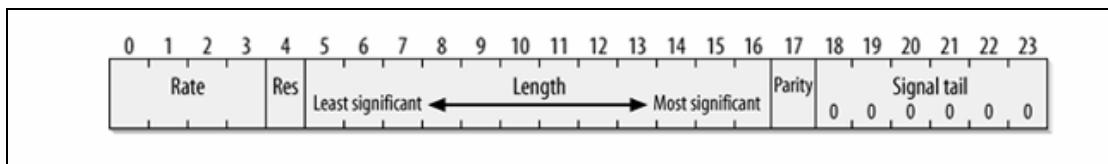


图 13-16: OFDM PLCP 帧的 Signal 栏位

Rate (4 个位元)

以四个位元编码的数据率。表 13-2 显示了每一种数据率所对应的位元编码。每一种数据率所使用之编码与调制机制的详细说明，请参阅 13.4 节〈OFDM PMD〉。

表 13-2：数据率及其位元编码

数据率 (Mbps)	位元 (依传送次序排列)
6	1101
9	1111
12	0101
18	0111
24	1001
36	1011
48	0001
54	0011

Length (12 个位元)

所包含之 MAC 帧中的位元组数目，以 12 个位元加以记录。和大多数栏位一样，此栏位由最低效位元至最高效位元逐一传送。Length (长度) 栏位会经过迴旋编码，以防止错误发生。

Reserved (1 个位元) 与 Parity (1 个位元)

位元 4 保留供未来使用，必须设置为。位元 17 是前 16 个 Signal 位元的 even parity (偶同位) 位元，用来避免数据损毁。

Tail (6 个位元)

Signal 栏位以六个值为 0 的结尾位元做为结束，以展开回旋码 (convolutional code)。因此，在定义上这六个位元必须交由迴旋编码处理。

Service (16 个位元)

PLOP 标头的最后一个栏位是长度 16 位元的 Service 栏位。和 PLCP 标头其他栏位不同的是，它是以所包含之 MAC 帧的数据率，通过实体协议单元的 Data 栏位来传送。此栏位前八个位元设置为。和其他物理层一样，在传送之前，MAC 帧必须经过搅码。前六个位元设置为。是为了敌动搅码器。剩下的九个位元目前保留，在未来另有他用之前必须设置为。

13.3.1.3 Data

数据所使用的编码机制取决于数据率。在传送之前，数据必须经过搅码，和其他物理层一样。标头的 Service 栏位之所以包含在物理层协议单元的 Data 栏位，是因为必须以它来启动搅码器。

13.3.1.4 Trailer

实体协议单元的 Data 栏位会以标尾 (trailer) 做结束。（802.11a 规格书并称结尾栏位为标尾，它把标尾当成术语来看。）标尾由两个栏位组成：

Tail (6 个位元)

和 PLCP 标头的结尾位元一样，附加至 MAC 帧结尾的位元，主要是让迴旋编码可以平顺结束。之所以需要 6 个位元，是因为迴旋编码的长度限制为 7。

Pad (位元数不定)

802.11a 所使用的、OFDM 是以长度固定的位元区块传送数据。Data 栏位之所以加上填塞位元，是为了使数据长度与位元区块大小一致。位元区块大小取决于数据所使用的调制方式与编码率；下一节将会加以探讨。

13.4 OFDM PMD

OFDM PHY 使用了各种不同的调制机制，数据率可达到 6 Mbps 至 54 Mbps。在所有情况下，物理层在 48 个子频道所使用的讯符率为每秒 250,000 个讯符，至于每个讯符可以装载几个数据位元则视情况而定。单一 OFDM 讯符会分布在所有这缠 8 个子频道中。

13.4.1 编码与调制

OFDM PHY 的速率有四级：6 与 9 Mbps、12 与 18 Mbps、24 与 36 Mbps 以及 48 与 54 Mbps。6、12 与 24 Mbps 是必要的项目，亦即前三级的最低速度，因此右一遇干扰时也最稳定。第一级的速率使用二进制相移键控 (binary phase shift keying，简称 BPSK) 在每个子频道编码一个位元，或者相当于每个讯符 48 个位元。迴旋编译(convolution coding) 意指这些位元中有一半或者四分之一是用于错误更正的多馀件元，因此每个讯符中实际只包含了 24 或予 6 个数据位元。第二级的速率使用正交相位键控 (quadrature phase shift keying，简称 QPSK) 在每个子频道编码两个位元，相当于每个讯符 96 个位元。去除冗馀的迴旋码。接收器实际收到的有 48 或 72 个数据位元。第三与第四级使用 BPSK 与 QPSK 的一般型式，称为正交调幅 (quadraturamplitude modulation，简称 QAM)。16-QAM 系以 16 个讯符编码 4 位元，而 6-QAM 则是以 64 了固讯符编码 6 个位元。第三级速率使用 16-QAM 以及 R=1/2 (1iiR 二夕 4 的标准型 旋码。不过，为了达到更高速率 64-QAM 系采用 R=2/3 与 R=3/4 的回旋码 • 表 13-3 列出了 OFDM PHY 中每种数据率所使用的编码方式。

表 11-3 各种 OFDM 数据率的编码细节

速率 (速率)	调制方式与 编码率 (R)	每个子频道所编 码的位元数[注 a]	每个讯符所编码 的位元	每个讯符的数 据位元数[注 b]
6	BPSK、R=1/2	1	48	24
9	BPSK、R=3/4	1	48	36
12	QPSK、R=1/2	2	96	48
18	QPSK、R=3/4	2	96	72
24	16-QAM、R=1/2	4	192	96
36	16-QAM、R=3/4	4	192	144
48	64-QAM、R=2/3	6	288	192
54	64-QAM、R=3/4	6	288	216
72[注 c]	64-QAM	6	288	288

注 a: 每个子频道所编码的位元数为调制方式(BPSK、QPSK、16-QAM 或 64-QAM) 的函数。

注 b: 每个讯符的数据位元数为回旋编码率的函数。

注 c: 虽然不使用返旋码的情况并未纳入标准。有些产品还是提供这项模式来提升传输量。

13.4.2 电波效能：灵敏度与频道拒斥

和其他物理层一样，802.11a 也规范了接收器的最低灵敏度要求，如表 13-4 所示。之前已经提过其他物理层的最低灵敏度。惟一比较值得注意的，就是 802.11a 的传输率比较多样，必须针对个别传输率订定最低效能要求。相较于直接序列物理层，802.11a 所订定的要求算是有过之而无不及 802.11b 要求接收器必须具备一 76 dBm 的灵敏度，相当于 802.11a 中 18 Mbps 与 24 Mbps 这两种速率。[注]

比较值得注意的是频道拒斥（channel rejection）的部分。和其他物理层一样，首先在任意频道输入一个比最低灵敏度稍高（约 dB）的信号，然后在相邻或不相邻频道输入第二个信号进行拒斥测试。当受测频道的帧错误率为 10% 时，注意两个频道间的功率差异。

由此表可知，当数据率愈高，接收器所收到的信号就愈容易损毁。如果 802.11a 网络的基站过于密集，位于相邻基站间的工作站可能会同时接收到来自两者的 54Mbps 信号，造成工作站的无线芯片无法判读。不过 54Mbps 的传输距离相对较短，因此不太会出现这种状况。此外，虽然有些芯片组效能优于标准所规定，不过大多数厂商并不会在网卡的规格表中列出邻频拒斥的数据。

表 13-4：接收器的效能要求

数据传输率 (Mbps)	最低灵敏度(dBm)	邻频拒斥值(dB)	非邻频拒斥值(dB)
6	-82	16	32
9	-81	15	31
12	-79	13	29
18	-77	11	27
24	-74	8	24
36	-70	4	20
48	-66	0	16
54	-65	-1	15

13.4.3 净空频道评估

OFDM PHY 规格书留下相当大的空间，让实作人员得以自行选择净空频道评估（clear channel assessment）技术。信号的强度门槛值可用来决定频道是否正在使用，不过 802.11a 设备的主要指导原则是，设备本身必须符合特定的效能标准。实作上可以使用 PLCP 标头的 Packet Length 栏位做为净空频道评估的参数，但并非必要。

13.4.4 传送与接收

802.11a 接收器的方块图如图 13-17 所示。准备传送帧时，802.11a 界面会进行下列步骤：

1. 选择传输率。速率选择演算法因实作而异，在相同环境下，不同厂商的产品也许会选择不同的速率。速率决定了所使用的调制方式与回旋码，以及各个副载波的数据位元数。参见表 13-3。
2. 传送 PLCP 同步信号，其中包含长短调整序列。
3. 开始传送 SIGNAL 栏位中的 PLCP 标头。它并未经过搅码，但经过回旋编码器的编码。
4. 产生封包的数据栏位
 - a. 产生 SERVICE 栏位，目前这个栏位的每个位元均设为 0。前面七个 0 是用来初始化搅码器，后面九个位元目前保留未用，均设为 0。
 - b. 附加数据
 - c. 放置六个 0 做为标尾。
 - d. 以填塞位元补。, 使之成为副载波区块数据位元的倍数。
5. 对数据进行搅码，如此可以避免出现长串的 0 或 1。
6. 以回旋编码器进行数据编码。如有必要，再对回旋编码的结果进行镂空处理，以高于 $1/2$ 以上的编码率产生编码后的字串。
7. 将加码数据（coded data）分成区块处理。区块大小取决于数据讯符的调制率。
 - a. 进行交错程序，将区块中的位元对映到缠 8 个副载波。
 - b. 在作业频道的特定位置插入四个导波
 - c. 使用反向 Fourier 转换，将频域数据转换为时域数据进行传送。
8. 重覆步骤 5 直到所有数据区块传送完毕。

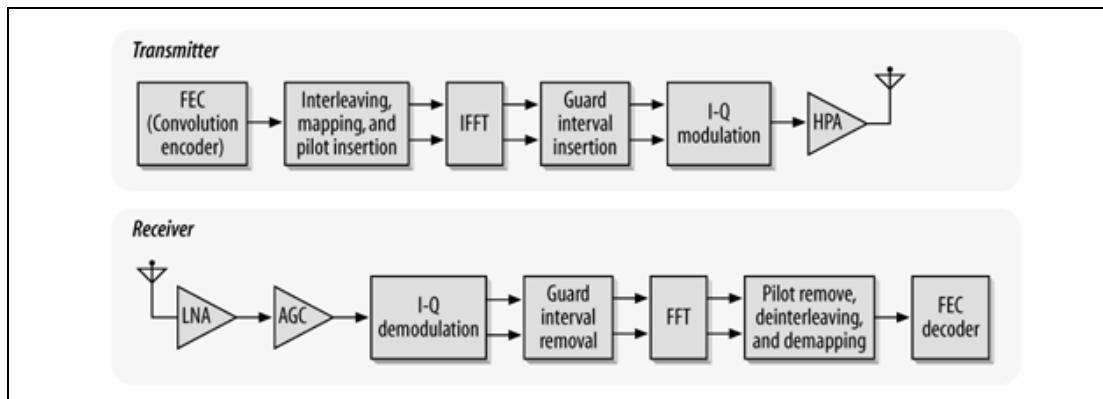


图 13-17：收发器方块图

3.4.4.1 正面回应

802.11a 标准规定 6、12 与 24 Mbps 是必要的（required）数据率。802.11 MAC 要求每个帧均必须得到正面回应。传送正面回应时，必须采用已连接工作站均支持的数据率。大多数设备是以 24 Mbps 的数据率传送正面回应讯息，如此不仅可以符合上述要求，也可以将网络的负担（overhead）降至最低。

13.4.4.2 .FDM 编码范例

正如读者到目前为止所见，OFDM 是个相当密集。由好几个步骤所构成的程序。802.11a 对原始规格的一项增补，记录于附录 G，内容是将「席勒的欢乐颂」(Schiller's Ode to Joy) 编码后以 802.11a 网络进行传输。802.11a 发行后不久，IEEE 802.11 工作小组在范例中发现了一些错误，因此发行了修正版。如果各位对 OFDM 编码的细节感到兴趣，可以参考该范例。

13.5 OFDM PHY 的特性

OFDM PHY 特有的参数列于表 13-5。和第 11 和 12 章所介绍的物理层一样，OFDM PHY 也包含一些参数，可用来调整电子零件不同处理阶段所造成的迟延。最后值得注意的是，额外的频宽提升了不少传输量。美国原本有 12 个频道，最近又清理出其他个频道。以传输时间的 50% 计算，20 个共存频道可以提供 500 Mbps 以上的传输。这个数字是其他物理层标准远远不及的。

表 13-5: OFDM PHY 参数

参数	值	备注
最大 MAC 帧长度	4.95 bytes	
时槽时间	9us	
SIFS 时间	16us	SIFS 可用来推衍出其他帧间隔值 (DIFS、PIFS 以及 EIFS)。
竞争期间的大小	15 至 1023 个时槽	
同步信号持续时间	20us	
PLCP 标头持续时间	4us	
接收器灵敏度	-65 至 -82 dBm	取决于数据传输速度

和其他的物理层一样，OFDM PHY 中也有些属性可供厂商调整，使系统各部分的迟延时间保持均衡。其中包括 MAC • PLCP、收发器等的迟延变数，以及收发器之电子零件个别变异的相关变数。

第14 章 802.11：延伸速率物理层（ERP）

当无线局域网络首度进入主流运算领域，实际上没有太多选择。当时 802.11b 刚成为标准，可望提供近似 Ethernet 的速度。平心而论，这种速度在当时并不算快。等到 802.11a 跨出实验室成为商业产品，使用者开始渴望速度更快，但能够相容于现有 802.11b 硬件的产品。802.11g 因此应运而生，除了提供相当于 802.11a 的额定速率，也使用原本的微波频段。由于作业频率不及 802.11a 的一半，相较于 5 GHz 的 802.11a 设备，802.11g 设备能够传输更远的距离。

802.11g 并非革命性的规格。事实上，只要看过规格书的新增条款，就知道它运用了不少现成的技术。其所制定的新物理层乃是以现有技术为基础，只是稍微做了修改。802.11 地规格书中绝大部分的篇幅都是用来提供回溯相容性。

14.1 802.11g 的组成元件

802.11g 其实是将好几种物理层规格合而为一。虽然统称为「延伸速率物理层」(Extended Rate PHY, 简称 ERP)，但是实际上 ERP 有好几种不同的“口味”：

ERP-DSSS 与 ERP-CCK

这两种模式回溯相容于第 11 章所提到的原始直接序列规格 (1 Mbps 与 2 Mbps)，以及第 12 章所提到的 802.11b 规格 (5.5 Mbps 与 11 Mbps)。为了回溯相容，规格上必须稍做变动。

ERP-OFDM

这是 802.11g 的主要模式。基本上，它是在 ISM 频段 (24 GHz) 中执行 802.11a，不过为了回溯相容，规格上必须稍做变动。它所支持的速率如同 802.11a：6、9、12、18、24、36、48 与 54 Mbps。其中 6、12 与 24 Mbps 为必要的(mandatory) 传输率。

ERP-PBCC

这是 802.11b 之 PBCC 标准的非必要延伸功能 (optional extension)，提供 22 与 33 Mbps 的数据传输率。虽然属于标准的一部分，不过市面上大多数芯片组并未实作此种模式，也未得到广泛使用。

DSSS-OFDM

这是一种混合模式，封包数据 (packet data) 系以 DSSS 标头进行编码，承载数据 (payload) 则是以 OFDM 进行编码。之所以开发此种模式，部分原因是为了提供回溯相容性。虽然 802.11b 无法辨识经 OFDM 调制的内容，但可根据标头所提供的信息来判断封包的持续时间。此功能并非必要？也未被广泛实作。任何实作 802.11g 的设备均须支持某些必要模式。为了回溯相容性，802.11g 设备必须支持 1 与 2 Mbps 的 DSSS 调制 (802.11)，以及 5.5 与 11 Mbps 的 CCK 调

制(802.11b)。除了基本的 OFDM, 所有的 802.11g 工作站也必须支持 6、12 与 24Mbps 的 OFDM 调制。

14.1.1 相容性议题

802.11g 的必要模式只是稍微修改了既有的物理层, 荡了顾及回溯相容性, 另外做了些许变动。802.118 工作站必须加以融合, 以便与其他旧式工作站并存。现有的规格并未改变。802.11b 网卡依然运作如昔。惟一的差别在于 802.118 网卡具备某些 802.11b 所没有的功能。

802.11b 设备实作了两种不同的规格: 原始 802.11 标准所规范之较慢的直接序列(DSSS), 以及 802.11b 所规范之高速的互补码键控 (CCK) 物理层。802.118 同时采用这两种标准, 只做了少许修改。除了旧式工作站, 802.118 工作站也得和其他 802.118 工作站沟通, 因此必须支持 802.118 所规范的同步信号以及同步作业。更重要的是, 802.118 工作站必须支持短同步信号, 因为短同步信号有助于维持较高的传输量。802.118 的无线电系统, 也必须具备更高的信号灵敏度。

此外, 802.11g 设备必须实作 ERP-OFDM, 而 ERP-OFDM 大致上是以 802.11a 为基础。事实上, 它与 802.11a 几乎完全相同, 只有少许显著的差异。最值得注意的是, 802.11g 采用了 802.11b 的频道规划, 因此仍然只有三个非重叠频道可以使用。(相邻频道重叠表, 详见第 13 章; 有关三个非重叠频道的注解, 同样适用于 802.11g。) 其所使用的帧间隔与时槽, 亦相容于使用 ISM 频段的旧式 802.11 工作站。不过, 802.118 的管制规定和 802.11b 有些差异。例如, 日本允许 802.11b 使用 1-14 频道, 不过只允许 802.11g 使用 1-13 频道。

14.1.2 防护机制

防护机制是 802.11b 与 802.118 的一项主要差异。之所以需要防护机制, 是因为实作这两种规格的芯片组间存在一种非对称性 (asymmetry)。设计人员面临的一个问题是, 802.118 所使用的调制机制与 802.11b 不同。802.118 芯片必须回溯相容, 并且能够正确接收与解读 802.11b 信号。如同技术领域常见的状况, 反之则不然。802.11b 芯片组无法解读较高速的 802.118 信号。解决方案的第一个部分, 是要求 802.118 工作站在基本服务组合进行传输时, 使用所有工作站均能够支持的速率。如果基站必须同时服务 802.11b 与 802.11g 工作站, 传送 Beacon 帧时, 就不能使用高于 11 Mbps 的数据传输率。

解决方案第二个部分, 则是要避免 802.118 与 802.11b 网络彼此干扰。为了确保 802.11b 工作站能够得知 802.118 正在进行传输, 802.11g 制定了一种防护机制, 以保护 802.11b 工作站免于受到干扰。防护机制的基本作业方式如图 14-1 所示。为了避免在 OFDM 帧及其回应讯息传送期间造成干扰, 必须传送一个较慢的帧来更新 NAV。防护机制主要有两种。通常, 802.118 工作站是使用「反身 CTS 防护」(CTS-to-self protection), 如图 14-1(a)所示。当工作站必须为待传帧采用防护机制时, 就会发送一个 CTS 帧, 并且将接收端位址设为本身的 MAC。换言之, CTS 帧的目的地为工作站本身 CTS 帧用来更新网络配置向量 (NAV), 告诉其他正在使用实体介质的工作站, 随后将占用无线链路多少时间, 以便传送 CTS。经 OFDM 调制的帧, 以及经 OFDM 调制的回应讯息。虽然工作站是将 CTS 传送给自己的, 不过网络上所有工作站都必须聆听 CTS 帧, 并且据以更新 NAV。CTS 帧是以可行的最高速率传送, 并且使用所有工作站均了解的调制方式。如此一来, 传输量必然会大幅降低。以最高速率传送最大的 Ethernet 数据帧及其回应总共需要 294 微秒, 不过用来净空网络的 CTS 帧至少需要 107 微秒。如果使用长同步信号的话, 可能需要 200 微秒以上的时间。

第二种机制是采用完整的 RTS/CTS 交换程序，如图 14-1(b)所示。完整的 RTS/CTS 交换程序在遭遇隐藏节点时比较可靠，不过必须牺牲一些传输量做为代价。以刚才的反身 CTS (CTS-to-self)为例，用来预订介质使用权的相容性帧，搞不好比传送数据占用更长的时间。RTS 与 CTS 各占用 100 微秒，而最大数据帧及其回应讯息总共也才用掉 300 微秒。将 RTS 所需要的额外时间纳入计算，我估计使用完整的 RTS/CTS 交换程序，会比使用反身 CTS 减少 1/3 左右的总传输量。【注】

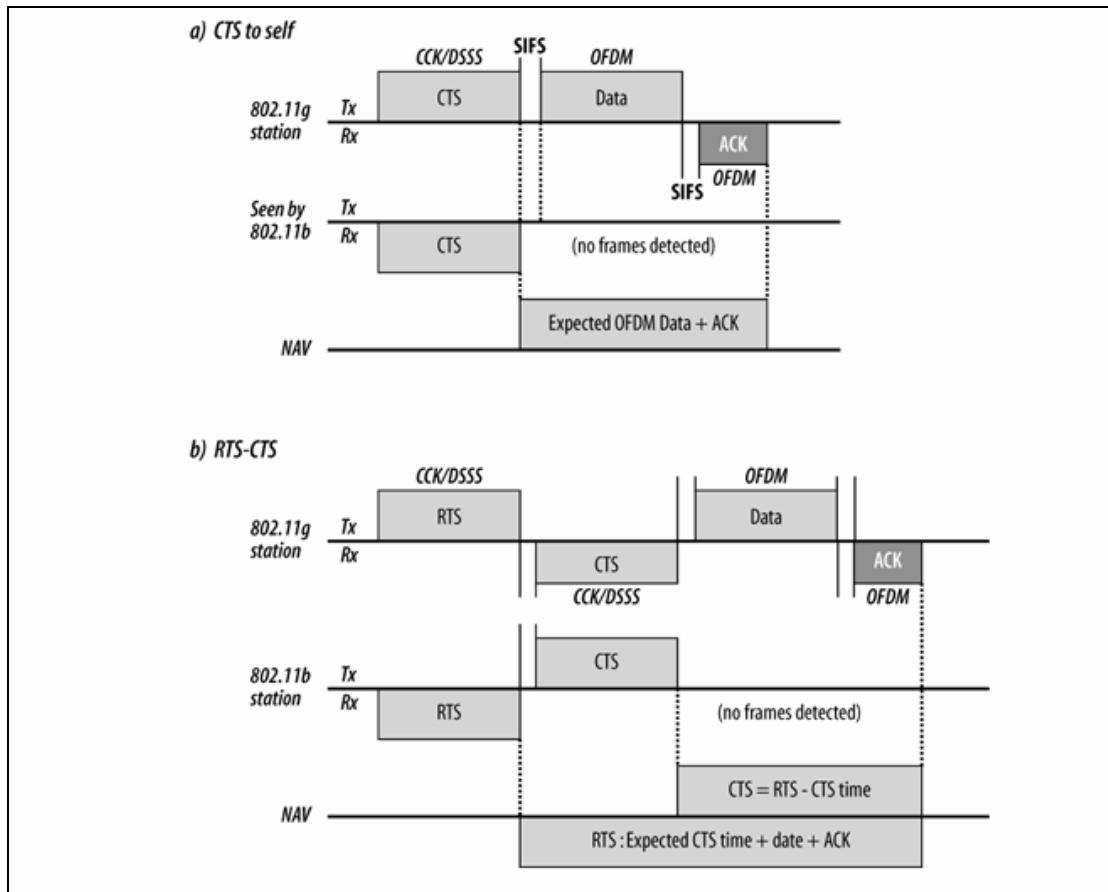


图 14-1：防护机制的基本作业方式

为了确保网络上所有工作站均能接收与处理防护帧，必须依循 802.11b 规范来传送防护帧。传送时可以使用 1 Mbps 或 2 Mbps 的相移键控，或者 5.5 Mbps 或 11Mbps 的 CCK。所有 802.11b 工作站均了解这种调制方式，并能据以更新本身的虚拟载波检测。图 14-1 显示了所使用的调制方式，而且只显示了 802.11b 工作站能够理解的相容调制方式。

注 详见<When is 54 Not Equal to 54: An Analysis of 802.119 Throughput>一文，网址为 http://aoww.oreillynet.com/pub/a/wireless/2003/08/OS/wireless_tbroughtout.html

只有防护帧需要以相容于 802.11 b 的数据率进行传输。防护机制并未要求 802.11 g 工作站在传递承载数据时也必须使用较低的速率，这是一般容易误解之处。

凡是需要确保 802.11b 工作站不致干扰 802.11b 工作站的场合，就得启用防护机制。比较明显的情况是 802.11b 工作站与基站进行连接时。此时所有与基站连接的 802.11b 工作站均会启动防护机制，以确保 802.11b 工作站不致于受到或造成干扰。比较不明显的场合，像是与 802.11b 基站共用频道的情况下也会启用防护机制。因为共用频道的两部基站必须分享实体介质，其他基站上使用相同频道的 802.11b 工作站也会触发防护机制。

防护机制系通过 Beacon 帧中的 ERP 信息元素来控制。802.11g 在 Beacon 帧的信息元素中加入了一个 Use Protection 位元。只要此位元设置为 1，工作站就必须使用防护机制。当一部非 802.11g 工作站连接到无线局域网络，此防护位元就会被设置。负责传送 Beacon 帧的工作站必须负责判断是否启用防护机制。在基础型网络里，防护机制是由基站所掌控。在独立型网络中，则是由 Beacon 发送者负责。每当非 802.11g 工作站连接到网络，或者该区有非 802.11b 工作站正在进行传输，就会启动防护机制。要判断工作站是否具备 802.11g 能力，可以从重叠网络所接收到的管理帧（包括 Beacon 与 Probe Response 帧）加以推论，观察其中是否包含 802.11b 所支持的速率。

802.11g 网络中的 Beacon 帧也可以用来控制同步信号的长度，藉此达到防护的目的。在 ERP 信息元素中，Barker Preamble Mode 位元可用来告诉所有已连接的工作站，究竟应该使用长同步信号或短同步信号。如果网络上所有工作站均能够使用短同步信号，则 Barker Preamble Mode 位元就会被设置为 0，并且所有工作站均将使用短同步信号以达到更高效率。不过，只要其中一部工作站无法使用短同步信号与网络连接，此位元就会被设置为 1，而且所有防护帧均将使用长同步信号。如同其他必须回溯相容的技术，802.11g 也会因此受到限制。如果不启用防护机制，802.11g 与 802.11a 的传输量不相上下。一旦启用防护机制，据我估算，大概只剩下 50% 传输量，这取决于 TCP 数据区段与 TCP 回应讯息两者的比例。通过 802.11 传送一个完整的 1,500 位元组 Ethernet 帧并且得到回应需时 428 微秒。如果使用「反身 CTS」防护机制，所需的时间就跳升为 557 微秒；RTS/CTS 会增加更多负担，同样的传输需时 774 微秒。有些 802.11g 基站不接受非 802.11g 工作站的连接要求，主要是为了避免使用防护机制。拒绝那些无法以 802.11g 速率连接的工作站，比较有机会不致启动防护机制。当然，被拒在外的工作站有可能会找到愿意接纳它们且使用相同频道的网络，如此一来仍会触发防护机制。

虽然 802.11g 能够达到 802.11a 的传输率，不过防护机制所占用的额外传输时间，或许会让数据传输量腰斩一半。ERP-PBCC 与 DSSS-OFDM 物理层不需要用到防护机制。两者均使用相容于 802.11b 的标头，因此不必传送额外的帧来更新虚拟载波检测与 NAV，如图 14-2 所示。802.11b 工作站能够解读标头，并且根据标头的内容来更新虚拟载波检测机制。除非介质解除锁定，否则不允许进行传输。虽然 802.11b 工作站无法解读帧的内容，但可以根据标头所提供的信息，避免造成干扰。不过，使用 ERP-PBCC 或 DSSS-OFDM 并非毫无代价。就某种意义而言，它们无异于随时使用防护机制，因为它们使用较长的标头。ERP-PBCC 与 DSSS-OFDM 所使用的标头无法丢弃，而且至少占用 96 微秒。相对地，常见的 ERP-OFDM 模式必须使用与 CTS 帧相同的标头，至少需要 107 微秒的传输时间，另外加上 10 微秒的 SIFS 间隔。不过，ERP-OFDM 只有在使用防护机制时才需要付出此种代价，但 ERP-PBCC 与 DSSS-OFDM 这两种模式则无法避免。

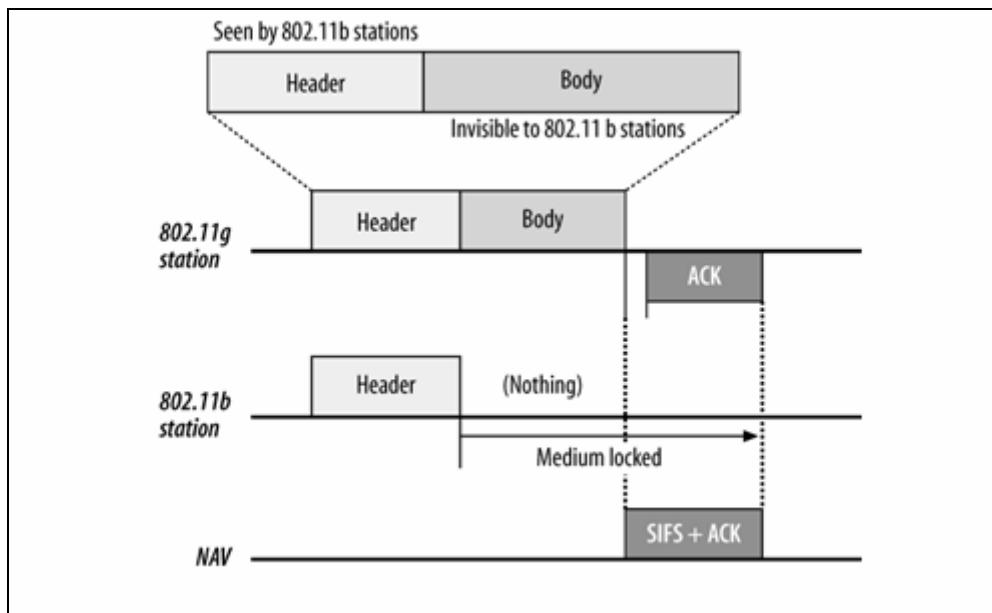


图 14-2: ERP-PBCC 与 DSSS-OFDM 的帧格式

14.2 ERP 的物理层收敛程序 (PLCP)

ERP PHY 的收敛附属层相当复杂。由于作业模式众多，要通过无线电波界面将帧传送出去就有好几种不同的方式。本章一开始所提到的各种模式，均自有一套物理层帧分封格式。

14.2.1 ERP-OFDM 的帧格式

此模式可说是本规格的核心，所有工作站均须实作此模式。一般所谓「支持 802.11g」即指 ERP-OFDM，因为大多数工作站预设使用此模式。事实上，了解 ERP-OFDM 物理层的帧格式，有助于了解大多数的 802.11g 传输作业。

ERP-OFDM 物理层所使用的帧格式，几乎和 802.11a 完全相同，如图 14-3 所示。ERP-OFDM 使用相同的逻辑协议数据单元，如图 14-3 最上方所示。事实上，它与 802.11a 的惟一差别，在于其后伴随 6 微秒的闲置时间。这段用来组装帧逻辑架构的时间，称为信号延伸 (signal extension)，如图 14-3 第二列所示。之所以需要这个额外的 6 微秒，是为了让时序的计算与帧的速率等同于 802.11a。802.11a 使用 16 微秒的 SIFS，部分时间是用来对上一个帧进行解码。为了回溯相容于 802.11b，802.11g 仍然采用 802.11b 所使用的 10 微秒 SIFS。因此，为了提供解码程序充裕的时间，802.11g 另外在帧后面加上 6 微秒，以便保留 16 微秒的间隔给硬件执行解码程序。当然，此时会一并设置 NAV，好让虚拟载波检测机制在信号延伸时间结束之际，能够回报介质的闲置状态。OFDM 传输显示于图 14-3 最下方，其与 802.11a 完全相同。

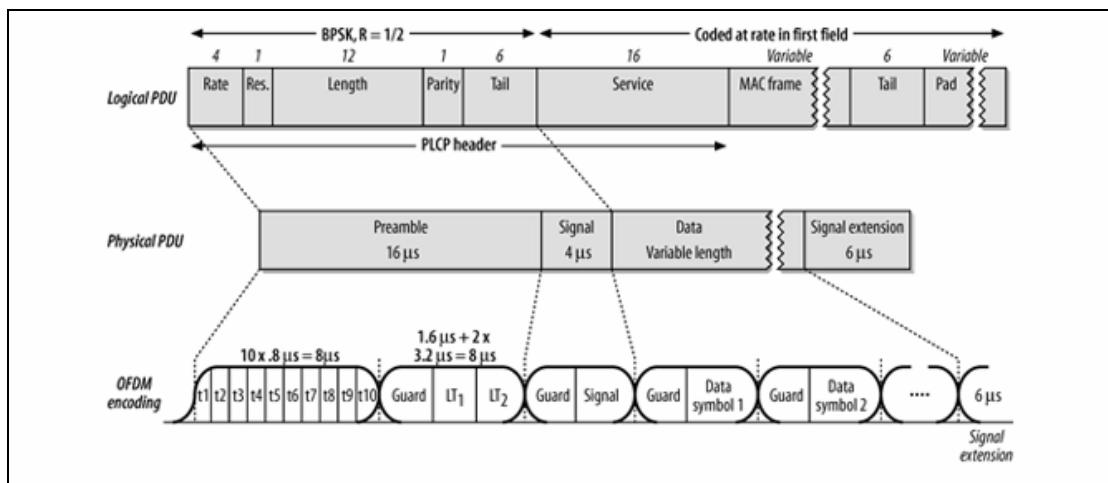


图 14-3: ERP-OF.M PLCP 帧格式

14.2.2 802.11 g 的单载波帧格式

虽然上一节所提到的 OFDM 是最常见的调制方式，不过较高速的数据内容，也可以使用相容于 802.11b 的帧格式。传统的帧封装方式可同时用于封包二进制迴旋编码以及 DSSS-OFDM 物理层。旧式的 802.11b 工作站也能够解读帧标头，因此可以避免在传输进行时访问介质，也无须用到防护机制。图 14-4 可以看到 802.11g 如何进行传统的单载波帧封装。

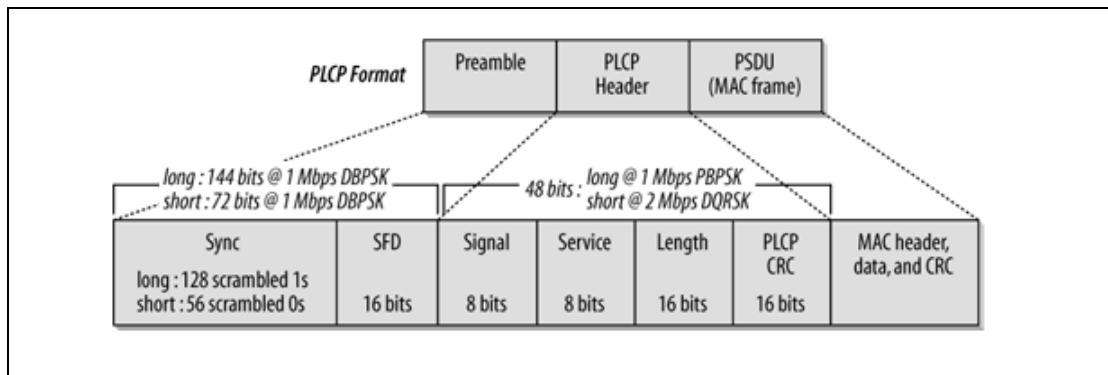


图 14-4: 采用长同步信号的 ERP PLCP 帧格式

Preamble

Preamble（同步信号）与第 12 章所提到的 802.11b preamble 相同，由一个同步（Sync）栏位，以及帧启始界定符（SFD）所组成。它可以是 144 位元的长同步信号，或者是 72 位元的短同步信号。不论长短，Preamble 均使用 DBPSK 调制，以 1 Mbps 的速率传输。调制之前，数据如同 802.11b 会先经过搅码。

PLCP Header

PLCP 标头与第 12 章所提到的 PLCP 标头相同。它是由 Signal、Service、Length 等栏位，以及一个 PLCP 层的 CRC 检查码所组成。Length 与 CRC 栏位的使用方式与 802.11b 相同。

Signal 栏位

此栏位用来指示 PLCP 承载数据（即 MAC 帧）所使用的调制速率。起初，它会被定义为 100 kbps 的倍数。由于此栏位只有 8 个位元，因此最高只能编码至 25.5 Mbps。为了容纳更高的速率，Signal 栏位改用数值来表示，如表 14-1 所示。基本上不需要通过 Signal 栏位来告诉接收器，DSSS-OFDM 帧使用何种编码率，这项任务由 OFDM 标头负责。

表 14-1：单载波帧标头中的 SIGNAL 栏位值

速率	Signal 栏位值 (十六进制/二进制)	Signal 栏位值, 十进制
1 Mbps (ERP-DSSS)	0x0A (0000 1010)	10
2 Mbps (ERP-DSSS)	0x14 (0001 0100)	20
5.5 Mbps (ERP-CCK, ERP-PBCC)	0x37 (0011 0111)	50
11 Mbps (ERP-CCK,ERP-PBCC)	0x6E (0110 1110)	110
22 Mbps (ERP-PBCC)	0xDC (1101 1100)	220
33 Mbps (ERP-PBCC)	0x21 (0010 0001)	33
其他的 DSSS-OFDM 速率	0x1E (0001 1110)	30

Signal 栏位

Service 栏位包含了一些控制位元，用来协助接收器对帧进行解码，如图 14-5 所示。如前所述，位元 0、1 与 4 目前保留未用，且必须设置为 0。所有 802.11g 工作站的传输与讯符时脉均会被锁定，因此位元 2 必然设置为 1。如果帧主体是以 PBCC 调制，位元 3 就会被设置为 1。如果是以 DSSS、CCK 或 DSSS-OFDM 调制，则位元 3 会被设置为 0。最后三个长度延伸位元则是用来协助接收器判断 Length 栏位所记载的帧长度。以位元组为单位，指示需要多少微秒来进行传输。标准当中有一套复杂的规则说明应该设置哪些位元，不过这些细节已经超乎本书的需要，何况单载波帧封装技术并不常用。

位元 Clock lock

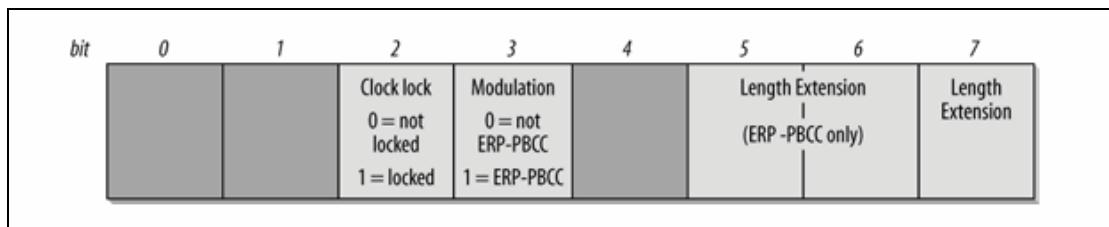


图 14-5：802.11 g 的 SERVICE 的栏位

帧主体

PLCP 帧最后的元件是它的承载数据，亦即 MAC 帧，以行调制。帧主体的调制细节，将在后续几节加以探究。

14.2.2.1 PBCC 编码

要使用 PBCC 传送帧，帧数据必须先经过迴旋编码。帧会被拆解成 2 个位元一组的元素，经过 旋编码，最后会输出予个位元。每一组予位元的区块会通过 8PSK 对映到一个讯符。接

收器只是反转整个程序，将每个相移转换为八种讯符之一。将讯符转换为 3 位元序列后，通过旋编码移除冗馀的位元，然后还原出原始数据。如图 14-6 所示。

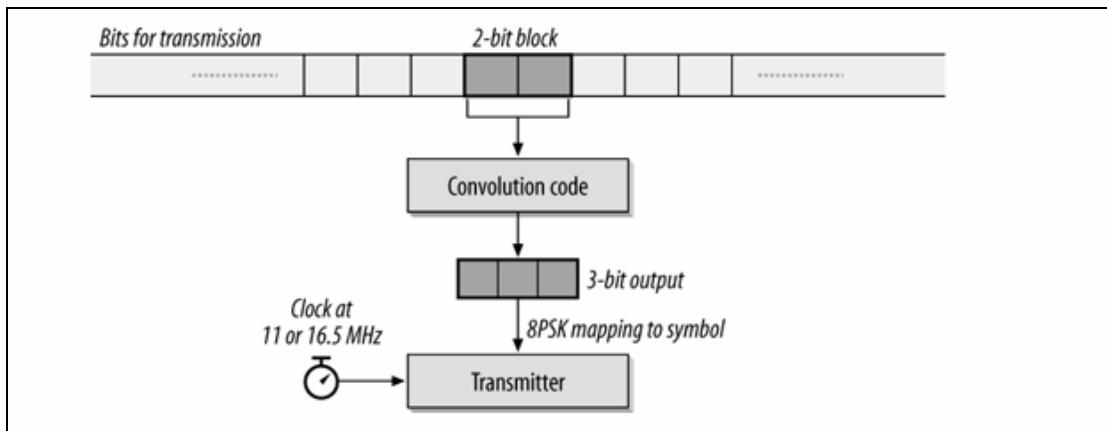


图 14-6：PBCC 处理程序

使用此种物理层编码要达到 22 Mbps 的传输率十分简单。讯符时脉，如同 802.11b 那样，维持在 11 MHz，但是每个讯符用来传递两个位元。若要达到 33 Mbps 的传输率，帧的数据部分必须使用 16.5 MHz 的讯符率。既然每个讯符可以传递两个位元，因此整体数据传输率即为 33 Mbps。切换时脉速度，必须在 PLCP 同步信号与承载数据之间的空档进行。

Atheros "Super G" 延伸功能

虽然过去几年速度已有显著的提升，无线网络还是不够快。最佳情况下，标准无线网络可以达到 30 Mbps 左右的传输量。在竞逐更高速率的过程中，几乎所有芯片组厂商均实作出一些延伸功能来提升速度。目前，最著名（或恶名昭彰）的算是 Atheros 的 Super G，其中包含三种不错的功能，另外一种功能则颇受争议。

区块回应（也称为帧宣泄）

在标准的 802.11 电波链路管理机制中，每个数据帧都必须伴随一个应讯息、之后工作站必须重新竞争介质的使用权。区块回应（block acknowledgment）让工作站得以连续传送几个帧，帧间以短帧间隔（SIFS）进行区隔，过程中无须竞争介质使用权。此帧序列伴随一佃区块回应讯息。只要是根据目前的 802.11e 草案进行开发，区块回应通常不至于造成厂商间的互通性问题。

封包丛集(Packet clustering)

802.11 帧可以承载多矜标准 1,500 位元组 Ethernet 帧的背料。尽可能装满数据有助改善数据负担比（payload-to-overhead ratio），并且提高速度二硬件压缩传输之前先将数据压缩可以缩短传输时间并且有效提升链路的传输量。存在冗馀数据（例如未经压缩的文字）时硬件压缩晕有效率。传送已压缩影像，效果就没那么显著了。合并频道（也称为 Turbo 模式）除了使用 22 MHz 的单一频道，也可以通过「合并频道」（channel bonding）功能，使频宽加倍。信号展开时若增加可用频谱，就可以在较宽的频道中塞进更多的位元。为了确保使用较大频宽时仍然符合管制规定的限制，有些产品限足只能在第 6 频道，丁即中央频段进行频道的合并。

目前，合并频道可说是 Super G 最具争议的功能。在 2003 年底，Eroadcom 指控 Super G 会干扰其他正常的 802.11g 传输，并在 Comdex 举办一场和人展示会。（我被拒绝入场）后续测试显示干扰的确存在，不过历现 Ilroadcom 品片组比其他厂商更界易受到影响 a Atheros 已经开发出一种监听模式。附近如有其他以 802.11g 标准进行传输的网络，则停止使用合并频道的功方匕。足以为舰的是，消耗更多稀有频谱的同时，合并频道的功能,9ft,更容易造成干扰。容易消耗频谱的传输模式不适用于需要多部塞地台的大

范围区域，因为原本已经少得可怜的可用频道，将由三个缩减为一个。合并频道设备在家中使用无妨，但不要部署在公司网络中。

14.2.2.2 DSSS-OFDM 帧格式

DSSS-OFDM 是一种混合型的帧封装技术。较上层封包以 OFDM 编码，经 OFDM 调制的封包，则是以传统的单载波标头封装，如图 14-7 所示。标头依 802.11b 标准进行传输（包含 802.11b 所使用的数据搅码器），帧主体则是通过 OFDM 加以调制，如第 13 章所提到的 802.11 编码程序。虽然编码方式类似 802.11a，不过 DSSS-OFDM 帧封装移除了一开始的短调整序列。此外，它新增了一个 6 微秒的信号延伸栏位，以便有充裕的时间完成解码程序。PLCP 标头结束后，必须从直接序列调制转换为 OFDM，从无线电工程的角度来看颇为复杂，不过这已经超乎本书的范围。

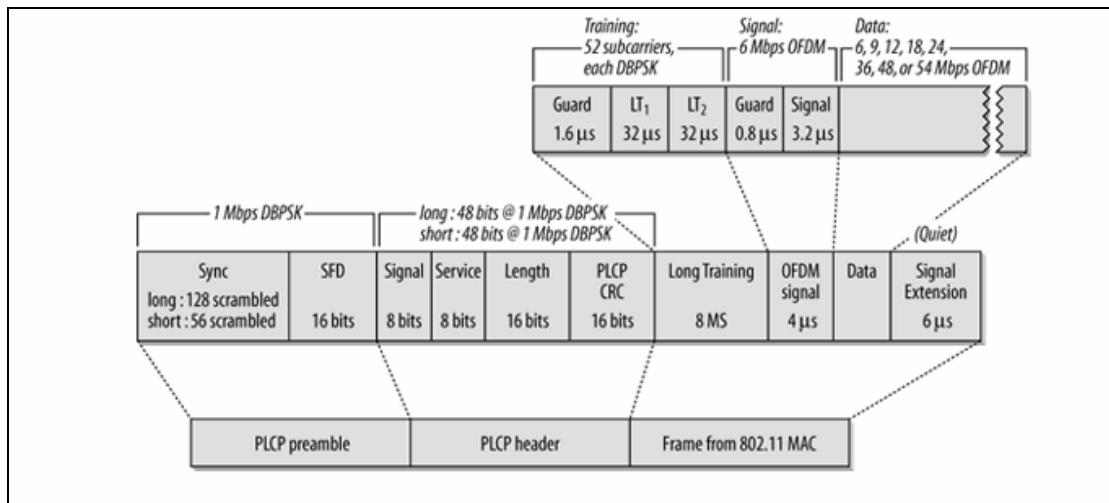


图 14-7：DSSS-OFDM 帧格式

14.3 ERP 的实际搭酬介质 (PMD)

一旦 PLCP 帧准备就绪，便会通过 PMD（实际搭酬介质）加以传送。PMD 负责取得数据经由天线传送。由于可使用的调制机制种类颇多，802.11 收发器必须实作好几种不同的传输模式（不论完整与否），并在必要时进行切换。不过，有些功能是收发器共通的，与作业模式无关。

14.3.1 净空频道评估 (CCA)

802.11g 只定义了一种 CCA 模式，除了检测能量的最低门槛，也用来解读信号。在传输时槽 (transmission slot) 开始时，若接收到功率高于 -76 dBm 的信号，则视括有效信号。在效能要求方面，在特定时间内，物理层正确回报介质处于忙碌状态的机率，必须大于某个数值。所需要的时间间隔与机率如表 14-2 所示。

表 14-2：802.11g 的 CCA 效能需求

	长时槽 (20μs)	短时槽 (9μs)
CCA 时间	15μs	4μs
检测频率	>99%	>90%

CCA 与 PLCP 层次的虚拟载波检测 (virtual carrier sense) 机制整合在一起。接收到 PLCP 标头时，其中会包含化 ng 属性，显示介质将忙碌多久时间。这段时间内，物理层将持续回报介质处于忙碌状态，就算物理层信号已经漏失。（不论是概念上或作业上，这种做法都类似于 MAC 层的网络配置向量。）之所以采取这种做法，部分是因为并非所有实作均支持所有的传输模式，因此物理层正确地避免干扰其所无法解调的传输就相当重要。

14.3.2 接收程序

相较于其他标准，802.11g 工作站的接收程序比较复杂，因为必须顾及回溯相容性。接收帧时，802.11g 工作站必须使用正确的物理层加以检测与解调。

1. 帧的同步信号，究竟属于 OFDM（如同 802.11a）或者 802.11b 所使用的传统单载波？以 OFDM 调制的帧将使用与 802.11a 帧相同的程序处理，只是所使用的接收频率不同。
2. 如果不是 OFDM 帧，则必须对同步信号进行解码，然后在同步信号的结尾找出 PLCP SIGNAL 与 SERVICE 栏位。
3. PLCP 标头解码后，便可以采用适当的调制方式，对帧主体进行解调。
 - a. 如果 SERVICE 栏位显示此帧是以 PBCC 调制的，便会触发 PBCC 接收程序。
 - b. 如果 SERVICE 栏位并未显示任何使用 PBCC 的迹象，便会进一步检视数据传输率。若传输率为 1 与 2 Mbps，则以 DSSS 接收演算法进行处理，若传输率为 5.5 Mbps 与 11 Mbps，则以 CCK 接收演算法进行处理；两者在第 12 章均已说明过。
 - c. 如果 SIGNAL 栏位显示传输率为 3 Mbps，则使用 DSSS-OFDM 接收程序 PLCP 标头结束后即切换为 OFDM 解调器。

14.3.3 ERP 物理层的特性

802.11g 与 802.11a 的特性十分相似，只有一项比较值得注意的例外。虽然 802.11g 的频道效能与 802.11a 相当，但只有三个频道可用。就算每个频道以最高速率运行，并且达到 50% 的效率，整体传输量也只有 81 Mbps。虽然这个数字不差，仍然无法和 802.11a 相提并论。

表 14-3：ERP 物理层参数

参数	值	备注
最大 MAC 帧长度	4095 个位元组	
槽位时间	20us 9us	如果网络上只有 802.11 g 工作站，便可以缩短槽位时间从相容于 802.11 b 的 20 us，缩短为 802.11 a 所使用的 9 us。
SIFS 时间	10us	SIFS 可用来推导出其他帧间隔值 (DIFS, PIFS 以及 EIFS)
信号延伸时间	6us	每个 802.11 g 封包均伴随此信号延伸时间
竞争期间的大小	15 或 31 至 1023 个时槽	如果工作站只支持 802.11 b，为了相容必须使用 31 个时槽。否则可以使用较短的竞争期间。

参数	值	备注
同步信号持续时间	20us	

第15 章 802.11n 前瞻 :MIMO-OFDM

802.11 任务小组 N (TGn) 的目标很有意思。大部分 IEEE 任务小组的焦点在于提升最高传输率，让数据能够尽快传输。TGn 的目标是在扣除协议管理功能（例如同步信号、数据帧间隔以及回应讯息）所造成的负担后，达到 100 Mbps 的净传输率。仅管目标是 100 Mbps 的净传输率，最终提案似乎不难超越原先设置的数字，最佳情况下甚至能够提供好几倍的传输率。要达到 100 Mbps 有两种方式：改善 MAC 的效能，将最高传输率拉到 100 Mbps 以上，或两者并行。

TGn 任务小组总共收到六份完整的建议书，不过焦点在其中两份，分别由 TGnSync 与 WWiSE ("World-Wide Spectrum Efficiency"的简称) 阵营提出。双方阵营均包含芯片制造商。Atheros、Agere、Marvell 与 Intel 属于 TGnSync 阵营；Airgo、Broadcom、Conexant 与 Texas Instruments 则是 WWiSE 的核心厂商。此外，不少用到 802.11 的电子设备制造商 (Cisco、Nokia、Nortel、Philips、Samsung、Sanyo、Sony 与 Toshiba) 也参与规格的制定，但大多倾向 TGnSync 阵营。

拉高层次来看，这两份建议书十分类似，仅管强调的重点不同。其中一方强调最高传输率的提升，另外一方则是侧重 MAC 效能的改善。在许多配置上，两者均采用「多进/多出」(multiple-input/multiple-output，简称 MIMO) 技术，并且回溯兼容于同频段的旧系统。操作上，两者均支持目前的 20 MHz 频道，另外可望使用两倍宽的 40MHz 频道来提升传输率。

标准之争才在全球的 IEEE 会议开打，市面上就已经出现所谓的 pre-N 基站，内部采用 Airgo 的芯片组。在标准出炉之前购买这类产品，有点像是在赌运气。当初 pre-G 产品问世时，任务小组虽然才刚起步，至少只需要与一份建议书奋战。目前，TGn 还处于“双份建议书”(dueling proposal) 的阶段，根本无法保证未来是否能以软件升级的方式，更新为最后的 802.11n 标准。“802.11n 可能是这十年内最后一份物理层标准。标准的开发既是技术工程，也是政治工程。IEEE 要求建议书在成为标准的基础之前，必须得到 75% 以上的支持度。本书即将付印时，虽然 TGnSync 得到大多数厂商的支持，但仍低与必要的 75%。预料对立阵营所提出的功能将被整合到未来的建议书中，好让支持率提升到必要水准。因此，本章将针对这两份建议书的内容提出说明。虽然 TGnSync 或将成为 802.11n 规格书的基础，终究还是会纳入许多 WWiSE 的功能。

本章会同时描述 WWiSE 与 TGnSync 这两份建议书。最后的标准将与之类似，并从中挑选出必要的功能。幸运的是，两者所用到的一些基本概念是共通的。当各位阅读至此，切记本章所依据的建议书草案尚有可能历经一番变动。

15.1 共同功能

虽然这两份建议书有所差异，两者间其实具备不少共同点，实际上，为了达到 100Mbps 的传输率，有些功能是不可或缺的。

15.1.1 多进与多出 (MIMO)

2004 年之前，802.11 接口仅使用单一天线。虽然有些接口使用两支天线做为天线分集，不过天线分集只是选用信号最佳的天线。就天线分集而言，任一时点都只用到单一天线。就算配置两组以上的天线，也只用到其中一组元件来处理信号或射频链路(RF chain)。接收器只有一组输入链路 (input chain)，发射器也只有一组输出链路 (output chain)。

为了进一步超越天线分集，必须将射频链路分配给系统天线。这就是多进/多出(MIMO【注】)操作的基础。任一射频链路均能够同时接收或传送，如此可以大幅提高传输率。此外，接收器平行处理的好处在于能够解决多重路径干扰的问题，也可以改善接收信号的品质，远胜过单纯的天线分集。个别射频链路及相应的天线负责传送空间串流(spatial stream)。单一数据帧可以经过拆解，多工处理后以多组空间串流传送，接收器再加以重组。WWiSE 与 TGnSync 建议书均采用 MIMO 技术来提高数据传输率，虽然两者的应用方式不同。

MIMO 的天线配置通常表示成「YxZ」，其中 y 与 z 均为整数，分别代表传输天线与接收天线的数量。举例而言，WWiSE 与 TGnSync 均将 2x2 操作列为必要，亦即使用两组传输链路，两组接收链路，以及两道或多工处理·以电波链路传送的空间串流。

注 MIMO 念成“*MyMoe*”。我曾经参加一场研讨会，一位委员提到，标准委员会曾就 MIMO 的念法进行表决。这两份建议书中尚包含其他必要(**required**)与选项(**optional**)模式。预料两者将采用相同的硬件配置，在用户端使用两组 RF 链路以节省电池电力，而在基站使用三组以上的 RF 链路。此种配置将使用 2x3 MIMO 做为上行链路(**uplink**)，以 3x2 MIMO 做为下行链路(**downlink**)。

15.1.2 频宽

802.11a 目前使用 20 MHz 频道，因为这是所有管制单位一致允许的频宽。理论上，将频宽倍增至 40 MHz，频道的传输率也会因此倍增。虽然可望在未来开放，一些管制当局目前并不允许 40 MHz 操作。日本是最明显的例子。

15.1.3 MAC 效能的提升

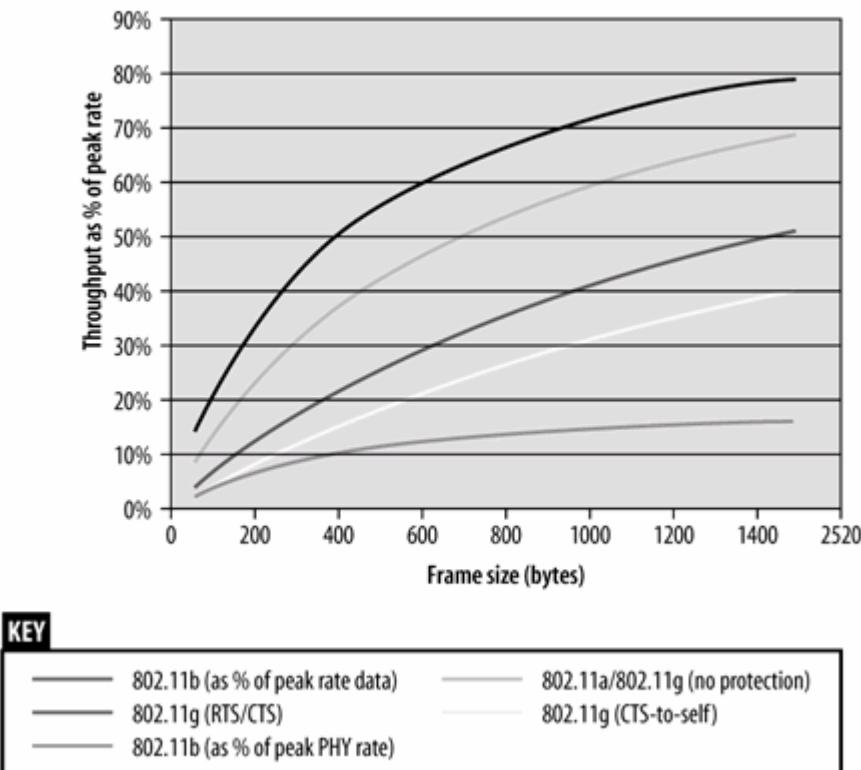
本书再三强调，802.11 MAC 效能一向很差。大多数情况下，它很难达到硬件层额定位元率(**nominal bit rate**)的 50-60%以上。每个待传数据帧都需要用到硬件层数据帧标头，以及只会造成负担的同步信号。802.11 MAC 要求每个数据帧都需要得到回应，这也是额外的负担。对小型数据帧而言这些负担更是沉重，因为它们可能比数据帧数据本身用掉更多传输时间。MAC 的效能，定义为【各种长度的数据帧中，MAC 承载数据(**payload data**) 占额定位元率的比例】，如图 15-1 所示。图中所标示的数值代表 MAC 承载数据。任何网络量测都必须加计额外的 LLC 数据，经加密的网络也会有额外的负担。此外，大多数网络协议都会提供本身的回应机制，这进一步拖累了实际的效能。图 15-1 的重点在于：数据帧愈小，效能愈差。

TGnSync 与 WWiSE 采用了一些技术来改善电波频道的效能。虽然概念相似，但是细节不同。两者均采用某种形式的区块回应(有时也称为数据帧宣泄)。如果不需要个别回应，就可以减少 ACK 数据帧、同步信号与分封所造成的负担。区块回应虽然有用，但在数据帧宣泄期间不能有任何闪失。只要漏掉任何数据帧或回应讯息就会严重影响协议的操作，整个区块必须予以重传。

数据帧的合并(**frame aggregation**)也同时见于这两份建议书。802.11 所承载的封包有时很小。互动式网络连接(例如 telnet 或 SSH)的封包通常很小，但需要立即传送。封包较小，数据帧也就跟着变小。每个小型数据帧都需要硬件层分封。因此造成额外的负担。将一些小型封包组合成较大的单一数据帧，有助于改善「数据负担比」(**data-to-overhead ratio**)。数据帧的合并通

常会搭配 MAC 标头压缩，因为目的地相同的数据帧会有相当类似的 MAC 标头。

Figure 15-1. MAC Efficiency



15.2 WWiSE

WWiSE 联盟的参与者包含了若干著名的芯片制造商：Airgo（首部 pre-N 设备制造商）、Broadcom、Conexant 以及 Texas Instruments。Motorola 于 2005 年 2 月加入此阵营，刚好在本书付印之前。

15.2.1 MAC 的改良

从名称上标榜光谱效能（spectral efficiency）即可预料，WWiSE 比较侧重 MAC 效能的改善。为了达到 100 Mbps 的净传输率，必须在 960 微秒的时间内传送 12,000 个位元组（960,000 个位元）。使用两组天线搭配两道数据串流的基本配置，WWiSE 硬件层规格可以有 135 Mbps 的传输率，在 711 微秒之内传送所有数据。其余的 249 微秒则是用于同步信号、分封、数据帧间隔以及单一区块回应。

15.2.1.1 频道与电波模式

WWiSE 同时使用 20 MHz 与 40 MHz 两种频道。40 MHz 操作可以使用单一 40 MHz 频道，或者一对同时用来传送数据的 20 MHz 频道。其中一个频道做为主频道，使用正常的操作方式。第二个频道只用于频道的合并（channel aggregation），不会让工作站与之连接。第二个频道用来承载主频道【溢出】（overflow）的流量；载波检测功能只在主频道进行。

虽然双频道操作属于硬件层，但是仍旧免不了若干 MAC 层操作。主频道的 **Beacon** 数据帧中会加入一个新的信息元素 **Channel Set**，让工作站得以被通知第二个频道的存在。基站也会在第二个频道发送 **Beacon** 数据帧；和一般 **Beacon** 操作不同的是，这么做的目的是为了避免工作站与之连接，或者避免其他设备选用此频道进行操作。第二频道的 **Beacon** 数据帧与主频道的 **Beacon** 数据帧类似，但只支持必要的 MIMO PHY 传输率。为了进一步避免他人使用此频道，也会包含 **contention-free** 信息元素。

15.2.1.2 防护机制

如同 802.11g，这些新式硬件层必须改良现有的防护机制，方能避免干扰现有的工作站。当然，使用 2.4GHz 的工作站必须采用 802.11g 所规范的防护机制，方能避免干扰其他较旧的直接序列或 802.11b 设备。如果基站检测到旧式设备，就会启动第 14 章所描述的 RTS-CTS 或 CTS-to-self 防护机制。

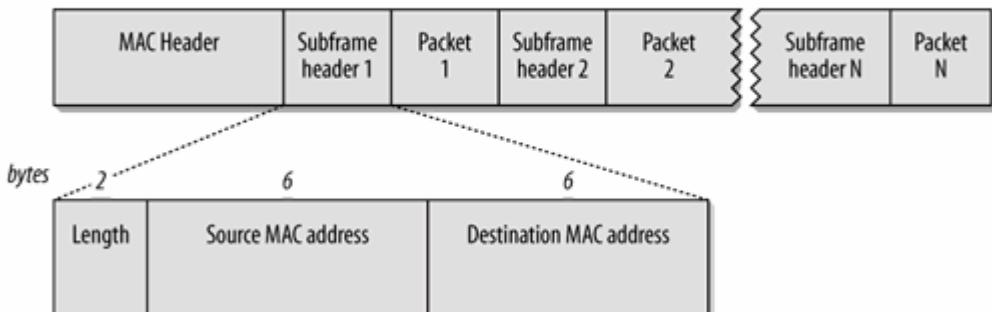
不过，为避免 MIMO 工作站以 802.11a 或 802.11g 设备无法理解的速率进行传输，必须设计一些额外的防护机制。WWiSE 建议书提出一种 OFDM 防护机制，允许 MIMO 工作站以适当的方式设置旧式 OFDM 工作站的 NAV。它相当于第 14 章所描述的防护机制，但使用 OFDM 数据传输率。

最后，WWiSE 建议书使用 **Beacon** 数据帧中 **ERP** 信息元素里的两个位元，指示是否需要用到 OFOM 防护机制。在某些情况，可能需要用到 OFDM 防护机制来协助 802.11g 网络，但无须提供 802.11b 工作站防护机制。基站会监控电波链路，判定是否需要 OFDM 防护机制为了协助使用成对频道的工作站，也会指示是否使用第二个频道。

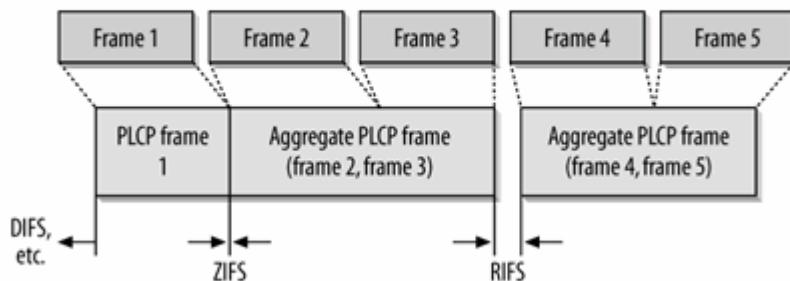
15.2.1.3 数据帧合并、数据帧宣泄与回应

WWiSE 建议书把可承载数据的最大长度，从 2,304 位元组提高到 8,000 以上。可承载数据变多相当于提升「数据负担比」，因此可以提升整体效能，如果较大的数据帧或数据帧宣泄能够顺利传送的话。

数据帧的合并是将几个较上层网络协议的封包封装在单一数据帧。每个封包均包含一个带有来源与目的位址的次数据帧标头，以及指定封包大小的长度栏位，如图 15-2 所示除非所要封装的各数据帧之 **Address 1**（数据帧的接收端）栏位值皆相同，否则无法合并数据帧。在基础型网络里，来自基站之数据帧的 **Address 1** 栏位代表目的地，因此基站只能合并传给单一工作站的数据帧。不过，基础型网络里的工作站可以合并传至不同目的地的数据帧。工作站会在 **Address 1** 栏位填入基站位址，因为传递至骨干网络之前，所有数据帧都必须经过基站处理。合并数据帧时，目的位址是「下一个」（**nexthop**）处理工作站，来源位址则是数据帧的产生者。拆解数据帧时，各个子数据帧(**subframe**) 将根据各自的标头进行处理。由于接收端位址必须相同，因此无法同时合并单点传播、组播与广播数据。建议书中并未规范何时该合并数据帧。

Figure 15-2. Aggregation in WWiSE

数据帧宣泄（bursting）是与数据帧合并相关，但稍有不同的概念。数据帧合并汇集了较上层协议的封包，以较大的数据量进行传输。数据帧宣泄在硬件层采取同样的做法。一旦工作站付出相当的代价取得了频道的控制权，就可以持续进行传输。相对于较上层数据帧，使用多个硬件层数据帧的优点，在于能够指定各个数据帧的来源与目的位址。数据帧宣泄可以包含传送到不同目的位址的传输操作。数据帧宣泄另外定义了两种数据帧间隔，称为「零数据帧间隔」(Zero Interframe Space, 简称 ZIFS)与「缩短型数据帧间隔」(Reduced Interframe Space, 简称 RIFS)。传输功率相同的连续数据帧，可以用 ZIFS 立即传送。如果数据帧的传输功率有所变动，则使用 RIFS。然而 RIFS 短于其他数据帧间隔，这让工作站得以持续掌控频道。图 15-3 中，第一个数据帧无法被合并，必须等到传送者掌控频道后方能传送。一旦取得控制权，它就可以在允许的时限内持续掌控频道。第二与第三个数据帧使用相同的传输功率，因此在 ZIFS 后进行传送。此外，它们的 Address 1 栏位值相同，因此被封装到同一个「合并数据帧」。要传送下一个数据帧，必须调整所使用的传输功率，因此得使用 RIFS。第四与第五个数据帧可以合并，当成单一「合并数据帧」传送。等到队列中的数据传送完毕，工作站随即释放频道的控制权。

Figure 15-3. Bursting in WWiSE

802.11 MAC 的最初版本规定，每个单点传播数据数据帧必须得到一个正面回应讯息 (positive acknowledgment)。WWiSE 移除了此项限制，允许使用较具弹性的回应政策，数据帧的传送可以不用得到正面回应，或者使用区块回应代替。

15.2.2 WWiSE MIMO 硬件层

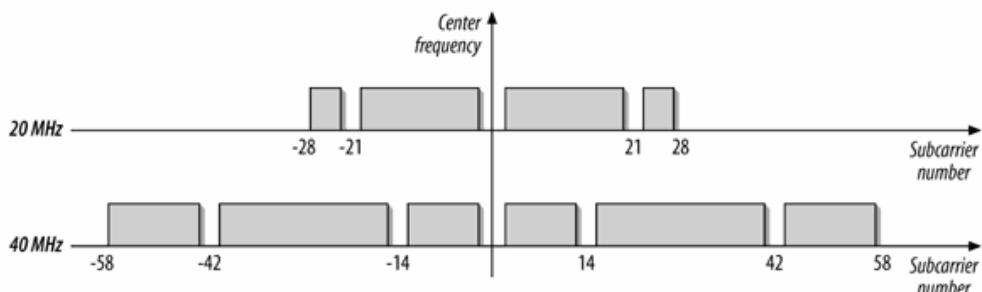
WWiSE 建议书是从 802.11a 演变而来，使用 MIMO 技术。基本的频道访问机制维持不变，OFDM 编码方式亦然。拉高层次来看，WWiSE PHY 主要是用来为各个位元指定不同的天线。

15.2.2.1 操作频道的结构

如同 802.11a，无线电频道的划分系以 0.3125 MHz 为副载波间隔。和 802.11a 的频道切割一样，在 WWiSE 建议书中，20 MHz 的频道被划分为 56 个副载波，40 MHz 频道则被划分为 112 个副载波。40 MHz 频道并非必要（optional），也只能用于 5GHz 频段，因为 ISM 频段根本挤不出几个 40 MHz 频道。（如果各位认为以三个频道进行网络规划已经很难，不妨试试看两个频道的情况）图 15-4 显示了 WWiSE 建议书中所规范的 20 MHz 与 40 MHz 操作频道。

如同 802.11a，其中有几个副载波(subcarrier) 会被设为导波(pilot carrier)，用来监控无线链路的效能。MIMO 系统用到较少的导波，因为导波涵盖好几个接收链路。20 MHz 的 802.11a 频道使用了 4 个导波。在 WWiSE 建议书中，20 MHz 的频道只需要两个导波，因为每个导波系由两个接收链路处理，效果相当于以单一接收链路处理四个导波由于导波数较少，多出来的副载波就可以用来传递数据。20 MHz 的 WWiSE 频道有 54 个数据副载波；40 MHz 频道则有 108 个，刚好是前者的两倍。

Figure 15-4. WWiSE pilot carrier structure



15.2.2.2 调制与编码

WWiSE 建议书并未规范新的调制速率。它广泛使用 16-QAM (4 个位元) 与 64-QAM(6 个位元) 调制技术，但不需要十分精确的调制星座图（modulation constellation）。

至于编码方面，则有所改良。WWiSE 新增 5/6 的迴旋编码率。如同 802.11a 所定义的 2/3 与 3/4 编码率，5/6 编码是将输出镂空得来的较高编码率。WWiSE 还定义了低密度同位元检查 (low density parity check, 简称 LDPC) 码的用法。

15.2.2.3 交错器

在 802.11a 中，交错器（interleaver）负责为各位元指定其所使用的副载波。MIMO 交错器比较复杂，因为除了指定位元在频道本身的位置，尚须指定位元所使用的空间串流。WWiSE 交错器从前溯错误编码器（forward error coder）取得传送位元，然后轮流分配给每个

空间串流。第一个位元指派给第一个空间串流，第二个位元指派给第二个空间串流，依此类推。交错器也负责每个空间串流中编码位元的编码事宜。

15. 2.2.4 时空区块编码

通常，每道空间串流由一组天线来传递。不过有时候，天线数可能远多于空间串流数。举例来说，如果基站使用三组天线，而工作站使用两组天线，就会出现所谓的“额外”传输天线，亦即两道空间数据串流必须指派给三组天线。通过多组天线来传道单一空间串流，称为「时空区块编码」（space-time block coding，简称 STBC）。

将一道空间串流划分给几组天线的基本规则，就是以不同天线传送两道相关串流。如第十三章对 802.11a 所做的说明，无线电波是由「同相」（in-phase）与「正交」（quadrature）两种信号组成，正交信号落后同相信号四分之一周期。数学上，其相移表现为星座图中复数的虚数部分。两个复数共轭指的是，它们的实数部份相同，但虚数部分的正负号相反。实际上，由共轭复数所形构的无线电波具备相同的「同相」信号，不过「正交」信号的相移刚好相反。如果有多余的天线，WWiSE 建议书要求，必须使用同一对天线来传送空间串流及其共轭复数。使用规则如表 15-1 所示。切割空间串流的规则与频宽无关，但 40 MHz 的空间串流显然能够承载更多位元的数据。

Table 15-1. WWiSE encoding rules when antennas outnumber spatial streams

Transmit antennas	Spatial streams	First spatial stream	Second spatial stream	Third spatial stream
2	1	Coded across antennas 1 and 2	N/A	N/A
3	2	Coded across antennas 1 and 2	Transmitted normally on third antenna	N/A
4	2	Coded across antennas 1 and 2	Coded across antennas 3 and 4	N/A
4	3	Coded across antennas 1 and 2	Third antenna	Fourth antenna

15. 2.2.5 调制速率

WWiSE PHY 定义了 24 种数据率，以及 49 种不同的调制选项。为了节省空间，此处只列出数据（传输）率的基本公式，不再列出表格：

$$\text{Data rate (Mbps)} = 0.675 \times \text{channel bandwidth} \times \text{number of spatial streams} \times \\ \text{coded bits per subcarrier} \times \text{code rate}$$

Channel bandwidth (频宽)

20 MHz 的频道此值为 20 • 40 MHz 的频道或成对频道此值为 40。

Number of spatial streams (空间串流数)

空间串流数可以是 1、2、3 或 4。它必须小于或等于传输天线数。建议书规定，至少必须支持两道空间串流。

Coded bits per subcarrier (副载波的编码位元数)

大多数情况下，64-QAM 为 6 位元而 16-QAM 为 4 位元。BPSK（每个副载波编码 1 个位元）与 QPSK（每个副载波编码 2 个位元）只能用于 20 MHz 且只有一道空间串流的频道。

Code rate (编码率)

16-QAM 可以搭配 $\frac{1}{2}$ 或 $\frac{3}{4}$ 的编码率 64-QAM 可以搭配 $\frac{2}{3}$ 、 $\frac{3}{4}$ 或 $\frac{5}{6}$ 的编码率。

要达到相同的数据率，有几种不同的方式。例如，有 4 种方式可以达到 108 Mbps：

- ◎ 使用 4 道 20 MHz 的空间串流，以 16-QAM 搭配 $\frac{1}{2}$ 的编码率($R=1/2$)。
- ◎ 使用 2 道 20 MHz 的空间串流，以 64-QAM 搭配 $\frac{2}{3}$ 的编码率 ($R=2/3$)。
- ◎ 使用 1 道 40 MHz 的空间串流，以 64-QAM 搭配 $\frac{2}{3}$ 的编码率($R=2/3$)。
- ◎ 使用 2 道 40 MHz 的空间串流，以 16-QAM 搭配 $\frac{1}{2}$ 的编码率 ($R=1/2$)。

在使用单一空间串流的基本模式中，频道的性能 (capacity) 稍高于 802.11a。因为所使用的导波数量较少。单一频道调制最高可达 60.75 Mbps，而非 802.11a 的 54Mbps。如果将所有参数调至极限（4 道 40MHz 的空间串流，以 64-QAM 搭配 $\frac{5}{6}$ 的编码率），WWiSE 建议书的传输率最高可达 540 Mbps。

15.2.2.6 MIMO 与传输模式

之前的 802.11 硬件层规格使用相当简单的传输模式。WWiSE 建议书提出了 14 种传输模式，使用哪一个取决于三项因素：

- ◎ 传输天线数，以 xTx 表示。其中 x 代表传输天线数。其范围从 1 至 4，不过单一天线只能用于 40 MHz 频道。所有 20 MHz 的频道至少必须使用两组天线，但可以只使用一道空间串流。
- ◎ 将数据帧用于 Greenfield (简称 GF) 模式或 mixed mode (混合模式，简称 MM) 的环境。混合模式使用回溯相容于其他 OFDM PHY 的硬件层标头，GF 模式则是使用速度较快的硬件层标头。
- ◎ 频道的宽度，可以是 20 MHz 或 40 MHz。

15-2 列出所有 14 种传输模式。每一种模式各自定义了几种不同的硬件层编码方，将于 PLCP 一节探讨。主动天线 (active antenna) 数与空间串流数只有粗浅的关连。以 4Tx40MM 模式进行操作的系统具备 4 支天线，但可以仅使用两道或三道空间串流。

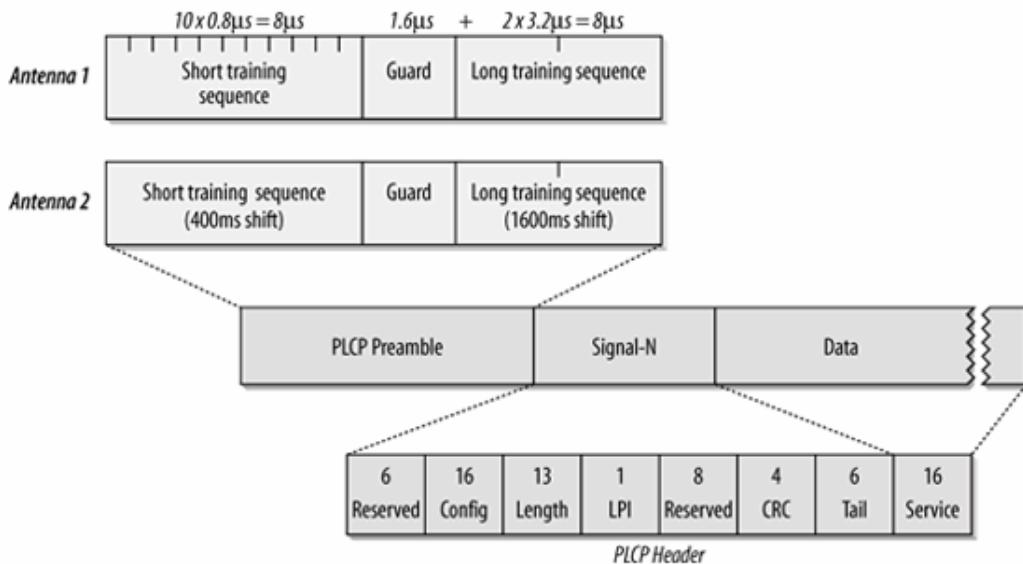
Table 15-2. WWiSE transmission modes

	20 MHz channels	40 MHz channels
Greenfield	2TX20GF	1TX40GF
	3TX20GF	2TX40GF
	4TX20GF	3TX40GF
		4TX40GF
Mixed mode	2TX20MM	1TX40MM
	3TX20MM	2TX40MM
	4TX20MM	3TX40MM
		4TX40MM

15.2.3 WWiSE PLCP

PLCP 必须能够操作于两种模式。操作于 Greenfield 模式时，PLCP 不会使用回溯相容的硬件层标头。Greenfield 的访问比较简单：它可以不用回溯相容。图 15-5 显示了 1TX40GF、2TX20GF 与 2TX40GF 所使用的 PLCP 封装格式。

Figure 15-5. Greenfield 1TX40 and 2TX20/2TX40 modes



数据帧中各个栏位的名称与用法，类似于本书其他章节所提到的其他 PLCP 数据帧。

MIMO-OFDM PLCP Preamble 栏位

此栏位包含已知的位元序列，协助接收器锁定信号。Preamble 可能划分为几个部分，取决于采用何种传输模式。它通常同时包含长短两种调整序列（training sequence）。在 WWiSE 建议书中，所有天线均会传送相同的同步信号，但有稍微的时间差。图 15-5 可以看到双天线传输模式所使用的调整序列。虽然调整序列包含不同位元，但时间差是一样的。当然，单天线 40 MHz 模式仅会使用一组主动天线来传送一组同步信号。

SIGNAL-N 栏位

SIGNAL-N 栏位中包含解读数据串流时所需要的信息。它通常以 QPSK • R=1/2 的编码率进行传送，而且未经编码。其中包含空间串流数、频宽、调制与编码的相关信息，以及一个 CRC 检查码。稍后将更进一步说明 SIGNAL-N 栏位的相关细节。

SERVICE 栏位

SERVICE 栏位与 802.11a 的用法相同。不同于 PLCP 标头的其他栏位，它位于硬件协议单元的 Data 栏位中，以内嵌之 MAC 数据帧的数据率进行传送。前 8 个位元设置为 0。和其他硬件层一样，传送 MAC 数据帧前会先经过编码；前 6 个位元设置为 0，是为了初始化编码器。其余 9 个位元目前保留未用，另有他用之前必须设置为 0。

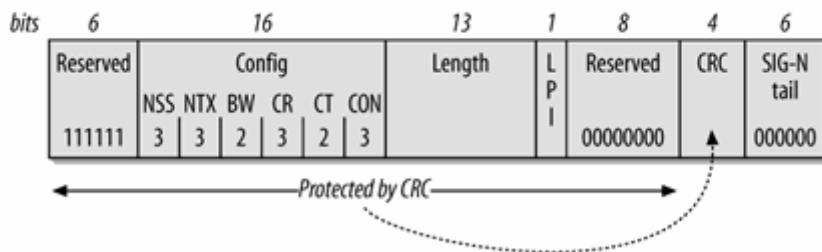
Data 栏位

最后一个栏位是一系列历时 4 微秒的讯符，用来承载数据。最后 6 个设置为 0 的结尾位元，用来结束错误更正码，并以填充位元(pad bits)使得讯符区块的长度变为偶数。

15.2.3.1 SIGNAL-N 栏位

SIGNAL-N 栏位用于所有传输模式。其中包含从数据讯符 (data symbol) 还原位元串流 (bit stream) 所需要的信息。SIGNAL-N 栏位如图 15-6 所示。

Figure 15-6. WWiSE SIGNAL-N field



CONFIG 次栏位

Configuration 次栏位由 6 个栏位组成。

NSS (空间串流数)

3 个位元用来指示所使用的时间串流数。此数值从 0 起算，因此范围从 0 至 3。

NTX (传输天线数)

3 个位元用来指示使用多少天线来承载时间串流。此数值从 0 起算，因此范围从 0 至 3。

EW (频宽)

2 个位元用来指示所使用的频宽。20 MHz 以 0 表示，40 MHz 以 1 表示。

CR (编码率)

3 个位元用来指示所使用的编码率 (cod rate)。1/2 以 0 表示，2/3 以 1 表示，3/4 以 2 表示，而 5/6 以 3 表示。

CT (编码类型)

2 个位元用来指示所使用的编码类型 (code type)。0 代表回旋编码 (convolutional code)，1 代表非必要的 LDPC。

CON (星状图类型)

3 个位元用来指示所使用的星状图类型 (type of constellation)：0 代表 BPSK，1 代表 QPSK，2 代表 16-QAM，而 3 代表 64-QAM。

LENGTH

长度 13 个位元，用来记载硬件层数据帧所承载的数据位元数。其范围从 0 至 8,191。

LPI (最终 PSDU 指示)

在数据帧宣泄期间，最后一个数据帧会设置 LPI 位元，告诉其他工作站此次宣泄已告结束。

CRC

除了 CRC 与 Tail 位元，将根据其他所有栏位计算出 CRC 值。

Tail

长度 6 个位元的结尾位元，用来关闭回旋编码器。

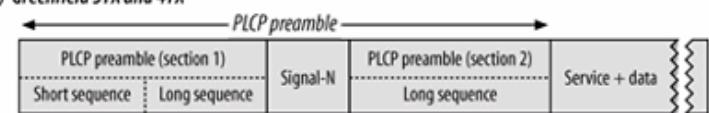
在其他传输模式中，preamble (同步信号) 会被切割成好几个区块，如图 15-7 所示。在这些区块之间，有可能包含 Signal 栏位。SIGNAL-N 栏位是由 802.11n 所定义，只有 802.11n 工作站才会进行解码；SIGNAL-MM 栏位用于混合模式，以便回溯相容于旧式的 OFDM 不工作站。它等同于 802.11a 所使用的 Signal 栏位，如图 13-16 所示。

15.2.4 WWiSE PMD

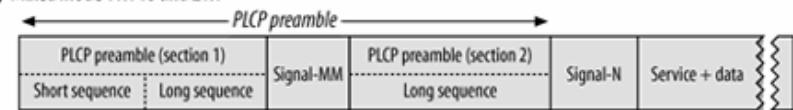
WWiSE 收发器的基本构造如图 15-8 所示。基本上，它和 802.11a 收发器没有两样，只不过具备多组传输链路（transmit chain）。交错器（interleaver）主要负责将已编码位元分配给不同的传输链路以及空间串流。

Figure 15-7. PLCP frame format for other transfer modes

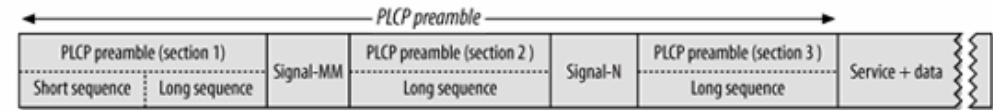
a) Greenfield 3TX and 4TX



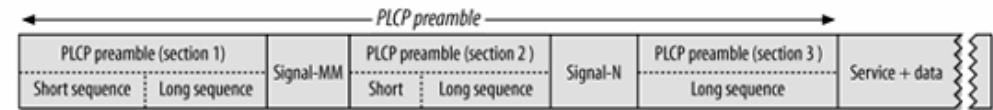
b) Mixed mode 1TX 40 and 2TX



c) Mixed mode 3TX 20/4TX 20



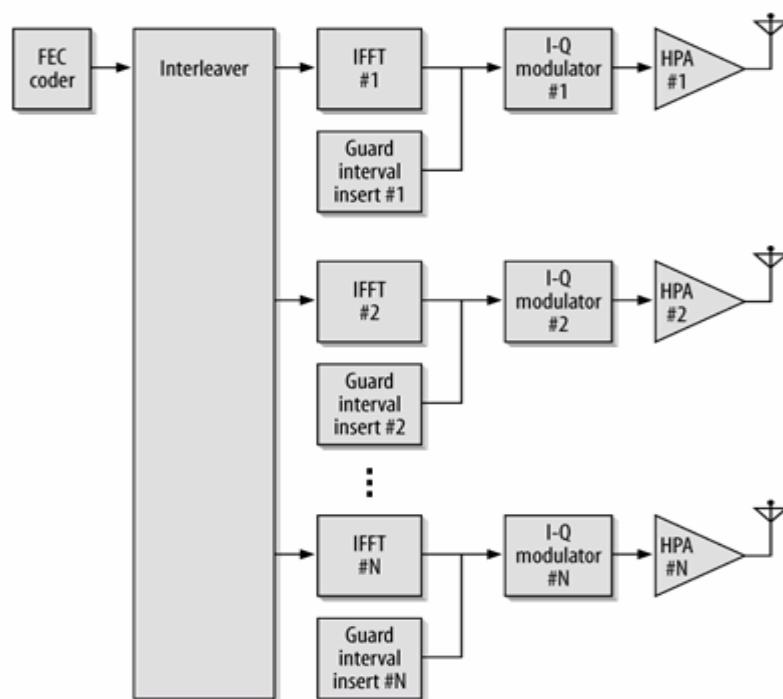
d) Mixed mode 3TX 40/4TX 40



建议书所规范的灵敏度，等同于 802.11a 对接收器的要求。表 15-3 列出所需要的灵敏度。至于邻频拒斥，建议书中并未加以规范。

Table 15-3. WWiSE receiver sensitivity

Constellation	Rate	Sensitivity (dBm)	802.11a Sensitivity (dBm), for reference
BPSK	1/2	-82	-82
BPSK	3/4	-81	-81
QPSK	1/2	-79	-79
QPSK	3/4	-77	-77
16-QAM	1/2	-74	-74
16-QAM	3/4	-70	-70
64-QAM	2/3	-66	-66
64-QAM	3/4	-65	-65
64-QAM	5/6	-64	N/A

Figure 15-8. WWiSE transceiver

15.2.4.1 WWiSE PHY 的特性

WWiSE PHY 特有的参数，列于表 15-4。和其他硬件层一样，WWiSE PHY 也包含了一些参数，可用来调整电子零件不同处理阶段所造成的迟延。

Table 15-4. WWiSE MIMO PHY parameters

Parameter	Value	Notes
Maximum MAC frame length	8,191 bytes	
Slot time	9 μ s	
SIFS time	16 μ s	The SIFS is used to derive the value of the other interframe spaces (DIFS, PIFS, and EIFS).
RIFS time	2 μ s	
Contention window size	15 to 1,023 slots	
Preamble duration	16 μ s	
PLCP header duration	4 μ s	
Receiver sensitivity	-64 to -82 dBm	Depends on speed of data transmission

15.3 TGnSync

TGnSync 联盟系由各式各样的公司所组成。除了芯片组厂商(Atelios、Agere、Intel 与 Qualcomm)，还包括其他设备制造商。网络设备制造商甚至消费性电子产品厂商均列名其中 TGnSync 的目标之一，就是支持能够自成网络的家用设备；文宣上提到如何通过无线网络来传送 HDTV 或 DVD 影片串流。这或许可以说明为何此阵营将焦点放在如何提升最大传输率（peak date rate）。

15.3.1 TGnSync MAC 的改良

虽然 TGnSync 建议书意在提供较高的最大传输率，此阵营并未完全忽略 MAC 的改良。效能的改善，主要是通过数据帧的合并与宣泄机制，以及回应政策的改变。对于旧式传输的防护机制，有些是在 MAC 层进行。值得注意的是，有些改良系设计来节省电池电力，这点可以从此阵营的成员略窥一二。

15.3.1.1 频道、无线电模式与共存

TGnSync 建议书将 40 MHz 频道支持列为必要项目，虽然有些管制当局并不允许。如果未来获得采用，TGnSync 芯片组将同时支持 20 MHz 与 40 MHz 频道，即使后者在某些管制区域并不允许使用。TGnSync 建议书亦加入若干 MAC 功能，让网络得以服务同时具备 20 MHz 与 40 MHz 能力的工作站。如工作站有大量数据待传，可以临时协调使用较宽的频道，传送完毕后才恢复 20 MHz 的操作方式。

MAC 的操作模式，也可以根据网络中的工作站类型加以分类。「纯粹模式」（pure mode）网络只包含 802.11n 工作站，因此没有必要为了旧式 802.11a 与 802.11g 工作站启用防护机制。此外，TGnSync 802.11 设备可以运行于「传统模式」（legacy mode），如同 802.11a

或 802.11g 工作站。不过，大多数操作将采用「混合模式」(mixed mode)，TGNSync 网络必须与旧式网络共存，使用相同频道，也可以接受旧式 802.11a 或 802.11g 工作站的连接。

不同模式对连接要求采取不同的处理方式。「纯粹模式」网络会完全忽略来自旧式工作站的连接要求，其所发送的 Beacon 数据帧带有一项信息元素，指示已连接工作站只能使用新的 802.11n 传输模式。「纯粹模式」网络使用 TGNSync 的高速 PLCP 来传送 Beacon 数据帧，因此旧式设备无法判读。旧式设备可以辨识【混合模式】基站，因为它们使用旧有格式来传送 Beacon 数据帧。

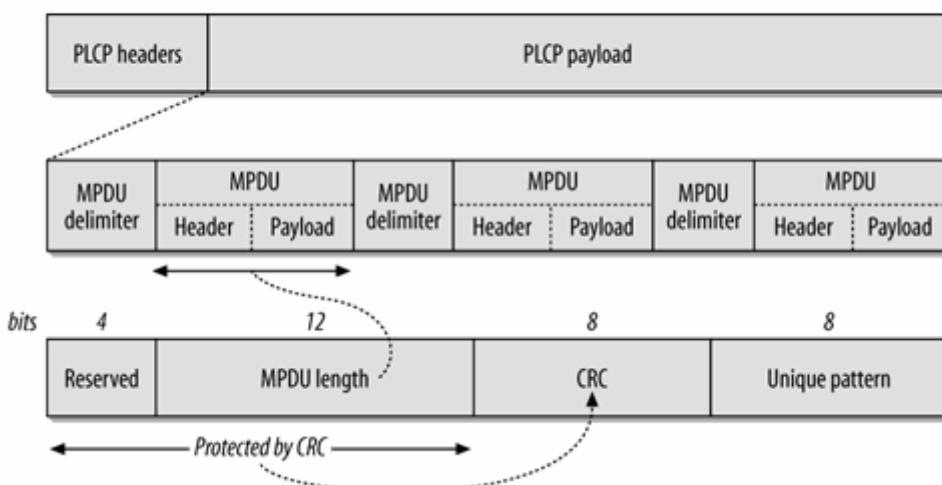
要与旧型设备共存，必须使用混合模式。（如果 802.11g 的部署经验有任何参考价值的话，大概可以推论 802.11n 设备大部分时间将以混合模式运行。）混合模式可以进一步细分为几种细项。「自行混合」(mixed capable) 网络允许旧式设备连接，但并未区分传统与高速传输的时间。「管制混合」(managed mixed) 网络的基站则会主动区分高速传输与传统传输的时间。有点类似免竞争期间与竞争期间的区别（参见第 9 章），操作于管制混合模式的基站允许旧式工作站拥有自己的传输时间，但使用类似防护机制的做法，在某些时段只允许 MIMO 工作站进行传输。

15.3.1.2 合并与宣泄

原始的 802.11 工作站通常依接收顺序来传送数据帧。基于传输率的考量，通常希望能够对数据帧加以排序，以便将它们塞进更大的合并数据帧。在 TGNSync 中，合并操作属于 MAC 层的功能，负责将数个 MAC 数据帧封装成单一 PLCP 数据帧进行传送。

图 15-9 所示为包含了数个 MAC 层数据帧之单一硬件层数据帧的基本格式。数个 MAC 数据帧被塞到同一个 PLCP 数据帧，并以适当的界定符 (delimiter) 做为区隔。此界定符包含了一个保留栏位。一个记录后续 MAC 数据帧大小的 length 栏位。一个用来保护界定符的 CRC，以及一个可用来协助将【合并数据帧】还原成个别数据帧的独特样式 (unique pattern)。置入「合并数据帧」的 MAC 数据帧并未更动，且包含完整的标头与 MAC CRC。就算「合并数据帧」中漏失了某个 MAC 数据帧，也可以成功还原其余的数据帧。

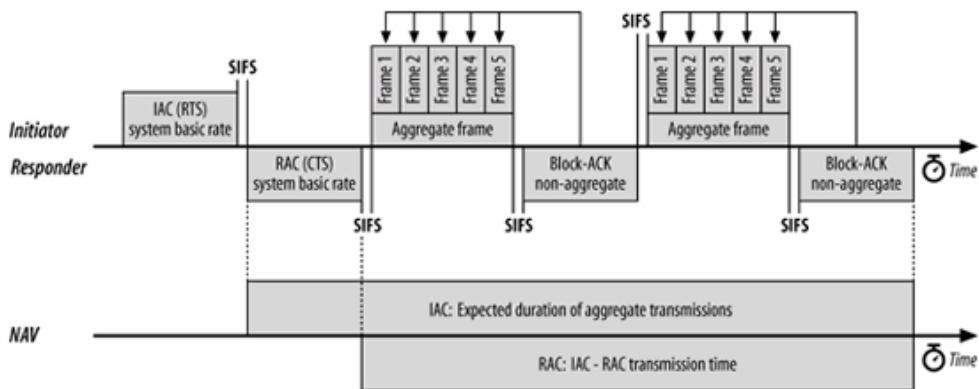
Figure 15-9. TGNSync frame aggregation



除非频道经过设置，否则无法进行【合并数据帧】的交换。整个交换程序如图 15-10 所示。「合并数据帧」的传送端称为启始者(initiator)，必须传送一个「启始者合并控制」(Initiator

Aggregation Control (简称 IAC) 数据帧。IAC 数据帧的作用类似 RTS 数据帧，但包含额外的栏位，用来协助控制频道。启始者可以要求进行频道量测、提供不同类型的编码方式，以及接收「合并数据帧」。一旦接收到 IAC，称为回应者(responder)的目的端系统就会产生一个「回应者合并控制」(Responder Aggregation Control，简称 RAC) 数据帧。RAC 数据帧的作用类似 CTS 数据帧：除了告诉传送端已经接收到「合并数据帧」，还得完成必要参数的协商。「合并数据帧」必须伴随回应讯息。TGNSync 定义了一种新的回应讯息，称为 BlockACK (区块回应)，用来回应「合并数据帧」中所包含的每个 MAC 数据帧。

Figure 15-10. TGNSync block acknowledgment

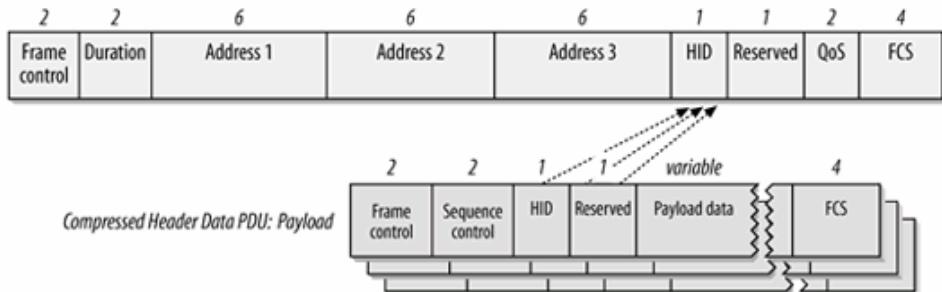


为了进一步改善 MAC 效能，TGNSync 定义了一种 MAC 标头压缩演算法，搭配「合并数据帧」使用。它的用法类似拨接所使用的 Van Jacobson 标头压缩。传送于两个端点间的数据帧，其 MAC 标头中的栏位大多相同，比较明显的是封包中的 MAC 位址。因此，MAC 数据帧所包含的三个 MAC 位址组合，就可以用长度 1 个位元组的标头识别码 (Header ID，简称 HID) 来代替。HID 还可以省略 Duration 栏位，因为「合并数据帧」自己就拥有 Duration，以及用来控制 QOS 的 2 个位元组。当数据帧的传送端与目的端相同，就以相应的单一 HID 来取代，无须重覆传送相同的 22 个位元组标头信息。MAC 数据帧的标头压缩方式，如图 15-11(a) 所示。首先，包含完整标头的标头数据帧被传送至目的端，并且被赋予一个 HID。HID 可用来代替之前的完整标头，只要传送一个位元组，就可以索引出之前传送的 Duration、定位与 Qos 数据相关信息。

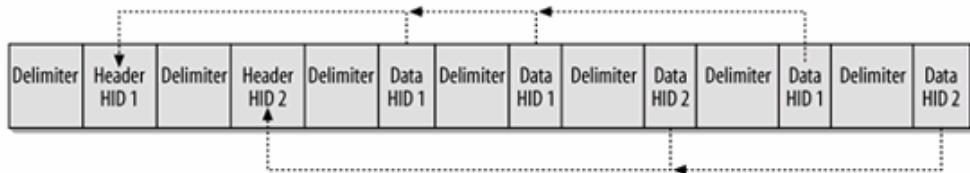
标头压缩的用法如图 15-11(b) 所示。打算分送至两个目的地的 5 个 MAC 数据帧，合并成单一数据帧后交付硬件层传送。此系统会对标头进行压缩，而不会在组成「合并数据帧」的各个 MAC 数据帧中附上完整的标头。既然有两个目的地，就会有两种不同的 MAC 标头。它们各自被赋予一个 HID 编号，然后被传送出去。随后的 5 个数据帧各自使用适当的标头编号。HID 编号的独特性只存在于单一合并数据帧的环境中。相较于 5 个数据帧均传送完整标头，如此可将 MAC 封装所造成的负担减低一半以上。

Figure 15-11. TGnSync MAC header compression

a) MAC Header PDU: Full header



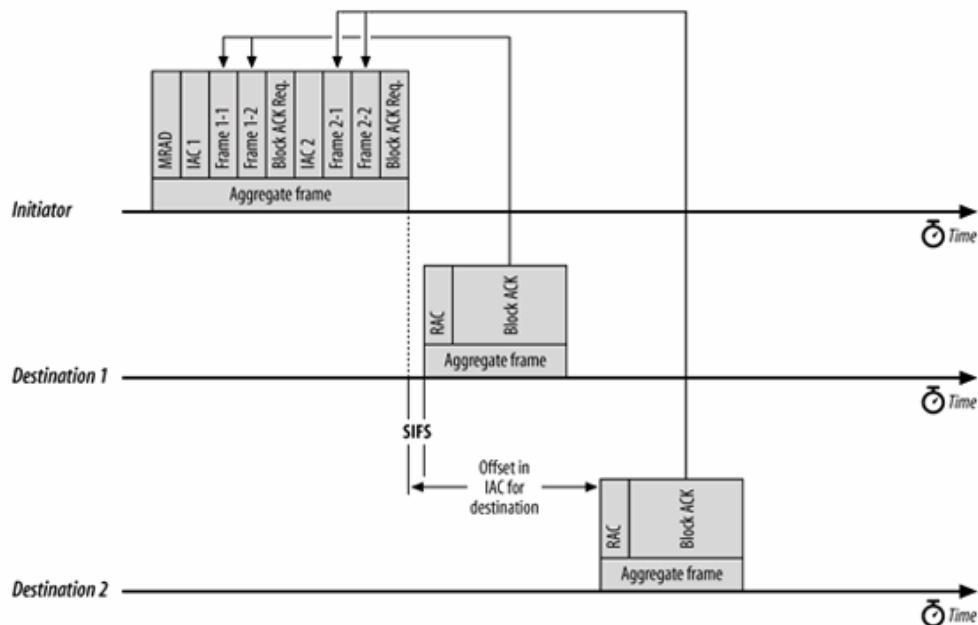
b) Using header compression



如果「合并数据帧」所包含的几个数据帧来源与目的地相同，标头压缩就特别有用。不过，TGnSync 合并操作的好处并不限于点对点传输。单一接收者的合并操作也是必要的（**required**）；另外一种非必要的延伸功能(**optional extension**) 允许「合并数据帧」包含传送给不同接收者的 MAC 数据帧，此种情况称为「多接收者合并」（**Multiple Receiver Aggregate**, 简称 MRA）数据帧。单一「合并数据帧」可以包含几个 IAC 数据帧。每个 IAC 会指定传送回应讯息的时间差（**offset**），这些回应讯息通常就是区块回应讯息。为了区别「多接收者合并数据帧」与「单接收者合并数据帧」，多接收者数据帧是以称为「多接收者合并描述符」（**Multiple Receiver Aggregate Descriptor**, 简称 MRAD）的控制项做为启始栏位。启始者的合并数据帧始于 MRAD，其后才是分送至各目的地的合并数据帧。数据帧之间系用 IAC 数据帧加以区隔。

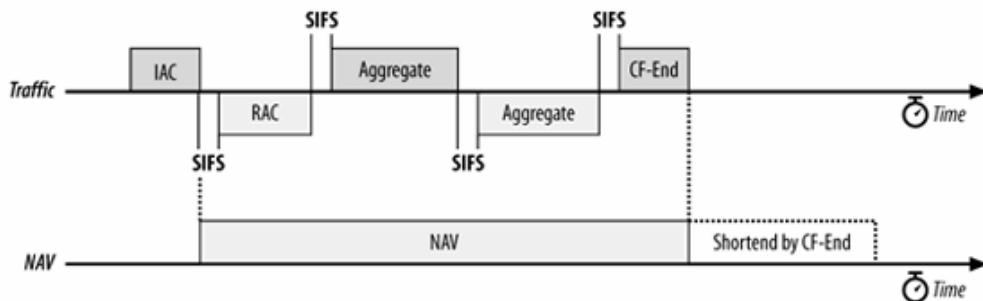
15.3.1.3 防护机制

如同市面上各式硬件层，TGnSync 建议书也提供防护机制，避免干扰旧有的硬件层。TGnSync 建议书的防护机制主要有两种形式。第一种是以 MAC 的虚拟载波检测机制与网络配置向量为基础。第二种是以「掩护」（**spoofing**）机制为基础，使用现有的 PLCP 标头格式来承载 **duration** 信息。工作站可以自行判断应该使用何种机机机制。

Figure 15-12. TGnSync MRA

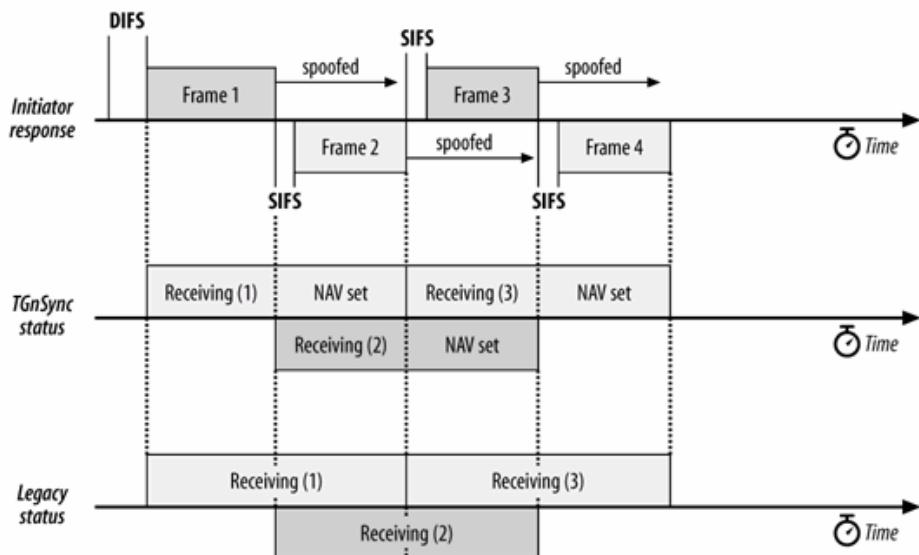
以长 NAV 值来保护数据帧交换程序，只是借用 802.11g 防护机制并稍作调整。数据帧交换程序一开始，会在 RTS 数据帧中设置够长的 NAV 值，以便防护整个数据帧交换程序。RTS 数据帧是以「传统」（比 legacy）速率进行传输，现有的 OFDM 接收器亦可辨识。目的端工作站会传回一个 CTS 讯息做为回应，当中亦包含一个长 NAV 值。根据 MAC 的基本访问规则，在 RTS/CTS 净空期间，其他工作站必须迟延访问介质，此时双方就可以使用旧式工作站无法理解的调制方式，以较高速率交换数据帧。CF-End 数据帧可用来提前结束 LongNAV 期间。此种防护机制用于「合并数据帧」时，必须以 IAC 取代 RTS，并以 RAC 取代 CTS。不过，操作的基本原则还是跟以前一样。参见图 15-13。

第二种防护机制称为「掩护」（spoofing），主要是设置 PLCP 标头中的 length 栏位来达成防护的目的。TGnSync 沿用第 13 章所提到的 OFDM 标头。由于和 802.11 a/g 格式相同，因此 spoofing 会影响所有工作站。OFDM PLCP 标头包含两个数值，接收端可以藉以判断传输需要多久时间。SIGNAL 栏位（如图 13-16 所示）将数据帧主体(body) 的传输率及其长度编码成几个位元。工作站会解码 signal 栏位，并用位元数除以传输率估计所需要的传输时间。【注】为了取得 spoofing 所需要的最长时间。传统 SIGNAL 栏位的数据率一律设为最小值，即 6 Mbps。

Figure 15-13. TGnSync protection: LongNAV

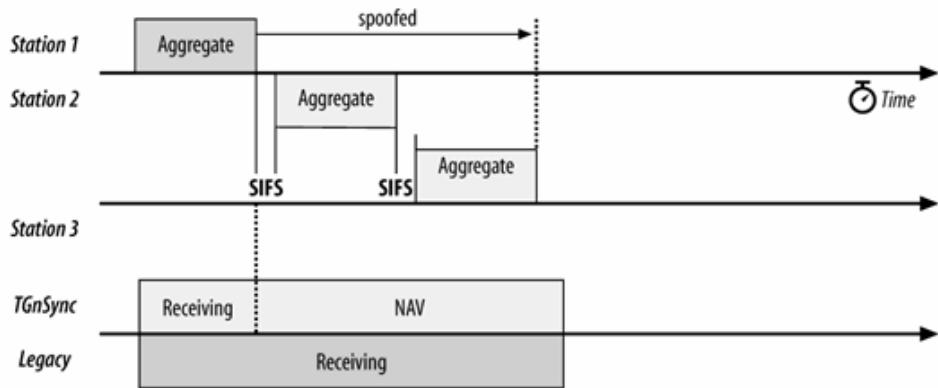
交叉掩护 (pairwise spoofing) 时，两部工作站会各自传送一个长度与速率均不正确的数据帧，所以旧式工作站会在此数据帧及其回应期间进入接收模式。TGnSync 工作站会忽略旧式的 SIGNAL 栏位，只使用 802.11n SIGNAL 栏位。交叉掩护机制如图 15-14 所示。传送 Frame 1 后，可利用交叉掩护将数据帧的接收时间设置至 Frame 2 结束。TGnSync 工作站会将此掩护解读为较长的 NAV，相当于将 NAS 设置至 Frame 2 结束时间。此时，回应者 (responder) 附近的工作站将进入接收状态；若有隐藏节点存在，此 NAV 也可以保护整个传输过程，直到 Frame 2 结束。802.11a/g 工作站会将这段掩护时间解读为接收时间，就算它们不在第二个数据帧的接收范围。Frame 2 传送完毕后，同样使用交叉掩护来保护 Frame 2 与 Frame3。

Figure 15-14. TGnSync protection: pairwise spoofing



如果单一数据帧必须得到多方回应，或许就需要较长的介质锁定时间，此时可以使「单方掩护」(single-ended spoofing)。使用单方掩护时，交换程序的第一个数据帧会使用掩护机制来保护整个交换程序，好让所有回应讯息能够在防护时间内到达。搭配数据帧合并操作的单方掩护机制如图 15-15 所示。第一个「合并数据帧」有多个接收端，必须得到其他两部工作站的回应。它将掩护时间设置为预计完成整个交换程序所需要的时间。TGnSync 工作站在第一个数据帧所设置的期间会进入接收模式，这相当于将 NAV 设置至掩护时间结束。旧式设备在整个掩护期间也会进入接收模式。

Figure 15-15. TGnSync protection: single-ended spoofing



15.3.1.4 省电机制

TGnSync 定义了「计时接收模式切换」（Timed Receive Mode Switching，简称 TRMS）协议，用来节省能源与延长电池使用时间。

传统的 802.11 省电机制是将接口完全关闭，并且在基站暂存数据帧。在单进/单出（single-input/single-output）接口，只有一组射频链路可以关闭。在 MIMO 系统，如果关闭未用的射频链路，而只留下其中一组来监视电波链路，必然可以省下可观的电力。这两种系统状态，分别称为「启用 MIMO」（MIMO enabled）与「停用 MIMO」（MIMO disabled）：前者会启用所有接收功能，后者则会关闭所有 RF 链路，只留下其中一组。工作站可以在连接要求中以一项信息元素来启动 TRMS 省电功能。TRMS 省电机制的主要参数为 hold time。工作站传送一个数据帧后，会在 hold time 所记载的时间内保持清醒。后续传送的数据帧会不断更新 hold timer 至所需要的时间。将 hold time 设置为 0，代表工作站进入睡眠状态前会持续运作一个槽位时间（slot time）。

在基础型网络里，是由基站负责为每部工作站维护 TRMS 计时器。时间一到，基站即推断工作站已经进入「停用 MIMO」状态，这会促使它启用睡眠接收链路。在独立型 BSS 中，每部工作站必须为所有其他工作站维护 hold timer。

此计时器是一个可调参数。如果被设置为较大的值，工作站将用掉较多的电力来维持接收器全力运作。虽然传输量会因此较高，代价是必须牺牲一些电池电力。有时候，网络性能不受是否使用省电模式影响。使用 NAV 进行防护的网络，必须以相容于所有 OFDM 工作站的单天线模式来进行最初的 RTS/CTS 交换，因此不需要传送额外数据帧，工作站就会以「启用 MIMO」模式操作。不过，较先进的传送模式将受困于此，因为它们需要使用多天线模式来进行数据帧交换，这样方能够完全发挥功能。

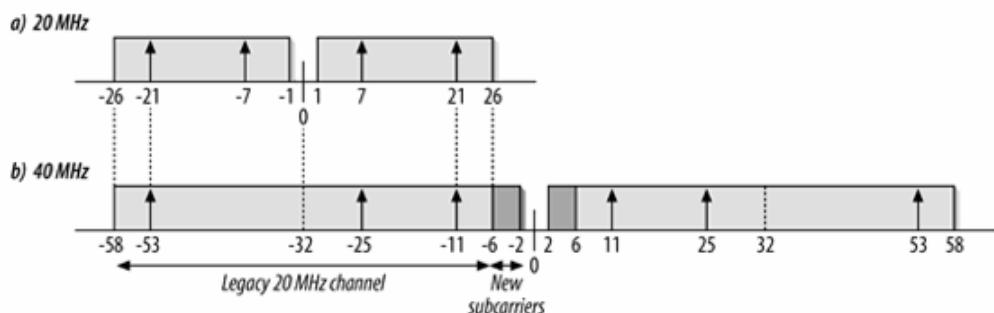
15.3.2 TGnSync PHY 的改良

为了达到较高的最大传输率，TGnSync 建议书采用类似 WWiSE 的技术。数据帧被划分为数个空间串流后，经多工处理以 MIMO 多组天线配置传输。为了提升传输率，TGnSync 使用较激进的编码方式，包括较大的星座图。较高的回旋编码率以及缩短的防护时间。此外，TGnSync 也需要使用较宽的频道。TGnSync 相容设备必须支持 40MHz 频道，在 WWiSE 中则非必要。

15.3.2.1 频道的结构

如同 802.1a, 20 MHz 与 40 MHz 频道的划分系以 0.3125 MHz 为副载波间隔。20MHz 频道与 802.11a 频道完全相同, 如图 15-16(a)所示。TGn (图 15-16(b)) 建议使用的 40 MHz 频道, 对加 MHz 结构做了一些修正。合并两个 20 MHz 频道后, 再划分为 128 个子频道。这两个 20 MHz 频道的中心频率, 会被摆在 + / -32。这两个 20 MHz 频道, 会在 -6 与 +6 之间加上频谱遮罩(spectral mask), 而且频段两端的传输振幅有下滑的现象(roll off)。如果使用单一连续频道, 则不需要使用频谱遮罩, 而且频段中央可以用最大功率进行传输。在频段中央以最大功率传输可以增加 8 个副载波。使用单一连续的 40MHz 频段, 可将原本浪费掉的副载波回收使用。因此在 TGnSync 中, 40 MHz 频道的最大传输率不只是 20 MHz 频道的两倍, 而是 2.25 倍。为了进一步提升传输率, 这两个 20 MHz 频道所使用的导波(pilot carrier)也被分别移除了一道, 因此 40 MHz 频道只用掉 6 道而非 8 道导波。

Figure 15-16. TGnSync channel structure



15.3.2.2 基本的 MIMO 速率

TGnSync PHY 定义了 32 种调制与编码配对方式。在基本的 MIMO 模式中, 每道空间串流均须使用相同的调制技术, 因此传输率即为个别空间串流传输率的倍数。为了节省空间, 以下仅列出传输率的计算公式, 不再以表格列出:

$$\text{Data rate (Mbps)} = 12 \times \text{channel bandwidth factor} \times \text{number of spatial Streams coded bits per subcarrier} \times \text{code rate} \times \text{guard interval factor}$$

Channel bandwidth factor (频宽系数)

频道至少为 20 MHz, 频宽系数设置为 1 - 40 MHz 频道可以承载两倍以上数据, 频宽系数设置为 2.25。

Number of spatial streams (空间串流数)

空间串流数可以是 1、2、3 或 4。它必须小于或等于传输天线数。至少必须支持两道空间串流。

Coded bits per subcarrier (副载波编码位元)

64-QAM 为 6, 16-QAM 为 4, QPSK 为 2, BPSK 为 1。

Code rate (编码率)

搭配 BPSK 可以使用 1/2 的编码率; 搭配 QPSK 或 16-QAM 可以使用 1/2 或

3/4 的编码率；搭配 64-QAM 可以使用 2/3、3/4 或 7/8 的编码率。

Guard interval factor (防护时闲系数)

基本防护时间为 800 ns，其系数设置为 1。400 ns 的防护时间可以稍微提升传输量，其系数设置为 1.11。

在使用单一空间串流的基本模式中，频道性能与 802.11a 相同，例外是可以使用 7/8 的编码率，达到 63 Mbps 的传输率。如果将所有参数调至极限(4 个 40MHz 频道，64-QAM 搭配 7/8 的编码率，以及短防护时间)，TGnSync 建议书的传输率最高可达 630 Mbps。

15.3.2.3 传输模式

TGnSync 建议书要求支持三种 MIMO 模式。在必要的基本模式中，空间串流数等于天线数。每道空间串流使用相同的调制与传输方式。每个频道使用相同的调制方式来编码，然后以相同的传输功率来传送。任何传输率的变动，均是为了因应漏失回应讯息所做的调整。

另两种非必要的模式会利用从所谓的「闭路」（closed-loop）操作得到的信息。TGnSync 设备会互相传送「探测」（sounding）数据帧以量测链路的效能。根据探测与校准所搜集到的信息，可以使用波束成型(beamforming)来提升信号品质。较高的信号品质意谓着既定的数据率可以传输较远的距离。讯噪比不变的情况下，以波束成型进行传输可以承载更多数据。波束成型并非必要的协议功能。并非所有用户端设备均能够以波束成型进行传输，但所有用户端设备都必须能够接收波束成型数据帧。

在搭配波束成型的基本 MIMO 模式中，每个频道都必须以相同方式编码。开始传输之前，必须先交换探测数据帧以校准无线频道。根据探测数据帧所得到的信息，可进一步为空间串流选用传输功率与编码方式。基本波束成型模式（basic beamforming mode）要求所有空间串流以相同的功率和相同的编码方式进行传输。不论空间串流少于或等于传输天线数，均可使用基本波束成型，不过当传输天线数目远多于接收天线，信号处理上才会有比较明显的优势。如果空间串流数小于传输天线数，就会使用空间操控矩阵(spatial steering matrix)，为每个位元指定传输天线。

此外 TGnSync 还定义了一种非必要、称为【先进波束成型 MIMO】(advancedbeamforming MIMO，简称 ABF-MIMO) 的模式。它的运作方式类似基本波束成型模式，但具备额外能力，可以在每一道数据串流使用不同的传输功率。以及为每一道空间串流使用不同的调制与编码方式。如同基本波束成型模式，它必须搜集无线电波状态信息来校准频道。先进波束成型模式中有一种选项模式，允许双方同时采用波束成型，如果双方均支持的话。ABF-MIMO 模式还包含了一种新的星座图：256-QAM，每个副载波可以传递 8 个编码位元。

要得到先进波束成型模式的传输率，可以使用上一节的公式，分别计算个别空间串流的传输率，然后再予以加总。以 256-QAM 而言，每个副载波使用 8 个编码位元。256-QAM 只能搭配 R=3/4 的编码率。

15.3.2.4 编码选项

除了原始 OFDM 规格书所支持的回旋编码（convolutional code），TGnSync 建议书也包含了两种非必要的错误更正码。第一种技术使用（开发于 1960 年代的）Reed-Solomon 区块码。它被广泛使用在许多数位应用中，特别值得注意的是 CD 与 DVD 所使用的错误更正码。TGnSync 建议书以传统方式结合了 Reed-Solomon 码与现有的回旋编码。首先以 Reed-Solomon 码进行

数据串流的编码。然后将编码的结果交付回旋编码处理。【注】这两种编码方式彼此互补。回旋编码是将错误于时间轴展开，能够处理比较零散的错误。Reed-Solomon 编码擅长于更正瞬间突发的错误；Reed-Solomon /convolutional 编码组合的替代方案是低密度同位元检查(*low-density parity check*, 简称 LDPC) 码。

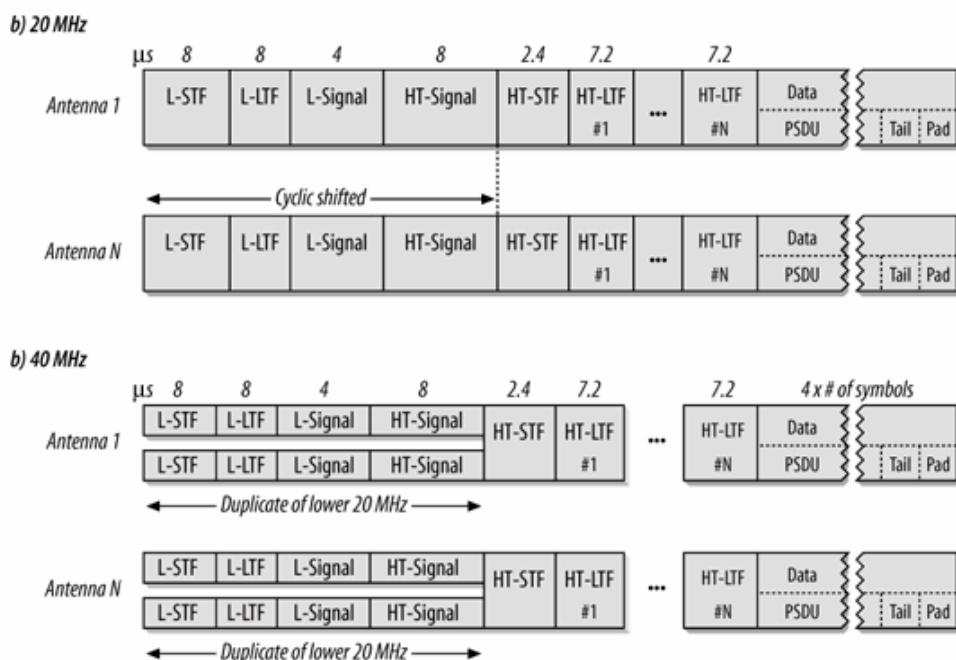
15.3.2.5 短防护时间选项

为了进一步提升 MAC 的效能，TGnSync 建议书允许使用短防护时间（*short guard interval*）。802.11a 与 802.11g 标准以及 WWiSE 建议书使用 800 ns 的防护时间。第 13 章曾经提到，防护时间应为迟延时间的 2 至 4 倍。800 ns 的防护时间容许 200ns 的迟延时间，远高于实际情况所需。大多数办公室与家庭的迟延时间远低于此，大概是 50-100 ns 左右。在这种情况下，使用 400 ns 的防护时间可以提升大约 10% 的传输量。

15.3.3 TGnSync 硬件层传输（PLCP 与 PMD）

在 TGnSync 建议书中，PLCP 的基本数据帧格式如图 15-17 所示。它使用与现有 OFDM 相同的标头，因此不需要用到会造成严重负担的防护机制来避免干扰 802.11a 或 802.11g 网络。图中前置“L-”的栏位属于 802.11a 与 802.11g 共用的旧有栏位；相关细节请参阅第 13 与 14 章。

Figure 15-17. TGnSync PLCP frame format



15.3.3.1 旧式标头

TGnSync PLCP 数据帧的前三个栏位与 802.11a/g PLCP 标头相同。

L-STF (旧式短调整序列栏位)

此栏位与 802.11a 中的定义相同。持续时间为 8 微秒。

L-LTF (旧式长调整序列栏位)

此栏位与 802.11a 中的定义相同。持续时间亦为 8 微秒。

L-SIG (旧式信号)

这三个栏位与 802.11a 相同，802.11g 亦使用相同栏位。相关细节详见图 13-16。此栏位系以 BPSK、R=1/2 进行调制与编码。

TGnSync 工作站会忽略 L-SIG 栏位的内容。使用掩护机制进行防护时，L-SIG 栏位的内容并不明显。TGnSync 工作站会在旧式标头之后的 high-throughput 标头中找寻所承载 MAC 数据帧的真正长度与编码方式。

为了利用空间分集 spatial diversity 的好处，亦即以多组天线传送相同的旧式标

头，TGnSync 提供了一种非必要的周期迟延 (cyclic delay)。每组天线传送旧式数据帧时，会对周期前置时间稍作更动，让总迟延时间差距 50ns。

使用 40 MHz 频道时，会同时在个别的 20 MHz 子频道上传送旧式标头。换言之，编号 -58 至 -6 (位于较低频段的 20 MHz 子频道) 以及编号 +6 至 +58 (位于较高频段的 20 MHz 子频道) 的副载波，均被用来传送旧式的 802.11a 标头。

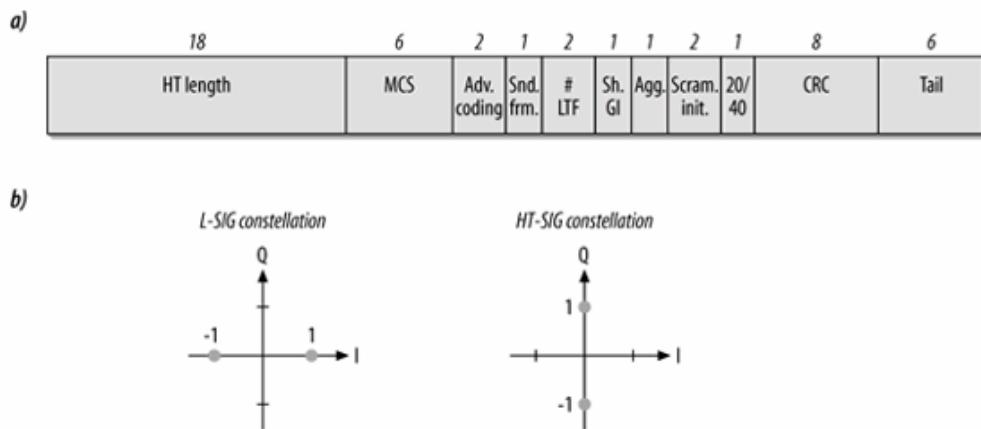
15.3.3.2 High Throughput 标头

紧跟在旧式同步信号之后的，乃是 TGnSync 建议书特有的“high throughput”标头。此标头的主要成份为 high throughput signal (简称 HT-SIG) 栏位，如图 15-18 所示。HT-SIG 栏位系用来检测数据帧是否承载以高速率传递的经 TGnSync 编码的数据，或者只是旧式的数据帧。HT-SIG 栏位采用较保守的调制方式，以 Q-BPSK、R=1/2 进行调制与编码。Q-BPSK 在星座图中使用两个数据点位，但出现在正交 (quadrature) 成份当中。图 15-18(b) 比较了 Q-BPSK 与 BPSK 星座图。

长度为 3 个位元组的 high throughput 标头是由数个栏位所组成，并且依出现的次序加以传送。最先传送的是每个栏位的最低效位元。

HT-Length (18 个位元)

此栏位是 PLCP 数据帧所承载数据的长度。进行合并操作时，如果承载数据中包含好几个全尺寸的 MAC 数据帧，此栏位的值就会很大。

Figure 15-18. TGnSync HT-SIG field**Modulation and Coding Set (简称 MCS: 6 个位元)**

MIMO 的缺点之一是其中包含了种种选项，除了有不同的调制机制，不同的空间串流数，还有不同的编码率。MCS 栏位系用来选择调制与编码机制，以及空间串流数。基本 MIMO 模式使用 0-31 的数值范围，33-60 则是留给高级 MIMO 模式使用。

Advanced Coding (2 个位元)

此栏位的长度为 2 位元，用来指示是否使用高级编码选项。0 代表不使用高级编码。1 代表使用 LDPC。2 代表使用 Reed-Solomon 编码。3 目前保留未用。

Sounding packet (1 个位元)

用来量测频道效能的要求与回应数据帧会设置此位元。一旦设置此位元，代表天线正在传送各自的空间串流。如果未设置此位元，就不该使用此数据帧来量测频道相关信息。

Number of HT-LTIs (2 个位元)

紧跟在 HT-Signal 栏位之后的是 high-throughput training 栏位。每道空间串流均需要具备一个 training 栏位。

Short Guard Interval (1 个位元)

如果此位元旗标设置为 1，代表 400 ns 的短防护间隔会被用在数据帧之 Data 栏位中的 MIMO 讯符。

Aggregation (1 个位元)

如果此位元被设置为 1，代表 PLCP 数据帧承载了合并宣泄(aggregate burst)的几个 MAC 数据帧。

Scrambler initialization (2 个位元)

这两个位元用来做为编码器的乱数种子。

20/40 Bw (1 个位元)

如果设置为 1，代表使用 40 MHz 的频道。如果设置为 0，代表使用 20 MHz 的频道。

CRC (8 个位元)

CRC 用来保护 L-SIG 栏位，以及之前的 HT-SIG 当中所有栏位。

Tail (6 个位元)

HT-SIG 标位受到回旋编码的保护。如同以往，需要 6 个位元来关闭(ramp down) 回旋编码器。

15.3.3.3 High-Throughput training 标位

紧跟在 **high-throughput** 标头之后的是 **high-throughput** 长短调整序列标位。单一短调整序列(**short training**)标位会延伸至整个作业频道。在 20 MHz 频道中, **high-throughput short training** 标位 (简称 HT-STF) 的频宽为 20 MHz。如果使用较宽的 40 MHz 频道，则 HT-STF 的频宽为 40 MHz - **short training** 标位用来微调 MIMO 作业所使用的接收器。

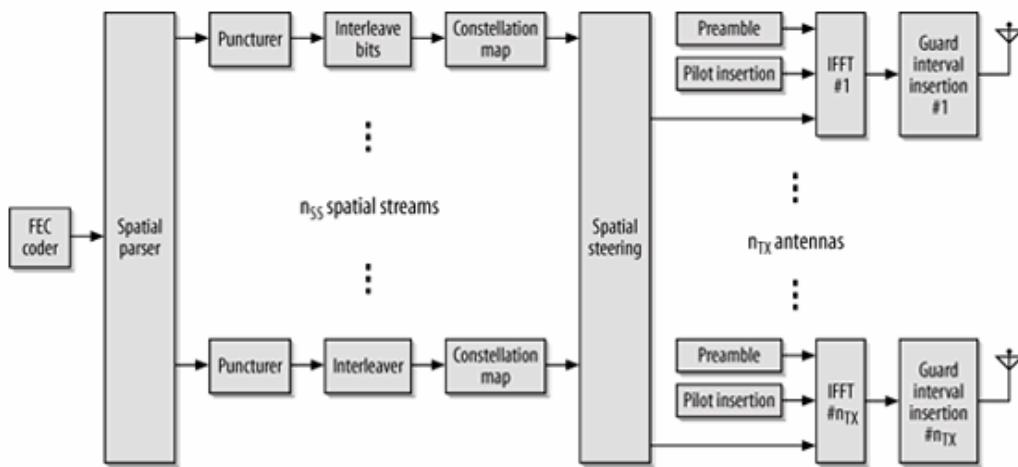
当数道空间串流通过数个链路进行传输，精确控制接收信号的放大作业就十分重要。**high-throughput long training** 标位 (简称 HT-LTF) 用来进一步调整各个接收链路。每道空间串流各自使用一种 HT-LTF。在基本 MIMO 模式中，每道空间串流对应到一个接收器链路；在高级模式中，接收器链路的数目多于空间串流的数目。

15.3.3.4 Data、Tail 与 Pad

Data 位元系根据 **high-throughput** 标头所定义的调制与编码方式进行编码。和其他的 FDM 硬件层一样，在传输之前数据必须经过编码，使用 **high-throughput** 标头中的编码器初始化位元。数据之后是长度 6 个位元的标尾(**tail**)，用来关闭回旋编码器，并且加入足够的填塞位元(**pad**)，让待传的数据长度符合讯符区块的大小。

15.3.4 TGnSync PMD

TGnSync 收发器的基本设计如图 15-19 所示，图中所显示的是波束成型发射器 (**beamforming transmitter**)，而非基本的 MIMO 发射器。接收到编码数据帧后，随即交付「前溯错误更正」 (**forward-error correction**, 简称 FEC) 编码器处理，它通常就是回旋编码器。来自 FEC 编码器的加码位元，随后被空间剖析器 (**spatial parser**) 送至不同的空间串流。空间剖析器的任务，是负责将单一位元串流切割为子串流以便进行传输。每道空间串流均被镂空为预计传送的速率。在波束成型模式中，每道空间串流均接受镂空处理，并且可以使用不同的速率。基本型发射器则必须以同样的速率对各道串流进行镂空处理。（逻辑上，基本型发射器的镂空程序可以先于空间剖析器）。此时，每道空间串流包含一系列加码位元，准备由交错器 (**interleaver**) 对映到 OFDM 载波。经过交错器处理后，每个位元区块会被星座图对映器 (**constellation mapper**) 对映至单一讯符。在基本 MIMO 模式中，每道经过交错的空间串流均由单一传输链路处理；高级模式则会使用空间操纵矩阵 (**spatial steering matrix**) 把每个讯符指派给任一传输链。图中所显示的空间操控矩阵可以用一对一的界面替代，介于空间串流处理器与基本 MIMO 作业的传输天线之间。每个传输链路取得本身的讯符序列后，会把它调制成空气的波动。规格书中并未提到邻频拒斥 (**channel rejection**) 或灵敏度效能 (**sensitivity performance**) 的相关规定。

Figure 15-19. 2x2 TGnSync MIMO transceiver

15.4 比较与结论

基本上，WWiSE 与 TGnSync 这两份建议书算是 802.11a 硬件层的 MIMO 修订版。

两者均要求支持 2x2 模式，亦即收送端分别具备两套收发器。不过，根据最后出炉的 802.11n 标准（不论是否与建议书相似）所开发的大部分产品，可能将至少支持几种非必要模式。基于成本考量，用户端设备可能只会使用两组收发器，但基站将使用较多收发器。基本型基站可能只会使用两组收发器，但大多数昂贵的企业级基站将使用三或四组收发器。

表 15-5 列出了这两种建议书各种空间串流模式的传输率。增加空间串流可以达到较高的传输率，但会增加芯片成本。TGnSync 建议书能够达到较高的传输率，但是必须使用较激进的编码率。要达到 WWiSE 135 Mbps 的传输率，必须使用 64-QAM 搭配 R=5/6 的编码率；要达到 140 Mbps，TGnSync 必须使用 7/8 的编码率，并且将防护时间减半。（如果不使用短防护间隔，TGnSync 的传输率仅达 126 Mbps）高价波束成型模式则采用较大的 256-QAM 星座图。虽然 TGnSync 的传输率较高，但我预料采用较激进的编码率将导致传输距离变短。

Table 15-5. Top speed for major 802.11n proposals (two spatial streams)

	20MHz channels	40 MHz channels
WWiSE	135 Mbps	270 Mbps
TGnSync		
Basic mode	140 Mbps (+3.7%)	315 Mbps (+16.7%)
Advanced beamforming mode	160 Mbps (+18.5%)	360 Mbps (+33.3%)

频谱的运用方式是两个阵营的主要争论点。WWiSE 强调 MAC 效率甚于传输率，甚至认为不先改善 MAC 效能就迳自使用 40 MHz 频道来提升传输率，根本就是浪费稀有的免照频谱。虽然不无道理，TGnSync 采用 40 MHz 频道做法的好处是可以回收频道中央的频谱。WWiSE 使用 40 MHz 频道时只能够让传输量增加一倍，但 TGnSync 可以在相同的频道中挤出两倍以上的传输量。这两种方式各有其缺点。TGnSync 方案或许会导致芯片组永远以 40 MHz 作业，带来额外的成本与复杂度，而且管制当局可能不允许使用 40 MHz 频道。允许使用 40 MHz 频道的国家当然会欣然接受更快的速度。但在限制使用 40 MHz 频道的地区，额外衍生的成本就不是芯片厂商所乐见的。另一方面，WWiSE 认为不需要高速频道，似乎等于拒绝让数据率提升五倍的可能性。

为了达到最高速率，TGnSync 要求使用闭路(closed-loop) 作业。要在芯片中实现闭路作业并不简单。除了以探测数据帧量测频道，也必须搜集回应讯息以便校准无线频道。WWiSE 只使用开路(open loop) 作业，实现上比较简单。不必使用闭路作业，WWiSE 建议书就能够将单一编码串流展开至多组天线。如果闭路作业在芯片的实现上有其困难，802.11n 标准将再度延迟推出。

为了达成 802.11n 最终标准所设置的远大目标，数据帧合并在其中扮演重要的角色。不过要完全发挥数据帧合并的优势，需要在目前所实现的伫列机制(queuing) 中加入更多智能。802.11n 能否大幅提升速度，取决于所改善的伫列演算法能否将较小的封包整合成较大的合并封包。这两份建议书均未规范伫列机制，因此效能的提升程度将因厂商而异。

TGnSync 所设计的合并功能比较聪明，虽然差距不会太大。MAC 标头的 Address 1 栏位值相同时，WWiSE 才允许数据帧合并。在基础型网络里，Address 1 栏位即为 BSSID。工作站传给基站的任何数据帧均可予以合并，因此这两份建议书在上行部分是相同的。在下行方面，WWiSE 必须通过硬件层数据帧宣泄来变换方向。任何新方向都必须使用新的 PLCP 标头。TGnSync 可以使用一个「多接收器」合并数据帧来减少负担(overhead)，并从「合并数据帧」中搜集来自各接收器的回应。

802.11 的省电模式向来无人重视，构造也过于简单。TGnSync 试图为新的 MAC 架构提供延伸省电功能，WWiSE 则否。或许是因为 TGnSync 联盟包含许多设备厂商，而 WWiSE 阵营完全由芯片厂商组成。虽然速度与电池电力的取舍会因应用而异，而且不见得合理，标准制定单位能够未雨绸缪未尝不是件好事。

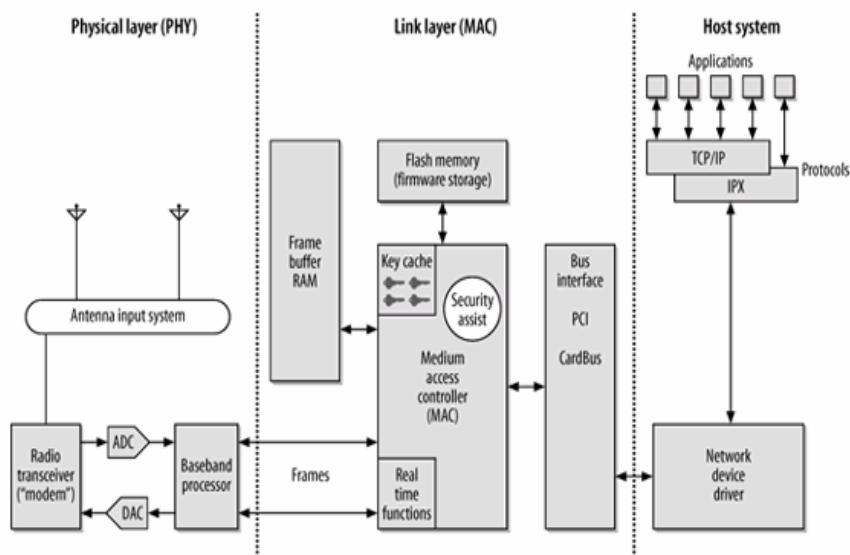
第16章 802.11 的硬件

制定规格时，重要的是为创新留点诠释的空间。标准过于严苛，实施起来就会死气沉沉；标准过于宽松，则无法顾及互通性。本章主要在探讨标准未曾明确规定的事项。例如：标准在硬件上如何实现？在协议的实现上，有哪些地方是标准允许自行斟酌的？对网管人员而言，这又代表什么意义？

16.1 802.11 界面的一般结构

图 16-1 是一般无线局域网络接口的方块图。这并不是特定厂商的产品，只做为讨论网卡结构的参考指南。网卡必须实现底层的硬件，以及操作系统所需要的链路层控制协议。就像其他使用无线电技术的产品，无线局域网络接口中同样内含天线。大多数 802.11 架构使用两组天线做为天线分集（antenna diversity），以便在多重路径干扰的环境下改善接收情况。接收到电波信号时，无线电系统会自动选择信号最强的天线，用它来进行收发。天线分集可以改善多重路径干扰，即使信号微弱是因为多重信号所造成的自相干扰，至少尚有一支天线可以接收到信号。如果信号微弱是因为距离太远所造成，天线分集就帮不上忙了，因为两支天线所接收到的信号同等微弱。天线分集有各种类型，目前最常见的实现方式，只有在接收帧时才会使用天线分集。几乎市面上所有产品都不会在传输帧时使用天线分集，仅使用“主要”（primary）天线进行传输。

Figure 16-1. Generic wireless card structure



早期的天线分集虽有帮助，却因为实现上过于简单而有所限制。多进/多出（Multiple-input/multiple-output,简称 MIMO）技术可以达到更高的传输率与更好的传输效果。不过 MIMO 的细节已经超乎本书的范围。基本上，它放弃了单一天线的做法，同时使用两组天线来提升接收的效果。

天线将电波信号传给收发器。以数据通讯常用的调制解调器（**Modem**）来类比，收发器（**transceiver**）有时也被称为无线电调制解调器（**radio modem**）。收发器使用放大器（**amplifier**）来强化对外传送的信号，或者将接收到的信号放大，以便进行后续的处理。无线电收发器还会通过从高频载波中取出信元的方式，将高频信号转换成比较容易处理的信号。收发系统通常需要加以屏蔽，防止高频信号干扰其他系统元件。这就是为什么无线硬件表面通常会有一层金属屏蔽，占据整个表面不少面积。

收发器之后是基频处理器（**baseband processor**），它是无线局域网络系统中，数字与模拟器件之间的接口。将位元转换成无线电波称为调制（**modulation**）；反之则称为解调（**demodulation**）。基频处理器负责处理复杂的展频调制，以及检测实体载波。当所接受到的电波能量超过一定的门栏，基频处理器就会加以解调。目前，无线局域网络可以使用多种不同的解调技术。**802.11b** 工作站之所以无法察觉 **802.11g** 的传输状态，原因之一在于 **802.11b** 所使用的旧式基频处理器无法解调 **OFDM** 信号。

介质访问控制器（**medium access controller**，简称 **MAC**）是整个界面的核心，负责从主机操作系统的网络协议栈中取出所接收到的数据帧，以及决定何时通过天线将数据帧送出去。**MAC** 会通过系统接口层从操作系统取得数据帧。大多数的无线局域网络接口采用的是 **CardBus** 标准，有些则是使用 **Mini-PCI - MAC** 另一端与基频处理器相连，由它传送数据帧给无线电系统。

MAC 可能必须同时处理许多数据帧，它可以申请少许的 **RAM** 缓冲区，暂存这些正在处理的数据帧。之所以要对数据帧进行处理，最常见的原因是为了让主机操作系统摆脱保安处理作业的负担。具备保安处理功能的 **MAC** 可以从驱动程序接收准备以特定密钥加密的数据包。不必在传送数据帧之前通过系统的主 **CPU** 进行加密。**MAC** 当中通常内建密钥快取，用来储存密钥。传送之前，驱动程序会将数据帧置于队列，同时指定以「**key1**」进行加密，随后操作系统就可以将加密的重担交付给 **MAC**。旧式的 **MAC** 芯片有能力处理 **WEP** 所使用的 **RC4** 加密，升级后也可以处理 **TKIP**，至于最新型的 **MAC** 芯片，则可以在硬件中进行 **AES** 加密。

除了用来暂存数据帧的 **RAM** 缓冲区，大多数接口还会使用少许的快闪记忆体来为 **MAC** 储存软件。供电之后，**MAC** 就会从快闪记忆体中取出程序并加以执行。若要实现类似 **TKIP** 的新式安全协议，只要将新的软件写入快闪记忆体，然后重新启动 **MAC** 即可。相较于变更不易的「特殊应用集成电路：(**application-specific integratedcircuits**，简称 **ASIC**)」，遇到 **802.11** 这类变动快速的协议时，使用软件只需要搭配一般的通用型处理器就行了，这对开发过程提供了不少帮助。大部分的 **802.11 MAC** 芯片，实际上就是一般的通用型微处理器。

实现上，有些 **MAC** 会针对需要立即回应的项目提供一个“即时”（**real-time**）单元。如此一来，这类数据帧就可以由 **MAC** 自动产生，不需交由主机操作系统回应相关的省电轮询（**power-save polling**）任务，或者传送应答讯息。有些系统则是将这类即时功能交付基频处理器处理。（目前 **MAC** 与基频处理器通常已经整合为单芯片，因此这种区别就无关紧要了。）

图 16-1 的方块图只做为参考之用。为了降低成本与复杂度，有些系统会使用将 MAC 与基频处理器整合在一起的单芯片。有些解决方案甚至会将无线电收发器也整合进去。使用 Atheros 芯片组的界面不须再使用额外的快闪记忆体来存放软件，因为 Atheros 芯片是在驱动程序启动 MAC 时才载入程序码。软件通常是指储存于硬件中的程序码；Atheros 设备可以通过系统软件进行编译。

16.1.1 软件控制的无线电：离题插播

802.11 所面临的两个主要问题，除了 MAC 效率不高，导致总传输量受限，还有物理层技术变动太快，导致产品生命周期缩短。面对效率不高的自然反应，通常是针对特定部分进行优化，或者在既有的硬件上采用新的协议功能，对沉浸于技术领域的工程师而言尤其如此。

无线局域网络通常无法自行定义界面的功能。为了速度上的考虑，通常会直接将基频处理器，或者基频处理器的功能组建于集成电路，因此无法任意变更。所谓特殊应用集成电路(ASIC)，乃是以本身的电路来实现特定的逻辑，因此无法用于原本设计以外的目的。此外，无线局域网络接口所使用的无线元件，通常已经针对管制当局所配置的频率做过优化处理。

不过，未来的无线电将可以重新编程（reprogrammable）。设计人员可以使用“可编程逻辑”（programmable logic）设备，例如 FPGA，来取代基频处理器这类特定硬件。无线电波是承载数位信息的模拟电波。在某些情况下，无线电波只需要进行可编程的信号处理，因此可以使用数位信号处理器(digital signal processor 简称 DSP) 芯片。不论使用何种的可编程逻辑，最终目的都是一致的。采用可编程逻辑的无线电波，可以随时通过新的软件来更换调制方式、编码方式与位元率，不必在设计阶段迁就固定的调制方式。较具弹性的代价，就是可编程逻辑设备的体积较大，执行速度较慢，而且比较耗电（也因此会产生较多的热量）。【注 1】使用可编程设备将可以任意调整电波的行为，只要载入新的软件即可。无须更改硬件，就可以实现新的调制方式、位元率，甚至是新的频段。【注 2】

完全以软件（或者可编程逻辑）控制的电波接口，称为「软件定义的无线电」（software-defined radio）或者「通用型无线电」（universal radio）它们在调制与编码方式经常或快速变动的环境中十分好用。SPEAKEasy 算是最早的软件定义无线电专案，由美国军方所推行。美军以单一的软件无线电来取代 10 组调制方式各异的无线电系统，它不但具备 10 组无线电系统所有的功能，体积也变得更小了。软件定义的无线电必须符合美国认证法规（certification rules），厂商必须采取相应措施以避免软件遭到篡改，而被使用在核准范围以外的频段。【注】

注 1 可编程逻辑设备通常用来设计一特殊应用设备。经过设计与完整的测试之后，再将 FPGA 重新设计一为特殊应用设备。最后出炉的固定逻辑设备，有时也称为之前可编程版本的“硬副本”（hard copy）

注 2 值得注意的是，开放源码社群已经开始探用可编程通辑。就像 SourceForge (<http://www.sourceforge.net>) 之于软件. OpenCores (<http://www.opencores.org>) 已经成为硬件设计的宝库。

虽然软件定义的无线电是个有趣且值得注意的发展，不过 802.11 设备大概不会完全以可编程逻辑来实现。（目前，Broadcom 与 Atheros 的芯片组只具备有限的可编程性）可编程逻辑不仅较贵，市场也不会接受此类 802.11 设备的价格。它或许可以搭配 802.11，在使用了多种电波链路的实现产品中找到立足点。

16.1.2 硬件实作上的议题

写作本书当时，市场上有四家主要芯片组厂商。依字母顺序，分别是：

Atheros

大多数包含 802.11a 的接口均会采用 Atheros 芯片组。有些 802.11g 设备也会采用 Atheros 芯片组。

Broadcom

目前，大多数非 Centrino 的内建 802.11g 接口均会采用 Broadcom 的 802.11g 芯片组。Apple 的 AirPort Extreme 亦然。

Conexant (Prism)

被 Conexant 收购之前，Prism 产品线曾经转手过好几家公司。

Intel (Centrino)

许多膝上型电脑内建的无线局域网络界面均会採用 Intel 的 Centrino。技术上而言，Centrino 乃是泛指一整组 Intel 芯片的行销名词，其中也包含系统 CPU。例如，Intel/PRO 2200 网卡即为 Centrino 802.11g 界面。

比较值得注意的一家新芯片组厂商是 Airgo Networks。他们所开发的 MIMO 芯片组，为目前市面上所谓的 802.11n 前标准(prestandard)产品所采用。

知道网卡采用何种芯片组十分有用。大多数芯片组厂商均会提供参考设计（俗称公版）给客户。参考设计通常包含软硬件。802.11 网卡制造商拿到参考设计后，只要稍微（或根本不用）修改，为产品贴上新的标签就可以开始销售。很少有网卡厂商会大幅修改驱动程序，通常只是将公版驱动程序重新包装。当然，每家厂商的口碑与评价不一。有些经常更新驱动程序，有些则否。知道网卡的芯片组由谁提供，比较容易取得公版驱动程序，或者使用相同芯片组的网卡所提供的最新驱动程序。当然，要为开放原码操作系统找到可用的正确驱动程序，必定得先知道网卡使用何种芯片组。

16.1.2.1 进一步认识网卡：FCC 文档

套句管制机构的术语，802.11 接口属于主动式辐射设备（intentional radiator）。在设计上，802.11 界面本身会主动发射无线电波，因此不能仅符合电磁辐射管制的标准限制。主动式辐射设备必须送测，并且要符合各国的管制规定，因此需要很多文件作业。

在美国，无线电设备是由 FCC 所管辖，无线电波传输设备必须经过测试并且符合 FCC 法规。在合法销售设备之前，必须取得检验编号 •看看各位手上的网卡，就可以找到上面的 FCC ID “FCC ID 分为两个部分：前三个字母称为授权单位代码（grantee code），之后的文数字称为产品码(product code)最多可达 14 个字符。每个组织有不同的授权单位代码。（授权单位代码也许以空白或破折号分隔，也许没有）。例如，Lucent 金卡的 FCC ID 是 IMR-WLPCE24H。其中，IMR 是 Lucent 的授权单位代码，WLPCE24H 则是该金卡专属的产品代码。

做为测试程序的一部分，厂商必须提出测试报告、产品照片以及其他文件，这些文件将被公开登录建档。要查询网卡的相关信息，可以到 FCC 工程技术局（Office of Engineering Technology)所维护的搜寻引擎查询，网址是 <http://www.fcc.gov/oet/fccid/>

要知道某张网卡使用何种驱动程序，FCC ID 十分有用。大多数产品均会提供内部照片，可以藉此得知该产品使用何种芯片组。譬如你手上有张 Proxim a/b/g 三合一金卡，想知道它采用

何种芯片。只要在 FCC 的数据库搜寻它的 ID (HZB-8460)，就可以看到该网卡的内部照片，主板上清楚显示该网卡使用的是 Atheros 芯片组。

16.2 实现上的差异

802.11 并非严格的标准。标准的某些部分比较宽松，留给实现上相当大的空间。大部分实现的产品都上市不久，有时会有出人意表的行为。我曾经参与几次测试，使用几部相同的电脑。相同的操作系统，也使用完全相同的无线局域网络硬件与相同版本的驱动程序。虽然位于相同地点，各部电脑的配置设置也完全相同，表现上还是会出现显著的差异。

16.2.1 重新激动界面卡

802.11 是个复杂的协议，何况它还附带许多选项。使用最新的协议，通常可以发现最新的软件瑕疵。802.11 接口使用通用型微处理器来执行软件。既然软件成份居多，网卡如果出现问题，就可以通过“重新启动”(rebooting) 来清除储存在 MAC 处理器中任何协议的状态。外接式网卡可以通过插拔 (removing and re-inserting) 加以重置；内建的网卡则必须通过系统软件以冷开机 (power cycling) 的方式重新启动。只是重载驱动程序并没有用，因为我们的目的是要清除无线局域网络接口中所有状态。要排除无法正常运作的问题。也许必须重新启动网卡。如果有以下情况发生，首要步骤就是重启网卡：

用户端系统已经连接，但无法收送数据。如果此为加密网络，问题通常出在加密密钥没有同步。这个问题通常出现在漫游时，因为基站之间的任何变动，均会导致密钥重新发送。

看不到扫描结果。如果确定附近有网络存在，但用户端软件却无法加以显示，可能是这张网卡正处于无法提供扫描结果的状态。

发生一连串身份认证/连接失败的现象。当网络被列在“偏好”(preferred) 连接名单，但用户端系统所处的状态使其无法连接成功，就会进行一连串的重试动作。

16.2.2 扫描与漫游

在搜寻可连接网络以及判定是否切换基站方面，每张网卡的表现不尽相同。802.11 并未限制用户端设备如何决定是否切换基站，而且不允许基站以任何直接的方式影响用户端设备的决定。大多数用户端系统以信号强度或品质做为主要依据，并试图与信号最强的基站进行连接。

大多数网卡会随时监测所收到帧的信噪比，并以目前所使用的数据传输率，判定何时应该漫游到新的基站。如果数据传输率已经很慢且信噪比又低，用户端系统就会开始寻找其他基站。有些用户端系统会尽量拖延切换的时间，部分是因为寻找其他基站的过程需要转换到其他频道，因此会有连接中断的情况发生。霸着某部基站不放的用户端系统，称为罹患捕虫灯症候群 (bug light syndrome)。一旦连接到某部基站，它就与之终生厮守，就像虫子受到捕虫灯吸引一样。就算用户端系统距离基站愈来愈远，而且信号强度持续滑落，大部分网卡也不会开始进行漫游程序，直到几乎收不到信号为止。

802.11 的漫游机制，完全取决于用户端的决定。何时何地送出 Association request 信帧，完全操之于用户端系统的驱动程序与软件，对此 802.11 规格书完全没有任何限制。就算用户端决定与信号最差的基站连接，虽然是相当糟糕的做法，却仍旧符合 802.11 的规范。（由此产生的不幸后果，就是为了解决问题而更新驱动程序，也会出乎意料地改变用户端系统的漫游行为。）基站中并没有相关的协议任务可以影响用户端该于何处连接，以及是否应该离开。当需要争取时

效 (time-critical) 的串斗应用开始运用于 802.11，如何设计出更好的漫游技术将成为 802.11 的首要任务。借用 Milton Friedman 的话：不论何时何地，漫游均属用户端现象 (roaming is always and everywhere a client phenomenon)。

16.2.3 速率的选择

802.11 为各种的速率需求制定了基本规则，但是将速率选择演算法留给接口上所执行的软件自行决定。一般而言，界面在降速之前会试著以较高的速度传送几次。这部分只能算是普通常识。同样传送 1500 位元组数据的数据帧，以 11 Mbps 传送比 1 Mbps 快上 8 倍，就算启动防护机制，以 54 Mbps 的 802.11g 传送也将快上 20 倍。（如果不用防护机制，甚至快上 40 倍！）如果因为偶发状况造成数据帧损毁，在接受降速的惩罚之前当然应该试著重传几次。

降速演算法通常十分类似。重传帧数次仍然失败的话，就退而使用较低速率。大部分网卡一次只降一级，直至收到回应为止，虽然没有规定非得如此。如果刚开始碰到问题就降至最低速，也算是有效的速率选择演算法。升速演算法的运作方式刚好相反。如果接收到“些许”数据帧的信噪比优于目前速率所需，接口就可以考虑往上升速一级。

16.3 解读规格表

早期有关 802.11 设备的测试通常将焦点摆在传输距离 (range) 与传输量 (throughput)，因为其他没有什么好量测的。在某些环境，传输距离会是一项重要的因素。传输距离多少，部分可以从网卡规格表加以判定。

大致上，传输距离可说是接收灵敏度 (receiver sensitivity) 的函数。所谓接收灵敏度，是指接收器能够正确将信号转换为数据的最微弱信号。灵敏度愈高，传输距离就愈长。（提高灵敏度也有助于改善其他效能，不过传输距离是最便于讨论的一个。）

大多数厂商将焦点摆在改善效能，成果发表时（如 Atheros 的 XR 与 Broadcom 的 BroadRange）也颇为自豪。

不过，并非所有厂商都会提供完整的规格表。其中，Cisco 就揭露了相当多的信息；对所支持的每个频段，Cisco 提供了各个数据率的接收灵敏度。（这张网卡在 5 GHz 的效能稍微受到频率的影响。）许多厂商只提供所支持的数据率，完全没有提到灵敏度。

16.3.1 灵敏度比较

以下就以几张常见的 802.11b 网卡为例，比较它们的灵敏度。灵敏度系由 802.11 硬件层所决定。以直接序列而言，它被定义为：接收 1024 位元组的数据帧时，数据帧错误率 (frame error rate) 为 8% 的接收功率 • 标准要求 11 Mbps 的灵敏度需为 -76 dBm 或者更佳，2 Mbps 则是 -80 dBm 【注】 灵敏度的数值愈低愈好，因为这代表网卡可以接收到比规定更微弱的信号。

表 16-1 所显示的灵敏度报告取自各家的规格表与使用手册，其中包括四片著名的 802.11b 网卡，以及一片较新的 a/b/g 网卡 Cisco 的 Aironet 350 在微弱信号的处理上有不错的评价，这点完全可以从以下数据得到佐证。在 11 Mbps，它可以接收到比 Orinoco 网卡弱上一半，比 Microsoft 网卡弱上四分之三的信号。不过，科技的进展已经使得高位元率的灵敏度有所改善。所有上一代的网卡，均无法与采用 Atheros 芯片的 Cisco 三模 (tri-mode) 网卡相比。

表 16-1：不同网卡的灵敏度（以 dBm 为单位）比较

Table 16-1. Sensitivity (in dBm) for various cards

Card	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Cisco 350	-85	-89	-91	-94
Orinoco Gold (Hermes)	-82	-87	-91	-94
Linksys WPC11 (Prism)	-82	-85	-89	-91
Microsoft MN-520	-80	-83	-83	-83
Cisco CB-21 (a/b/g); 802.11b performance only	-90	-92	-93	-94

16.3.2 延迟范围

当无线电波碰到物体，接收端就会汇聚许多折射或反射波。最早与最后到达的两个波之间的时间差称为延迟范围（Delay Spread）。接收端可以在杂讯中检拾信号，前提是延迟范围不能超过限度。有些厂商会在规格中列出最大延迟范围。表 16-2 列出了三张网卡的延迟范围。

表 16-2：不同网卡的延迟范围（以 ns 为单位）

Table 16-2. Delay spread (in ns) for various cards

Card	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Cisco 350	140	300	400	500
Orinoco Gold (Hermes)	65	225	400	500
Cisco CB-21 (a/b/g); 802.11b performance only	130	200	300	350

延迟范围较大的网卡能够处理较严重的多重路径干扰。与此再度证明 Cisco Aironet350 不愧是当今的超级网卡。相较于采用 Hermes 芯片组的网卡，可以容许两倍以上的延迟时间。

第17 章 802.11 与 Windows

不论你是直接跳过第 3 至 16 章，或是已经读过所有理论性的章节，从现在开始，让我们卷起袖子，著手安装设备。

802.11 管理界面的发展，同样步上其他 Windows 应用程序的后尘。起初，每家厂商各自发展不同的配置界面。等到逐渐流行，Microsoft 就将 802.11 的状态设置整合到操作系统里，将各家厂商的管理工具统合为一个整体架构。

从系统与网络管理人员的角度来看，802.11 的操作与 Ethernet 并无不同。安装 802.11 驱动程序几乎和安装 Ethernet 驱动程序一样，而且无线网络接口的运行方式，也几乎和 Ethernet 接口相同。802.11 接口会产生 ARP 快取，甚至其他软件也会将无线接口视为 Ethernet 接口。不过和 Ethernet 驱动程序不同的是，在 802.11 驱动程序中有一些高级的选项与功能，其中包含了第八章所提到的额外管理功能。

本章主要探讨如何在 Windows XP 与 Windows 2000 操作系统上设置无线网卡。个人强烈建议使用 Windows XP，除了使用上比较容易‘也因为它实际上额外支持了一些较新的协议。第三方厂商(third-party)的【认证申请者】(supplicant)通常会将系统内建的【认证申请者】停用。不过，有时候驱动程序会拒绝使用 Microsoft 安全协议组 (security stack) 以外的安全系统。

17.1 Windows XP

Windows XP 延续视窗操作系统长久以来的传统，将原本只由其他协作厂商所提供的功能整合到操作系统当中。Microso 打造了一个标准的状态设置工具，能够设置多数网卡，称为 Windows Zero Configuration (也称为 ZeroConfig、ZeroConf 或 WzC)，不再仰赖 802.11 网卡厂商自行提供的设置工具。尽管网卡厂商还是必须提供驱动程序，不过状态设置则交由一致的视窗界面处理，不再通过个别网卡所提供的设置程序。本节之所以探讨 ZeroConfig，是因为它呈现出了一种与网卡无关的状态设置观点，因此得到网管与客服人员的青睐。

17.1.1 安装网卡

著手安装网卡之前，最好从网卡厂商网站下载最新的驱动程序。其他网络技术远比 802.11 成熟，所以不用经常更新驱动程序。遗憾的是，无线领域的产品随时推陈出新，驱动程序的变动也因此十分频繁。

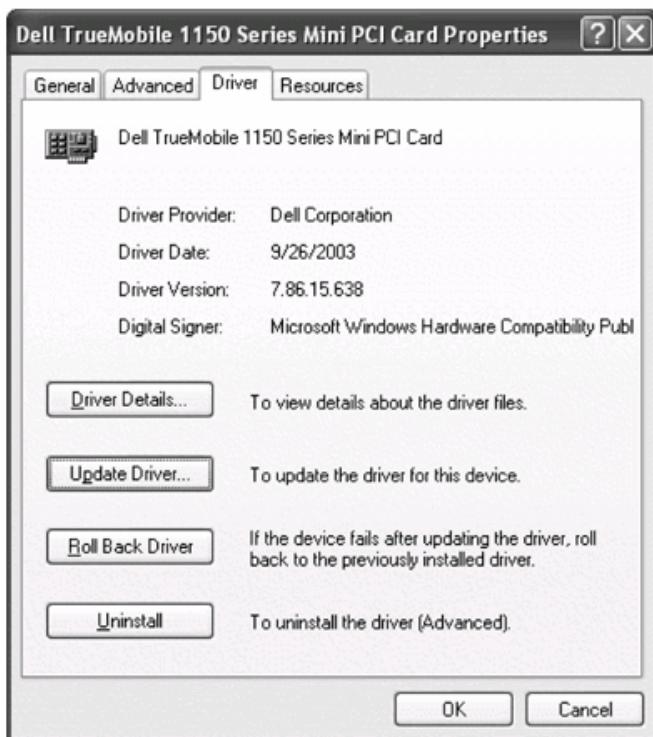
在主要厂商的网站上，通常可以找到 support (产品支持) 或者"download" (软体下载) 的网页。有些规模较小的厂商只是将公版 (reference design) 重新包装，也许并未在网站上提供驱动程序。遇到这种情况，通常可以使用芯片组厂商所提供的公版驱动程序。

有些驱动程序包在安装程序里头，我通常避而不用。有些网卡厂商会另外支付权利金，使用其他第三方厂商所开发的 802.1X 协议组，不过可能会与 ZeroConf 相冲。安装网卡之前，最好的做法通常是从网卡厂商的网站取得最新的驱动程序。

17.1.1.1 第三方厂商的 802.11 X 协议组与驱动程序更新程序

市面上有许多第三方厂商 (third-party) 所开发的 802.1X 协议组。在 Windows 操作系统上，它们通常被实现成网络协议组的一个层级，在硬件与网络协议之间拦截 EAPOL 数据帧。有些网卡厂商无法忍受内建之 Microsoft **suplicant** 开发进度的落后，转而采用第三方厂商所提供的协议组来支持 802.1X，许多第三方厂商所开发的协议组与 ZeroConfig 并不相容，它们通常需要额外的软件设置工具，并非通过 Zeroconf 来设置参数。这些协议组可能也需要额外的「认证申请者」 (supplicant) 软件来支持比较高级的设置。要避免使用这些附带的 802.1X 协议组，更新驱动程序时就不要使用厂商所提供的安装程序。最好的做法是从厂商的网站下载驱动程序，解压缩后，利用设备管理员 (device manager) 的更新驱动程序按钮为操作系统更换新版驱动程序。图 17-1 显示了如何仅更新驱动程序。只要点选「hardware properties」的「Driver」标签页，就可以看到「Update Driver」按钮。

Figure 17-1. Updating the driver without the baggage



要避免安装其他第三方厂商的 802.1X 协议组有两个小技巧。有些驱动程序的安装程序，其实是自行解压缩的 ZIP 文件，可以用解压缩软件打开。将驱动程序解到临时文件夹，然后以个别文件进行更新。另外一种方法是以安装程序进行安装，然后立即执行反安装程序。大多数反安装程序只会移除状态设置工具以及第三方厂商的 802.1X 协议组，但会留下新版的驱动程序。

17.1.1.2 Cisco 用户端软件

Cisco 网卡还有另外一个陷阱。防护型 EAP（Protected EAP，简称 PEAP）是仍在开发中的标准。虽然由 Cisco 与 Microsoft 双方代表所制定，两家公司的实现版本并不相容。业界所发行的大多数 PEAP 产品通常会自动检测系统使用的是哪个版本。

即使 Cisco 的认证服务器 CiscoSecure ACS 当中也有一个选项，可以设置与 Microsoft 的 PEAP 实现相兼容。Microsoft 的 PEAP 实现版本支持以 EAP-MS-CHAP V2 与 EAP-TLS 做为内部身份认证协议(*inner authentication protocol*)；Cisco PEAP 实现版本则支持 EAP-SIM 与 EAP-GTC。大部分使用 Windows 的组织会倾向使用既有的用户数据库，例如 Active Directory，如此一来，就只能以 EAP-MS-CHAP-V2 做为内部身份认证协议。

做为集成软件的一部分。Cisco 会以本身的 PEAP 软件取代系统所使用的标准(Microsoft)PEAP。如要使用 Microsoft PEAP，必须先移除 Cisco PEAP 驱动程序，然后以 Microsoft PEAP 取代。由于整个系统只能使用一套 PEAP 软件，因此安装 Cisco PEAP 将会影响系统目前所有的卡片，而不只是 Cisco 的网卡。参见表 17-1

Table 17-1. Inner EAP methods

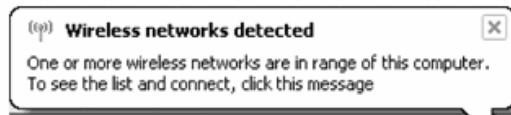
EAP method	Cisco or Microsoft PEAP?	Authentication credentials	Notes
EAP-MS-CHAP-V2	Microsoft	Shared password (or MD4 hash of the password)	Used with Windows domain authentication; easy to plug in to Active Directory
EAP-TLS	Microsoft	User certificate	Generally not used
EAP-SIM	Cisco	Subscriber Identity Module (SIM) card	Based on GSM mobile telephone authentication; not yet widely used
EAP-GTC (Generic Token Card)	Cisco	Cleartext authentication string passed through encrypted tunnels	Can be used for token cards as well as a generic method for static passwords

有些膝上型电脑厂商已经在系统中预先安装好 802.11 网卡，而且也载入与设置好相关软件。如果配备 Cisco 网卡，系统中可能已经预先安装 Cisco PEAP，那么你的组织就必须调整系统的建立程序，以便回头使用 Microsoft PEAP。要回头使用 Microsoft PEAP，必须重新安装最新的更新套件（service pack），以 Microsoft 的 PEAP 驱动程序覆盖 Cisco 的 PEAP 驱动程序。

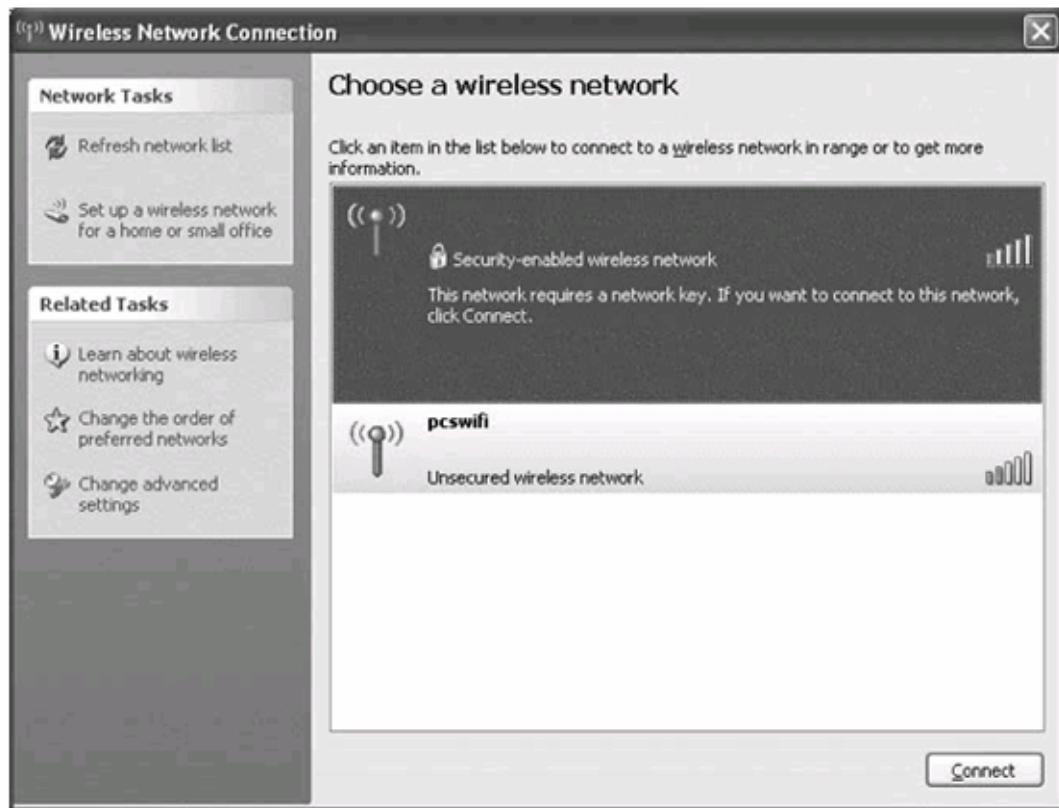
17.1.2 选择网络

Windows 启动后, ZeroConfig 系统就会尝试找出附近所有网络。ZeroConfig 会自动连接到目前已有状态设置文件的网络。如果尚未设置任何网络, 无线接口上将会出现如图 17-2 所示的气泡 (bubble) 视窗。

Figure 17-2. Prompt that WLANs are in the neighborhood

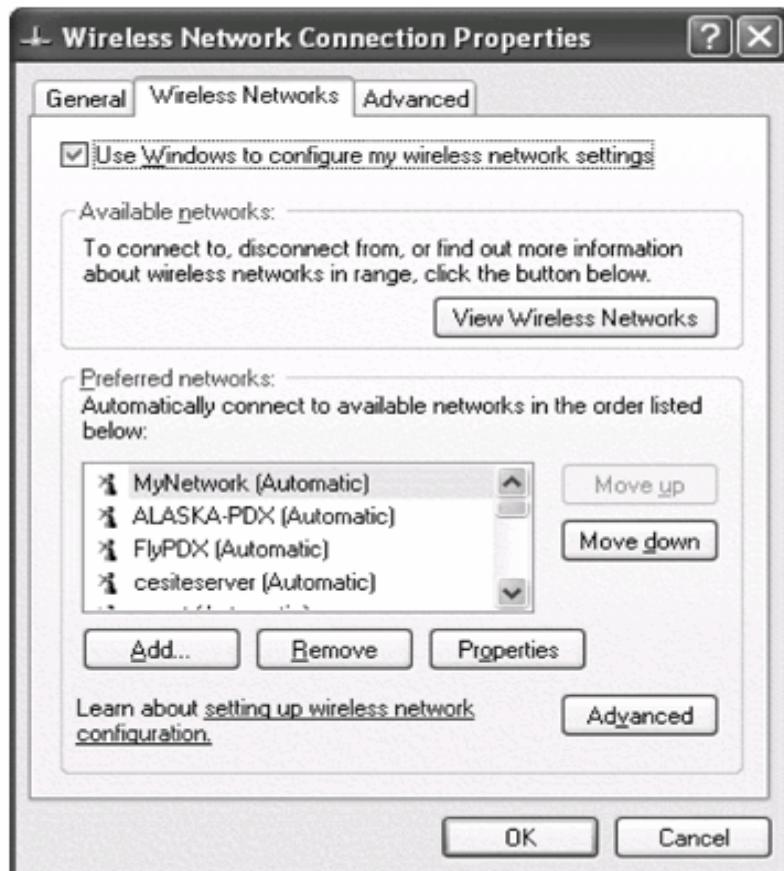


只要点选该视窗, 或者以右键点选无线界面选取“View Available Wireless Networks”, 就会列出所检测到的无线网络 (图 17-3)。任选其中一个网络加入, Windows 就会自动尝试正确的状态设置。不过, 它无从选择适当的 EAP 认证方式, 因此通常不能自动连接至加密网络。连接到未加密的网络十分容易, 不过系统会提示即将连接至不安全的网络, 要求使用者确认。

Figure 17-3. Viewing available wireless LANs

17.1.3 安全性参数与 802.1X 的状态设置

有时候，网络的安全性属性必须通过手动方式设置。Windows 能够自动选用预设的加密与身份认证方式，不过还是可能出错。802.1X 通常预设使用 EAP-TLS，虽然 EAP-TLS 并不常用。要更改安全性参数，可以点选「Change Advanced Settings」进入【interface properties】页面，然后点选【Wireless Network】标签页（图 17-4）。

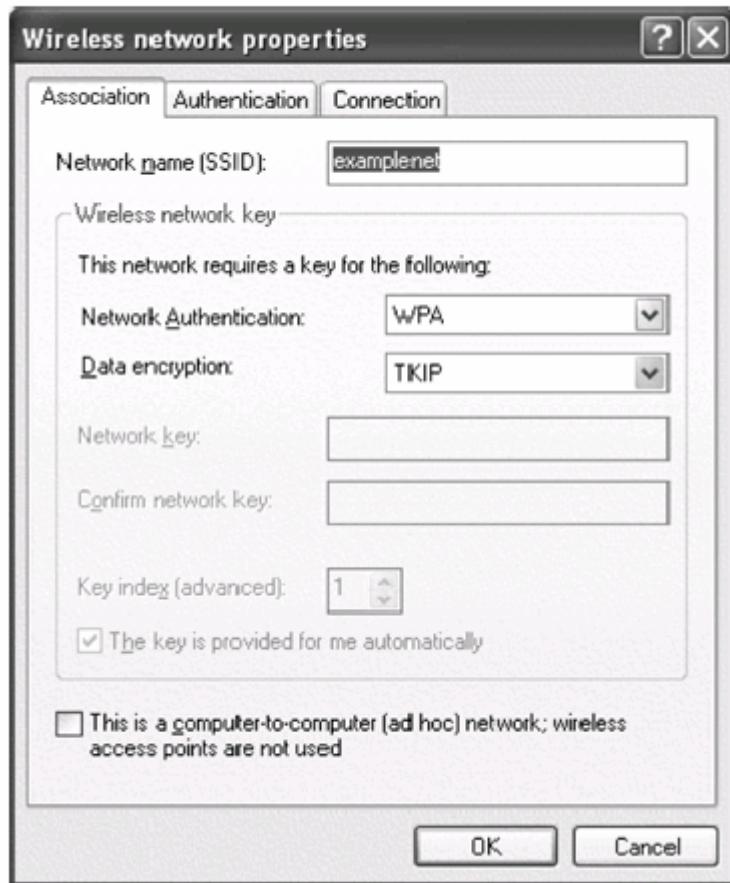
Figure 17-4. Wireless Networks tab

要新增一个网络，可以从「Preferred Networks」中点选，然后选择「Properties」，

或者也可以指定一个网络名称然后手动加入，如图 17-5 所示。如果要手动加入网络，必须从头开始设置正确的属性。如果 Windows 已经自动设置好网络，它将会从可用的协议中挑选安全性最高者。

ZeroConf 的优点之一，就是可以同时维护多个不同无线局域网络的属性，然后连接至已经设置无误的网络。

Figure 17-5. Association properties



首先必须决定的是，你打算使用的身份认证类型【译注】·图中只显示出 WPA · 不过其实有四种选项：

Open authentication (开放系统身份认证)

用于完全不进行身份认证，以及使用旧式动态 WEP 的网络。使用这个选项，代表一开始所进行的链路层身份认证，使用的是第八章所描述的开放系统认证方式。实现开放系统认证的网络可以搭配 802.1X，但非必要。

Shared authentication (共享密钥身份认证)

这个选项用与，以共享密钥 WEP 进行身份认证的网络。它会要求使用者在 Network Key 栏位输入密钥。以共享密钥 WEP 进行身份认证并不是十分牢靠，也无法提供严密的保护。除非所欲连接的 AP 要求，否则没有理由使用这个选项。

WPA authentication (WPA 身份认证)

这是 WPA Enterprise 的简称。它使用 802.1X 进行使用者身份认证，同时使用 802.11i 所定义的验证密钥模式。除非已经安装 WPA 软件且驱动程序支持 WPA，这个选项才会出现。

WPA-PSK authentication (WPA-PSK 身份认证)

这是 WPA Personal 的简称。此验证方式使用预设主钥 (preshared master key)，而非使用衍生的主密码 (master secret)。链路加密密钥是由此预设密钥以及用户端与基站之间所交换的随机值所衍生。

选好身份认证方式之后，接下来需要选择链路所使用的加密方式。

Disabled (停用)

这个选项用于不采用链路层加密的开放网络。有些 802.11 热点会使用这个选项，虽然未来应该会提供较坚固的加密方式。

WEP

这个选项包括人工与动态密钥。要使用动态 WEP，则勾选「The key is provided to me automatically」选项。人工手动设置 WEP 密钥则不需勾选这个选项，只要输入密钥即可。

TKIP

这个选项用于 TKIP，这是 WPA 网络的预设值。

AES

Windows 并未提到 CCMP，在 ZeroConf 状态设置中是以 AES 称之。【注】这是目前无线网络上最坚固的加密方式。

此对话框也提供手动输入密钥，或者使用自动提供密钥的选项。使用 802.1X 时会自动提供密钥，所以这个选项就不让使用者勾选。使用 WPA 身份认证的网络必须使用自动密钥；使用 WPA-PSK 的网络则必须在此输入预设共享密钥。表 17-2 整理出了目前已支持的加密与身份认证选项。

Table 17-2. Summary of encryption and authentication methods

Authentication framework	Supported encryption	Authentication methods
Open	Disabled (no WEP)	802.1X optional
	WEP (key specified)	
	WEP (automatic key)	
WPA	WEP (automatic key)	802.1X required
	TKIP	
	AES (supported cards only)	
WPA-PSK	WEP (automatic key)	802.1X not used
	TKIP	
	AES (supported cards only)	

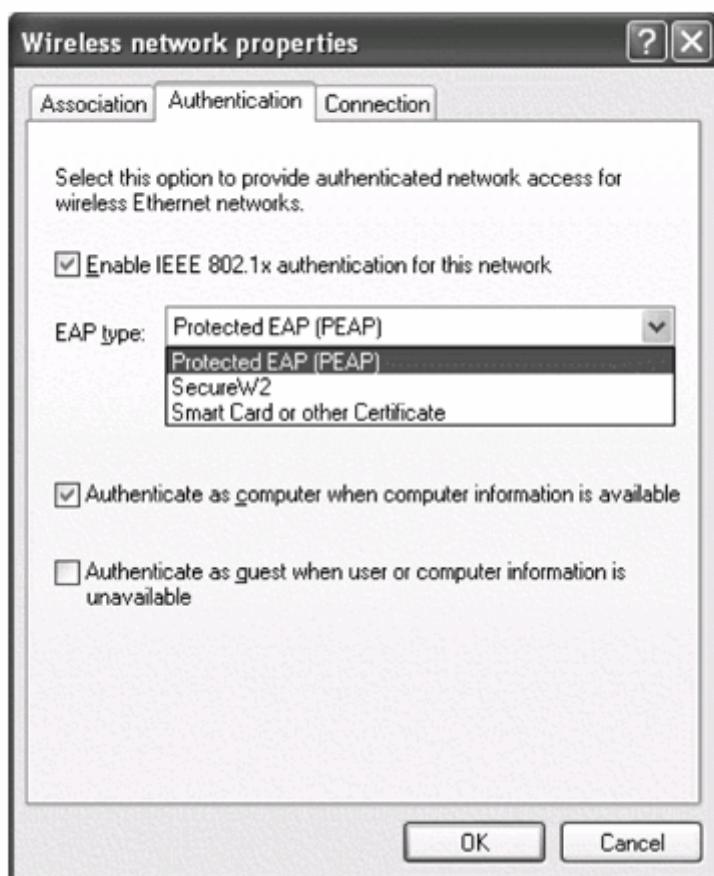
设置好「association」属性后，接下来是设置「authentication」属性。图 17-6 显示的「authentication」属性标签页，是用来选取 EAP 认证方式的画面。画面显示这部机器有三种选项：PEAP、EAP-TLS ("Smart card or other Certificate" 以及 TTLS ("SecureW2")。点选【properties】按钮之后，接著对所选的 EAP 认方式进行状态设置。

在 EAP 认证方式底下，有一个「Authenticate as computer when computer information is available」选项。勾选这个项目允许系统在网络上使用机器凭证(machine credential)进行身份认证！如此可以在验证使用者之前，让 Windows 网络进行一些必要的设置。此一程序的运行方式将留待本章稍后探讨。

17.1.4 设置 EAP 认证方式

虽然可以在「authentication」标签页选择一种 EAP 认证方式，但状态设置还是过点选「Properties」按钮来进行。并非所有出现在「authentication」属性页的认证方式均由 Microsoft 提供。其他第三方厂商所提供的软件，也会在下拉式选单中加入其他 EAP 类型。「EAP type」方格中所显示的文字，可用来判定目前究竟使用的是 Microsoft 或 Cisco 的 PEAP - Microsoft PEAP（技术上称为 PEAPv0）显示为“Protected EAP (PEAP)”，而 Cisco PEAP 仅显示为“PEAP”。

Figure 17-6. Authentication properties



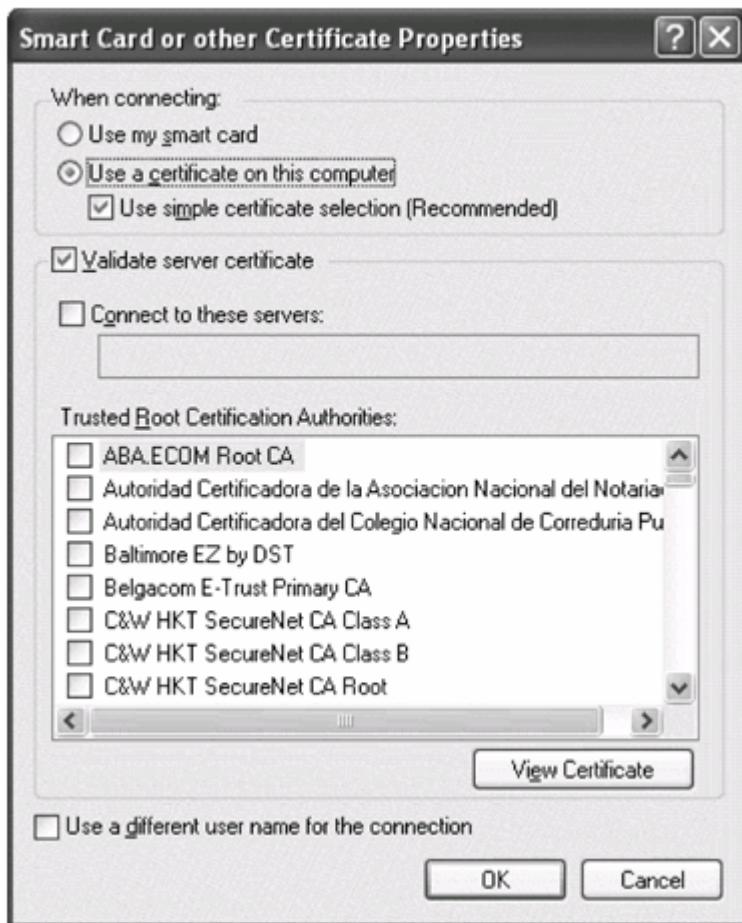
17 . 1. 4. 1 EAP-TLS

图 17-7 显示了选用 EAP-TLS 时所出现的状态设置画面。最上方的选项指出用来验证使用者的用户端凭证(client certificate) 究竟储存于智慧卡，或是由 Windows 所维护的凭证存放区 (certificate store)。大型组织会发智慧卡给员工，有时就内建于员工识别卡当中。中小型公司则比较倾向发行电脑凭证 (certificates stored on each machine)。

服务器验证是打造安全网络的关键。Microsoft 认证申请者允许两种不同层次的身份认证。当认证服务器对用户端展示凭证时，用户端可以验证该凭证是否发自所信任的凭证机构。如果使

用自行签署的凭证，就不该勾选这个「validation」选项。如此一来，认证申请者便会信任所收到的任何凭证，门户便因此洞开。验证列于服务器凭证上的名称，确定它的确来自自己知的 DNS 网络，可提供额外的防护。

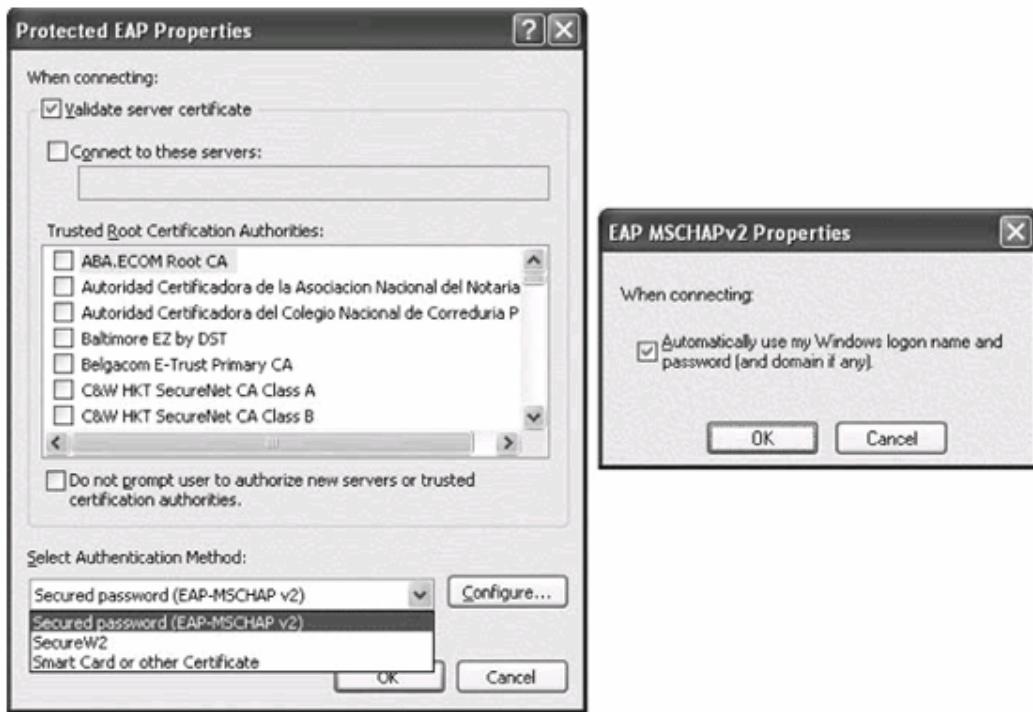
Figure 17-7. EAP-TLS configuration screen



17 . 1. 4. 2 PEAP version 0

图 17-8 所显示的 Microsoft PEAP 状态设置与 EAP-TLS 类似。服务器验证不变，应该予以启用。主要的设置项目，在于防护管道(protected tunnel) 中所使用的内层身份认证方式 (inner authentication method)。表 17-1 对这些选项有简短的说明。

Microsoft 的实现版本允许此列表中包含其他 EAP 身份认证的外挂 EAP authentication plug-in 选项。预设上，此列表中包含 EAP-TLS 与 EAP-MSCHAP-V2。后者比较常见，因为它可以轻易地与 Active Directory 或者 NT Domain 使用者帐号整合在一起。每种内层身份认证方式都可以有自己的子设置页。以 EAP-MSCHAP-V2 为例，子设置页只有一种选项。一旦勾选这个选项，Windows 登入凭证将被自动转送至网络上。这个选项有时也称为 PEAP 单一登入 (single sign-on)，因为接下来认证申请者会自动送出登入凭证 (logon credential)，不会再提示终端使用者输入帐号密码。

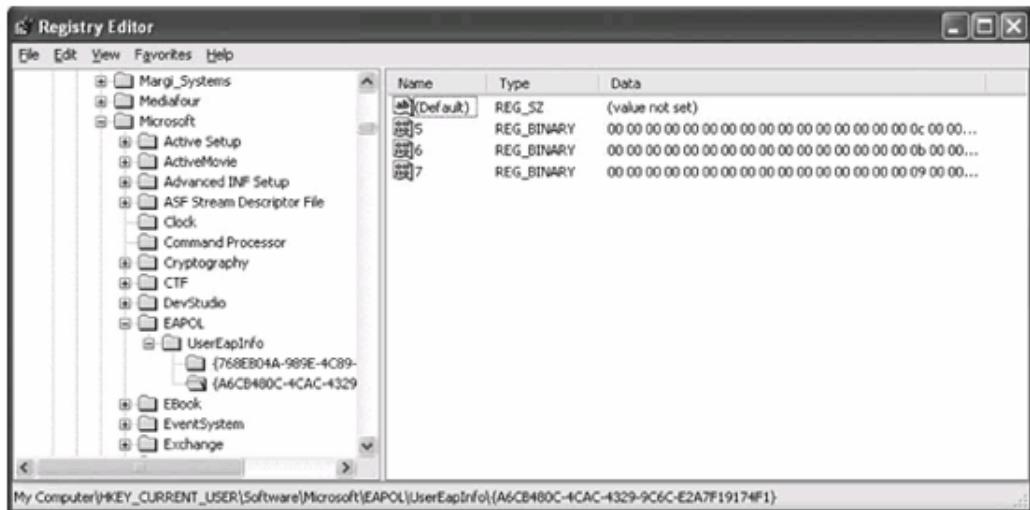
Figure 17-8. PEAP version 0 configuration

17.1.4.3 清除系统登录档中的凭证

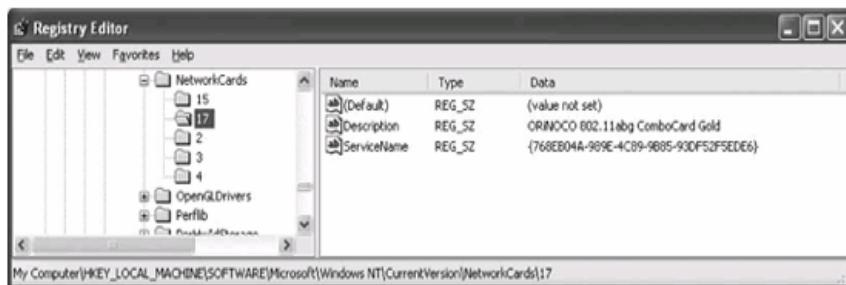
如果不使用单一登入，使用者的密码将会储存于系统登录档（Registry）。当使用者连接至某个网络，系统便会提示使用者输入使用者名称、密码以及 Windows 域。如果身份认证成功，凭证就会被存在系统登录档供以后使用。未来，每当使用选择与此网络连接，Windows 就会自动传送之前已经验证成功的凭证。

虽然十分方便，不过凭证快取功能还是有所不足，主要是缺乏一种便利的方式。清除不再需要的使用者凭证。许多无线网络采用既有的身份认证方式，然而人们通常均采行定期更换密码的政策。当密码被迫更新，系统登录档中的凭证快取而失效，使用者必须将它从系统登录档中清除之后，方能变更密码。

使用者凭证存放在系统登录档的 HKCU\Software\Microsoft\EAPOL\User 路径，如图 17-9 所示。不使用单一登入进行 PEAP 身份认证的网络接口，会分不同的识别码来表示。识别码是一连串文数字所组成的长字串。

Figure 17-9. Stored user credentials in the Registry

每张网卡均会有一个识别码。在图 17-9 中，识别码为 {768EB04A-989E-4C89-9B85-93DF52F5EDE6} 的接口存放了三个之前快取的网络密码。要移除某个网络的快取密码。可以删除相应的登录机码 (registry key)。要找出哪个字串对应到哪个网络接口，请先找出 `HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NetworkCards`，然后检视该值底下的机码。图 17-10 显示该字串对映到“ORiNOCO 802.11abg ComboCard Gold”。

Figure 17-10. Cross-referencing the interface to the text name in Registry

将使用者密码储存于系统登录档，有损要求使用者输入密码之 Windows 申请者易用性，Microsoft 方面辩称密码快取是相当方便的功能使用者可以不需要一再输密码，同时也指出使用既有 Active Directory 使用者帐号与自动使用 Windows 的好处。不过，其他厂商所提供的申请者，则是将使用者密码储存在更方便访问的地方。

Windows CE 上的 Microsoft 申请者并不会快取使用者凭证。每当申请者重新进行身份认证，就会提示使用者输入凭证（即帐号密码）。大多数 Windows CE 设备有键盘。很难快速输入凭证。

17 . 1. 4. 4 SecureW2: TTLS 与 ZeroConfig

第三方厂商所提供的申请者软件让网管人员陷入困难的抉择。使用者通常习惯使用 Windows 界面来设置无线网络。不过 TTLS 功能通常只能通过第三方厂商所开发的软件提供，但是要使用这些软件，却得停用 ZeroConfig。所幸并非没有别的解决方案。ZeroConfig 提供了一个编程界面（programming interface），可以通过实现特定认证方式的外挂程序（plug-ins），支持额外的 EAP 认证方式。SecureW2 是给 Window ZeroConfig 使用的 TTLS 外挂程序。它是一个开放源码方案。以 GPL 授权方式发行。源码与可执行套件可从 <http://www.securew2.com> 网站下载。要访问外挂程序 SecureW2 的状态设置，也是通过 EAP-TLS 与 PEAP 所使用的画面。初次点选【Properties】按钮时，SecureW2 就会显示状态设置主画面（图 17-11）。SecureW2 的状态设置数据会被汇集到一个设置文档中。ZeroConfig 所储存的每个无线网络均会对应到一个 SecureW2 设置文件(profile)。不同的网络可能分别对应到各自的 SecureW2 设置文件。管理人员可以使用安装程序包装工具(packaging tool)来产生所需要的 SecureW2 安装程序(installer)，将设置文件包含在安装程序中。

设置文件是由画面中四个标签页来定义的。其中，【Connection】标签页用来指定 TTLS 在第一阶段所使用的身份。如图 17-12 所示。如果不勾选这个项目，则第一阶段将会使用第四个标签页所指定的使用者帐号。外层身份(outer identity) 预设会使用匿名(anonymous) 选项。

服务器认证是通过第二个标签页 Certificates 来设置的，如图 17-12 所示。这里不会列出一长串的凭证供使用者挑选，使用者必须自行输入每个凭证授权单位(certificate authority)。只要点选【Add CA】按钮就会显示凭证授权单位列表。在 XP Service Pack 2 中，此处所列的名单取自电脑的凭证存放区(certificate store)。和 Microsoft 认证申请者一样，使用者还可以验证凭证中的服务器名称是否相符。

Figure 17-11. SecureW2 main screen

设置好外层使用者名称与网络身份认证后，接下来就是设置内层身份认证所需要的使用者帐号。身份认证类型是通过【Select Authentication Method】下拉式选单来设置的（如图 17-14）。之所以使用 TTLS，通常是因为需要使用明文密码进行身份认证；在这种情况下，必须将「Select Authentication Method」设为 PAP。第四个标签页用来设置使用者帐号。

17.1.5 WPA 的状态设置与安装方式

Wi-Fi访问防护(Wi-Fi Protected Access, 简称 WPA)是大多数组织所认可的安全底线。Windows XP Service Pack 2 内建 WPA, XP Service Pack 1 则需要另外下载补丁(patch)。使用 WPA, 相当于在 WPA 与 WPA-PSK 这两种身份认证方式当中选择其一。Microsoft 并未在其他操作系统版本中实现 WPA, 要在其他操作系统上使用 WPA, 必须使用第三方厂商的认证申请者软件。

要使用 WPA, 必须得到整个系统的支持。除了操作系统, 硬件和驱动程序都必须支持 WPA。驱动程序不会显示末支持的选项。以 Dell TrueMobile 1150 无线网卡为例，并没有所谓的 AES 选项，因为该网卡只支持 RC4 加密。如果 WPA 使用上不如预期，住连络厂商的客户支持部门之前，记得确认是否已经安装最新的驱动程序。

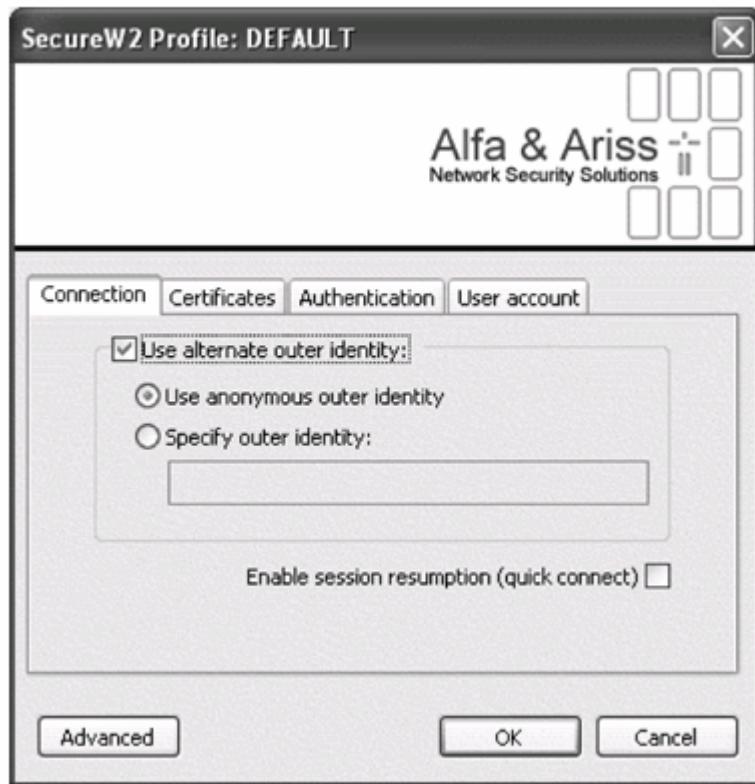
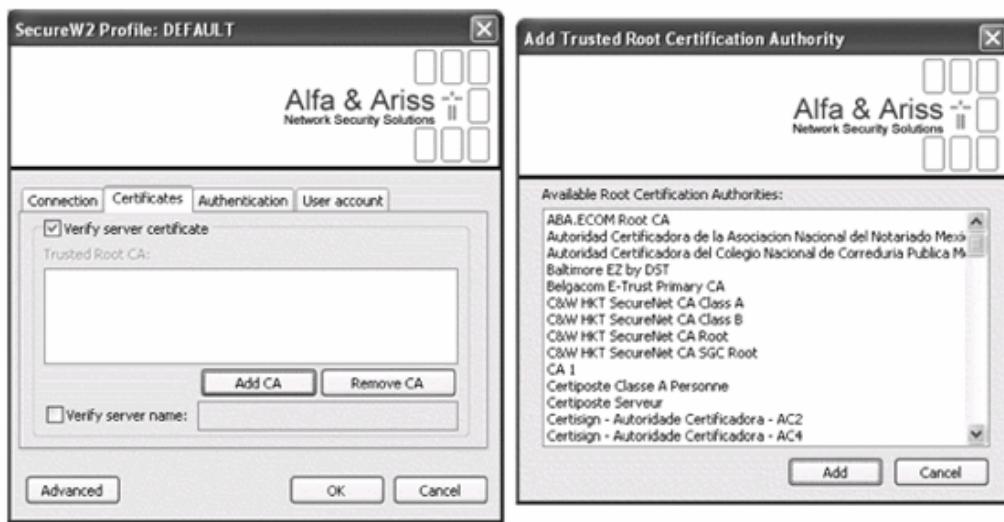
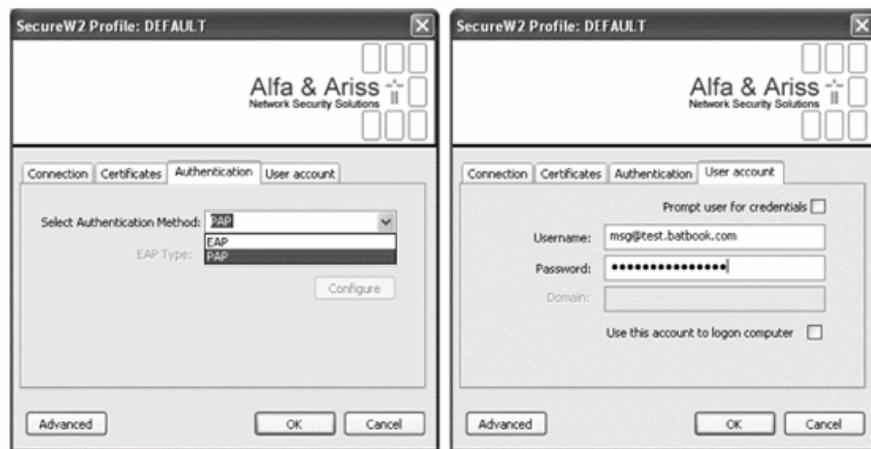
Figure 17-12. SecureW2 profile creation**Figure 17-13. SecureW2 certificate configuration**

Figure 17-14. SecureW2 authentication method and user account screens



17.2 Windows 200

Windows 2000 仍然广为使用。为了省钱，许多旧机器并未升级到 Windows XP，Windows 2000 依然是堪用的操作系统。Windows 2000 上的无线网络设置比 Windows XP 复杂，绝大部分是因为在无线网络的选择以及相应的安全性设置上缺乏实质的整合。

从一开始，Windows 2000 就不支持 802.1X。802.1X 是在 Service Pack3 之后才出现的补丁 (patch)，【注】后来整合到 Service Pack 4 当中。Microsoft 并未将 WPA 功能移植到 Windows 2000，不过在 Windows 2000 上可以使用 WirelessSecurity Corporation (<http://www.wirelesssecuritycorp.com>) 所开发的 WPA 用户端程序。有些观察家认为让 Windows 2000 支持 802.1X 算不上 Microsoft 的优先事项，如今居然出现在最近发行的更新套件中，显然要说服使用者升级操作系统已经愈来愈难。

虽然已经将 802.1X 的状态设置整合到驱动程序层，Windows 2000 还是必须使用工具程序来设置系统所要连接的网络。对必须往返加密与未加密网络的使用者而言，这样特别容易造成问题。虽然使用工具程序进行网络切换很简单，不过通常需要手动启动或停用安全性选项 Windows 2000 为网管人员带来困难的抉择。如果软件设置工具包含第三方厂商所提供的 802.1X 协议组，就必须额外付出心力来区分两者。

17.2.1 动态 WEP 的状态设置

Windows 2000 的无线状态设置服务 (Wireless Configuration Service) 只支持动态 WEP 加密。至于 TKIP，则必须通过第三方厂商的申请者软件提供支持。要设置动态 WEP，必须通过网卡所提供的工具设置 WEP 密钥。网卡设置程序在乎的是，目前是否使用人工手动设置的 wEP 密钥。驱动程序会将数据帧传给网卡，并且使用网卡密钥快取中的密钥为之加密。不过，无线状态设置程序会依网络所设置的安全性政策，将新的密钥塞进网卡。

人工 WEP 密钥无须加以设置，只要长度正确即可。在使用 128 位元 WEP 的网络上，必须输入 26 个十六进制的数字做为密钥，例如 12345678901234567890123456。这个假密钥 (dummy key) 永远派不上用场，因为 802.1X 身份认证成功后，就会被动态产生的密钥所取代。

就我经验所及，Windows 2000 的无线状态设置服务不如 Windows XP 稳定。有些瑕庇（bugs）导致此服务即使在身份认证成功后依然会失灵。值得注意的是，这类情况所表现出的症状是初次连接可以成功，之后进行重新身份认证时连接就会中断。没有软件负责处理 802.1X 数据帧，任何尝试重新进行身份认证或者更换密钥的操作均将失败。

17.3 Windows 电脑验证

当初设计 Windows 身份认证子系统时，系通过网络连接传送使用者凭证（usercredentials）给网域控制服务器（domain controller）来进行验证。当网络子系统开始运行，如果所使用的协议需要，就会取得一组网络地址，然后连络网域控制服务器。除了验证使用者身份，网域还会提供若干其他的服务。网络管理人员可以定义网域政策，用来规范网域内任何系统的行为，也可以定义登入命令稿，将自定用户环境纳为登入程序的一部分。

在有线世界中，网域服务不成问题。使用者只要连上网络，系统本身就会开始发送数据包。当初设计 Windows 开机程序时，还不存在任何方式可以对有线网络连接进行身份认证。然而，在无线世界中，使用者必须通过身份认证方能启动无线连接，网络身份认证就有点变成鸡生蛋蛋生鸡的问题。只要在登入视窗输入帐号密码，使用者当然可以通过无线网络身份认证，不过一开始若无网络连接可以将数据包传送给网域控制服务器，又如何验证这些凭证呢？Windows NT、2000 与 XP 以凭证快取提供部分解决方案。只要使用者成功登入属于 Windows 网域成员的电脑，就会将使用者凭证置于快取供未来使用。

凭证快取只是部分的解决方案，因为这意谓著必须先以有线方式登入电脑。Microsoft 后来开发出比较好的解决方案，称为电脑验证（computer certificate）或机器验证（machine certificate）。当系统初次启动，电脑便向无线网络验证其身份。当无线网络开始启用运行时，电脑就可以从网络下载必要的信息，然后与网域控制服务器进行使用者身份认证。如此一来就算过去从未登入，系统中也不存在凭证快取，使用者还是能够进行登入。

有相当多的功能都倚赖是否可以在开机程序进行时及早取得网络连接。除了网域服务，网络磁碟机连接（drive mapping）也进行得相当早，如果电脑没有通过身份认证，这些操作就会失败。在大多数情况下，Windows 电脑验证都应该被视为网络能否运作顺畅的必要条件。

要使用 Windows 电脑验证，后端必须有部 Active Directory 服务器。每部电脑在 Active Directory 中必须有自己的帐号，而且必须具备拨入权限（Dial-Inpermission）。

17.3.1 运作方式

电脑验证在开机程序中额外加入了 802.1x 身份认证程序。一开始电脑会先验明正身。从登入视窗取得使用者凭证（帐号密码）后，随即进行 802.1x 交换程序，对使用者进行身份认证。整个程序如图 17-15 所示。

本图说明了整个开机程序的主要步骤。当电脑开机并且启动它的网络系统时，便会开始此程序。进行其他系统开机任务的同时，开始通过 802.1x 验证机器。

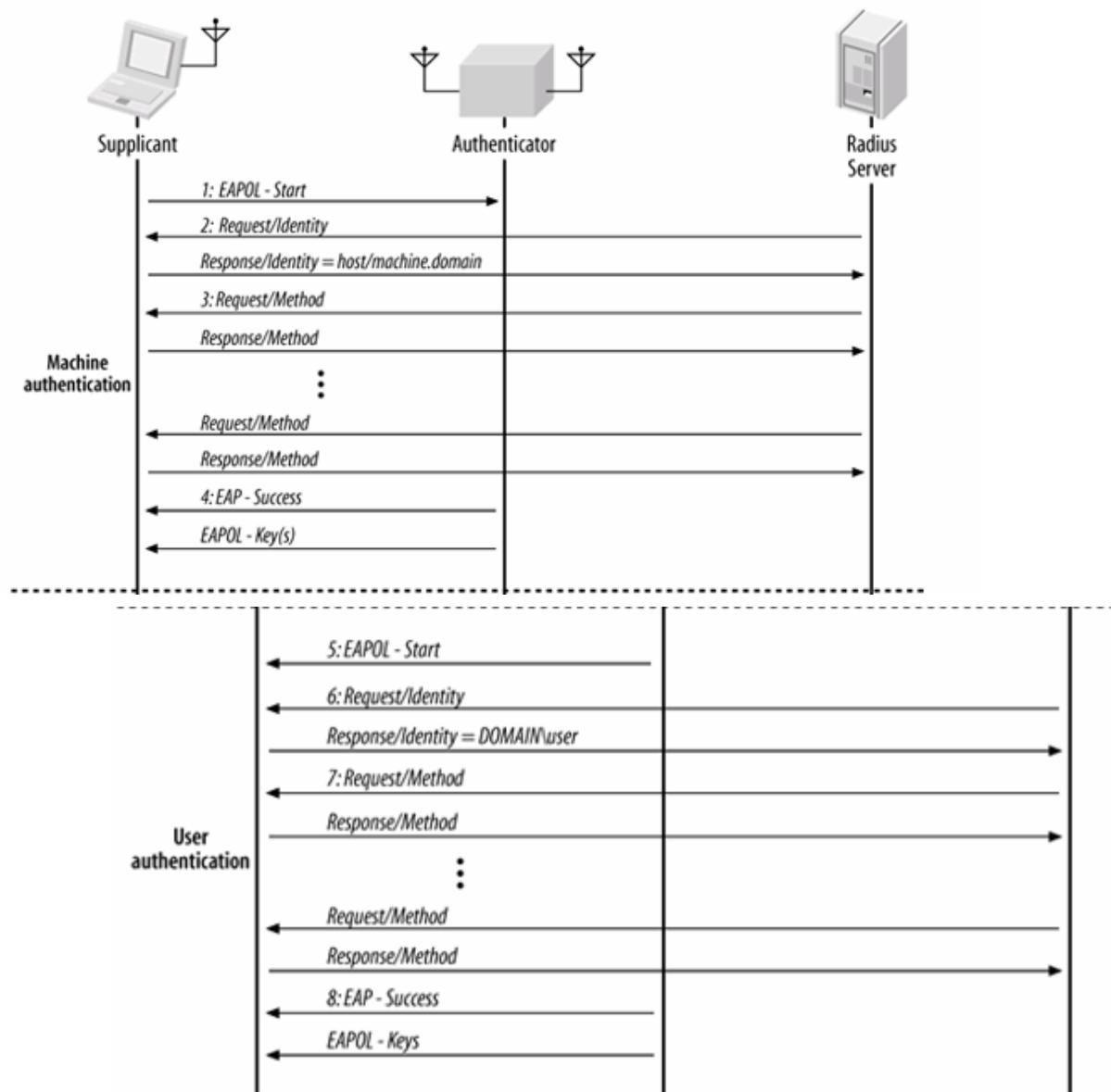
1. 机器验证开始。它可以始于申请者所发出的一个 EAPOL-Start 数据帧，也可以始于认证者所发出的一个 Request/Identity 数据帧。

2. 网络得知机器的身份。进行初次验证时，“使用者”（机器）身份系以 host/ComputerName. Active DirectoryDomain 的格式出现，ComputerName 与 ActiveDirectoryDomain 可以通过系统属性得知。

3 电脑与 RADIUS 服务器上的帐号（或是 RADIUS 服务器后面的数据库）进行验证。这个程序或许需要来回进行好几回合，因为必须交换凭证，产生加密密钥 等等。

电脑验证与使用者验证使用相同的 EAP 认证方式。如果使用者验证使用 EAP-TLS，则电脑也必须有自己的凭证。如果使用者验证使用 PEAP，电脑则会使用 EAP-MSCHAP-V2 做为内层认证方式。内层认证所使用的“密码”，是在电脑加入网域时产生的，其他软件无法使用。

Figure 17-15. Startup process with Windows computer authentication



4、一旦验证成功，电脑就会与网络连接。它会从认证者方面接收到 EAP-Success 数据帧，在无线局域网络上，则是接收到 EAPOL-Key 数据帧，提供连接所需要的密钥。

验证完成后，电脑就会与网络连接，并且可以收送数据包。送出 DHCP 请求之后，电脑就可以加入网络，并且通过 NetBIOS over TCP/IP 找到最近的网域控制服务器。在开始进行使用

者身份认证之前，电脑可以跟网域控制服务器建立一种关系。使用者按下 **Control-Alt-Delete** 开始登入程序。系统将会通过其与网域控制服务器的连接，载入使用者登入命令脚本（**user login script**），设置 **Windows** 网域政策，以及进行其他登入操作。

5.当使用者桌面即将启动时，开始进行第二道身份认证。终端使用者的身份认证必须由操作系统启动。通常，程序一开始所建立的机器验证只会被使用几分钟，之后就开始进行使用者身份认证。

6.网络要求终端使用者表明身份。在 **Windows** 网络上，通常采用 **DOMAIN\ user** 形式的身份格式，其中包含 **Windows NT** 风格的网域名称以及使用者帐号。

7. 申请者以使用者凭证进行身份认证。就 **Windows** 申请者而言，电脑验证与使用者验证必须使用相同的 **EAP** 外挂软件。和上一个步骤相同，必须经过几个回合，方能够建立安全的加密通道。

8.使用者验证成功，同时取得连接所需要的密钥。这些密钥有别于电脑密钥，因为来自不同的 **TLS** 会谈（**session**）。

电脑验证和使用者验证可以分开处理。这两种验证的授权可以各自进行。例如，在动态指定 **VLAN** 的网络中。可以分别为电脑帐号与使用者帐号指定不同的 **V LAN**。早期版本的 **Microsoft** 申请者在验证成功后不会触发 **DHCP** 请求，造成使用者无法收送数据包。目前已有修正程序可以解决这个问题。

第18 章 802.11 与 Macintosh

Apple Computer 向来是 802.11 设备市场上开疆辟土的主要造势者。大部分 802.11 厂商是在标准委员会的参与，以及技术开盘方面有所贡献。Apple 的贡献则是以简驭繁，将复杂的技术萃炼为易用的型式，以及发挥大众行销的专长。

1999 年当时，802.11 技术相当看好，也在一些应用市场中证明其价值。当时，802.11 接口卡售价约 300 美元，基站则叫价 1.000 美元左右。Apple 看出 802.11 技术的发展潜力，因此态度十分积极，推出价格只有 300 美元的基站，以及 99 美元的接口卡。当竞争者突然以三分之一的价格介入市场，其他厂商只好大幅降价以为因应，整个市场随即起飞。从那时起，价格就开始一路下跌。

Apple 以 AirPort 做为无线网卡的品牌名称。第一代 802.11b 网卡就叫做 AirPort，新一代的 802.11g 硬件则称为 AirPort Extreme。（由于 Apple 主推 SOHO 市场，因此并未销售 802.11a 相关产品。）本章将只讨论 AirPort Extreme 产品，不过两者在配置设置与管理方面的差异不大。不论是无线界面，或者 Apple 802.1X *supplicantC*（认证申请者）的设置均十分容易。802.1X *supplicant* 首度出现于 OS X 10.3，不过大家可能比较熟悉这个版本的代号：Panther。

18.1 AirPort Extreme 网卡

Apple 所提供的系统整合程度相当高，因为软硬件在设计上完全由自家包办。和纷乱的 IBM 相容系统不同，Apple 必须完全为软硬件负责，而他们的确办到了。几分钟内，使用者即可安装好软硬件并且连上现有网络。如果在系统安装过程中将 AirPort 网卡插入，上述步骤就会被整合到初次配置设置程序中。

18.1.1 软件安装

OS 9.1 之后的过程系统均内建 Airport 驱动程序，因此无须下载与安装驱动程序。系统第一次使用之前，如果已经安装 AirPort 网卡，首次开机配置设置工具就会让使用者设置 Airport 接口卡，选择所要使用的网络名称以及 TCP/IP 相关设置。如果使用 DHCP，整个设置程序只需几个画面而已。

已经启用的系统若要加装 Airport 网卡，可以稍后使用 Airport Setup Assistant 程序【注】加以设置。插入卡片后，执行 Setup Assistant 程序。程序开始执行后，可看到如图 18-1 所示的对话框。

选择设置 Airport 网卡配置，然后点选[Continue]钮。下个步骤是选择所要加入的网络，如图 18-2 所示。收讯范围内所有网络均显示于跳出式选单（POP-upmenu）：图 18-2 显示使用者选取了[secure.utah.edu]网络。



图 18-1: Airport Setup Assistant 的启动画面

【注】网卡可以通过 System Preferences 应用程序加以设置。本章之所以将 Setup Assistant 的讨论放在 System Preferences 之前，主要是为了在监拉与变更配置设置各方面力求内容的完整。不过，各位没有明白不能直接以 System Preferences 应用程序进行配置设置。



图 18-2: 选取 AirPort 网卡所要加入的网络

选好网络后，开始进行第三个步骤：键入网络密码，这用于以 WEP 或 WPA 保护的网络。802.1X 配置必须在 Internet Connect 中设置，本章稍后将会述及。

进行网络连接时，有好几种不同的安全性设置可供选择，如图 18-3 的对话框所示。下拉式选单（drop-down box）中有几种安全性选项可供选择：WPA Personal(WPA-PSK)。WPA Enterprise (WPA 搭配 RADIUS 身份认证) 以及 WEP。为了让使用者更容易上手，Apple 允许网管人员以任意长度的密码设置 WEP 密钥。之后，这些 ASCII 文字所构成的密码会经过杂凑函数的处理，成为长度适中的 WEP 密钥。WEP 密钥也可以是十六进制的数字，键入时只要在字符串前加上「\$」即可，例如 \$EB102393BF。十六进制密钥的长度若非 10 位数（40 个位元），就是 26 位数（104 个位元）。只要在所键入的密钥前后加上双引号，就可以强迫系统以 ASCII 解释之。

[注]

进一步的信息，请参阅 Apple 的知识库（Knowledge Base，位于 <http://kbbase.info.apple.com>）中编号 106250 的文章。

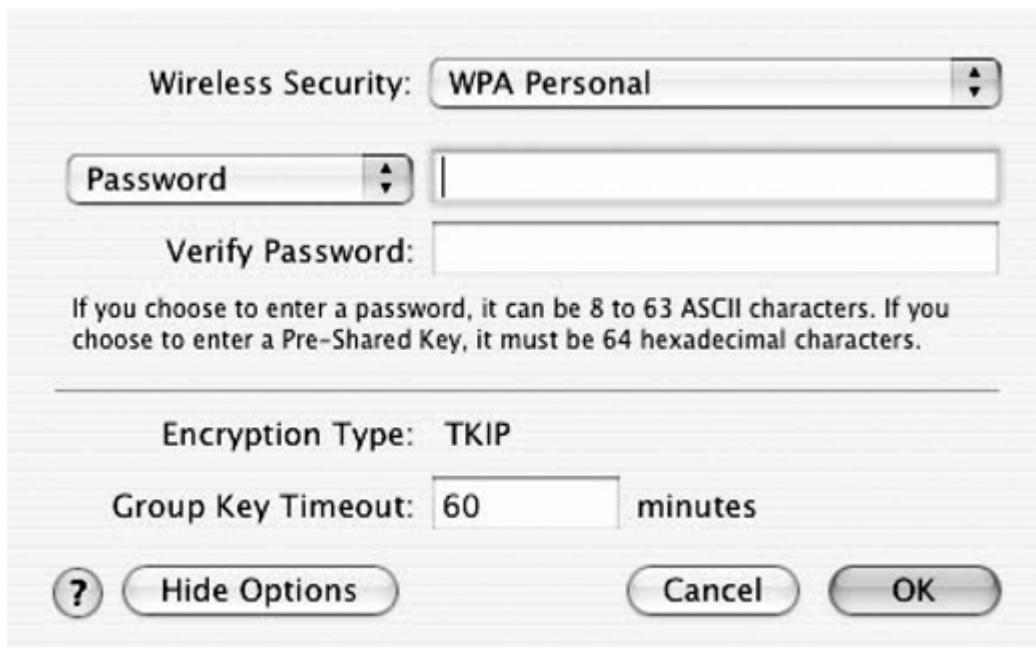


图 18-3：AirPort 网络密码输入画面

18.1.2 设置与监视 AirPort 界面

有时候，或许需要变更 AirPort 的配置、在不同的 802.11 网络 (ESS) 间移动，或更改 WEP 密钥与 IP 的设置值。安装好卡片后，可通过 OS X 所提供的工具变更配置。Apple 的设置程序并不允许使用者更动比较复杂的 802.11 参数。举例而言，加入某个网络所需要的一切信息均广播于 Beacon 帧。Apple 认为，大部分情况下，只要告诉使用者网络名称，要求他们选择安全性设置就够了。

18.1.2.1 以 AirPort 状态图示进行基本配置设置

配置设置完毕之后，AirPort 状态图示（status icon）就会出现在萤幕右上角，位于喇叭音量。电池与时钟图示旁—如果之前没有关闭这些图示的话 AirPort 图示同时会显示信号强度・图

18-4 中，图示上会出现一些实心波前（solid waveform）。如果离基站远一点，信号就会减弱，线条也会减少。点选状态图示后，会出现一个下拉式命令选单，可以开启或关闭 AirPort 的电源，选取或新建网络，以及执行 InternetConnect 应用程序来监视无线界面。可以随意开关网卡对使用者而言相当方便。当使用者离开网络的覆盖范围，或不需要使用网络时，即可关闭网卡电源以节省电力。



图 18-4: Airport 状态图示

图 18-4 中，收讯范围内有两个网络：[Little Green Men]以及[Luminiferous Ether]。[Little Green Men]旁边的打勾符号，代表使用者目前正与之连接。使用者可以随意在两个网络间进行切换。如果尚有其他网络，可以选取[Other...]选项，然后键入网络名称。

要新建一个 IBSS 网络，可以通过 Create Network 选项，选择如图 18-5 所示的基本无线参数。该电脑准备设立一个名为 Very Independent BSS 的 IBSS 网络，使用预设的 11 频道 b 在北美或欧洲，这 11 个频道可以任意使用。每部加入 IBSS 的电脑必须使用相同频道，IBSS 网络只能使用 WEP 加密。



图 18-5: IBSS 参数的设置

设置完成后，系统就会在下拉式选单中新增一个名为「Computer to Computer Networks」的项目，如图 18-6 所示。Airport 状态图示也改变为 pie wedge 形状，表示目前所使用的是 IBSS，而非 infrastructure 网络。



图 18-6：当连接至 IBSS 时，AirPort 所显示的状态图示

18.1.2.2 以 System Preferences 应用程序进行设置

如果想在不同的 ESS 之间移动，你可以为每个网络建立一个[地点名称](location)，并以此设置相应的[ESS/密码]组合，此后只要移动至不同的地点，就可以从选单中点选使用，就算目前不在所要加入的网络范围内，也可以预先设置好[ESS/密码]组合。

System Preference（系统参数设置）应用程序允许使用者设置许多系统属性，包括网络方面的属性。图 18-7 显示了 System Preference 应用程序的 Network Preferences（网络参数设置）面板。Show 跳出式清单(pop-up list)可以设置成系统中任何一个网络界面。此处当然是设置成 AirPort，如图所示。预设的参数设置标签为 TCP/IP（图 18-7），可以手动设置接口卡，也可以通过 DHCP 或 BootP 自动设置。设置成 DHCP 时，就会显示出所取得的位址，如图所示。虽然我网络上的 DHCP 服务器会提供 DNS 服务器的 IP 位址，但此处并未显示出来。（不过，一般 Unix 系统会将之置于/etc/resolv.conf 档中）。

其他值得注意的参数设置标签是 AirPort（图 18-8），用来设置预设要加入的网络。大部分情况下，应该将它设置为 Automatic，这让工作站得以在已设置好的网络中进行搜寻。如有必要，Automatic 选项可以参考 Internet Connect 中已设置好的安全性配置。

18.1.2.3 监控无线界面

无线界面的使用状态，可通过 Internet Connect 应用程序加以监控。InternetConnect 应用程序可从 Application 文档夹，或由 AirPort 状态图示来执行。它可以用来显示距离最近之基站的信号强度，以及切换所要连接的网络。如果切换到别的网络，它将会参照任何必要的 802.1X 配置设置，以便进行身份认证，如图 18-9 所示。



图 18-7: Network Preferences 面版的 TCP/IP preferences 标签

18.2 在 AirPort 上使用 802.1X

在 Panther 版本系统上, 802.1X 系统通过 Internet Connect 应用程序来设置。Internet Connect 可以从 AirPort 状态图示的下拉式菜单（或是直接从硬盘）来执行。要查看 802.1X 的配置设置，可以点选标示为 802.1X 的锁头图示。如果画面中并未出现该图示，请由 File 选单点选 New 802.1X Configuration，或直接按 Command-Shift-X 组合键。一旦启用过 802.1X，该图示就会永远出现在顶端的选单画面中（图 18-10）。



图 18-8: Network Preferences 面版的 Airport Preferences 标签



图 18-9: Internet Connect 监控程序

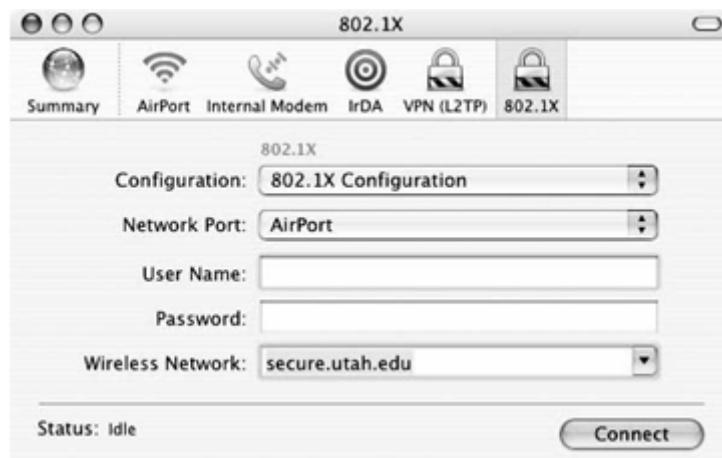


图 18-10: Internet Connect 中的 802.1X 配置设置

要查看完整的配置设置，可以选择 Configuration 下拉式选单，然后点选 EditConfiguration 一这样就会显示配置设置主画面（图 18-11）。在此，最简单的做法就是直接编辑既有的配置，由此进入配置设置画面。键入 **username** 与 **password** 之后，就可以点选想要使用的身份认证协议。此画面允许使用者选择要在哪个网络界面上使用 802AX。大多数情况下，这项设置是针对 Airport 网卡的，不过 802.1X 在有线网络上也逐渐得到广泛应用。**username** 与 **password** 的设置十分直接，**Wireless Network** 选项亦然。预设上，**Wireless Network** 下拉式选单会列出 Airport 检测到的所有加密网络，不过使用者也可以自行键入 SSID。

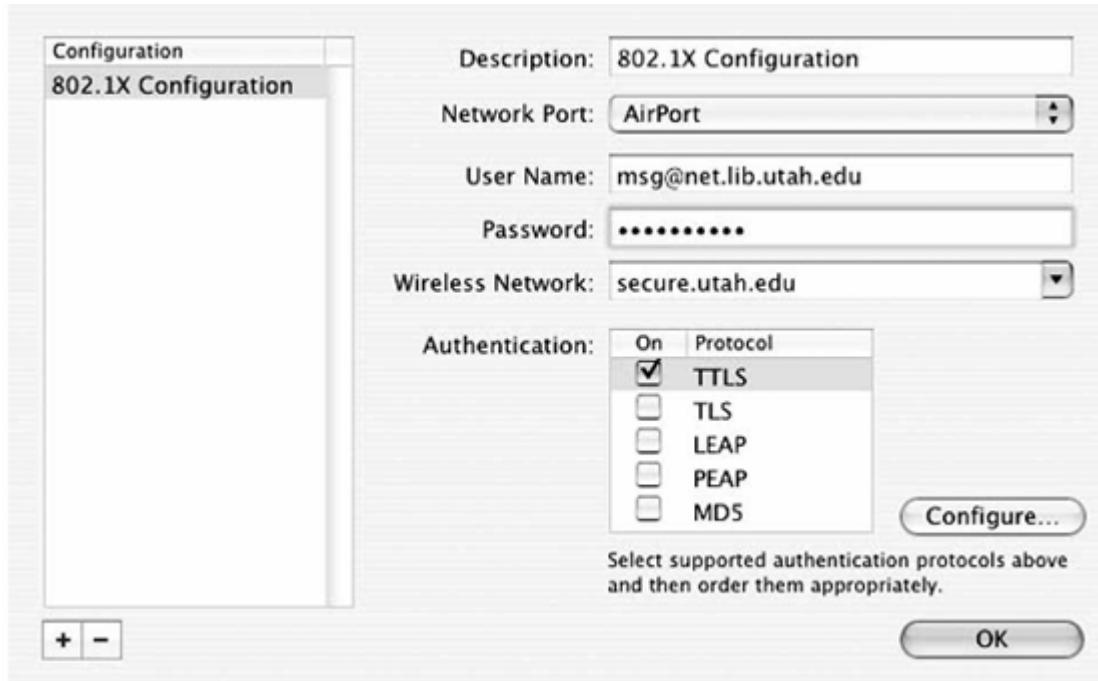


图 18-11: 802.1X 配置设置画面

键入帐号密码后，接下来可能需要设置身份认证方式。每一种认证方式各有不同的纠态设置画面，稍后会加以说明。

回到 Internet Connect 主画面后，就可以点选 Connect 按钮进行网络连接以及必要的 802.1X 身份认证程序。画面下方的状态列（status bar）将会经历下列阶段：

Idle (闲置)

AirPort 尚未连接到任何网络。

Connecting (连接中)

AirPort 正与所选择的 SSID 进行连接中。

Authenticating (身份认证中)

AirPort 与 AP 或交换器正在交换 EAPOL 帧，尝试验证使用者身份。

Connected via (EAP method) (已 (通过 EAP 方法) 连接)

如果通过身份认证，状态列将会显示系统已经连接，并且显示所使用的 EAP 方法，以及通过身份认证的时间。

18.2.1 EAP 方法的配置设置

每一种 EAP 方法均有不同的配置设置方式。除非必要，否则 Mac supplicant 通常会将比较复杂的设置隐藏起来。

18.2.1.1 TTLS 配置设置

TTLS 有两种可能的配置设置选项，如图 18-12 所示。第一种属于内部的身份认证，此为必要 (mandatory) 选项。大多数情况下应该会将这个选项设为 PAP，不过也可以使用 CHAP、MS-CHAP 或者 MS-CHAP-V2。和大多数 supplicant (认证申请者) 一样，Mac supplicant 也可以通过设置一个匿名 (anonymous) 的外部身份 (outeridentity) 来隐藏使用者身份。

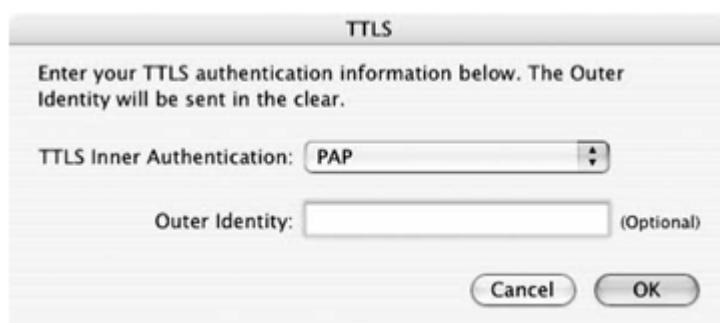


图 18-12: TTLS 配置设置画面

18.2.1.2 PEAP 配置设置

Mac supplicant 只支持以 EAP-MSCHAP-V 2 做为内部身份认证方式。如此即可与以 MD4 杂凑或明文格式储存的使用者帐号互通。这种方式的主要用处，是为了支持储存于 Windows 网络的使用者帐号。在图 18-1 予的配置设置画面中，只有一个用来设置外部身份的选项，以便隐藏使用者身份。

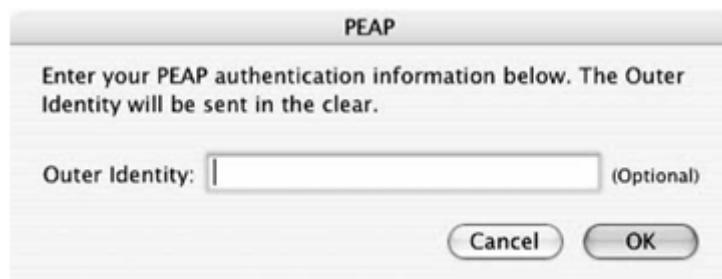


图 18-13: PEAP 配置设置画面

18.2.2 密钥链

在 Mac OS 中，密码与凭证系储存于密钥链（keychain）之上，用来集中保管安全相关信息。登入之后，使用者有权执行的应用程序即可使用网络身份认证所需要的凭证与识别信息。简单的密钥链如图 18-14 所示，其中包含 RADIUS 服务器凭证（certificate）。签署该凭证的 CA，以及某个网络的 802AX 配置设置。密钥链提供了访问控制以保护配置设置。

18.2.2.1 将凭证汇入密钥链

第一次连接至受 802.1X 保护的网络时，任何未被信任的凭证均会导致身份认证失败。不过，**supplicant** 会向使用者出示凭证内容，而非迳自判定身份认证失败，如图 18-1 所示。检视过凭证后，使用者即可决定是否信任该凭证。比较可能出现的情况是，信息科技部门将系统交付一般用户之前，会在无线网络上先行测试帐号密码，同时为他们汇入相关的凭证。

18.2.3 障碍排除

如果 802AX 身份认证失败，所出现的错误讯息（图 18-16）并不能提供多少线索。错误码无法提供详细的诊断信息，告知失败的真正原因。

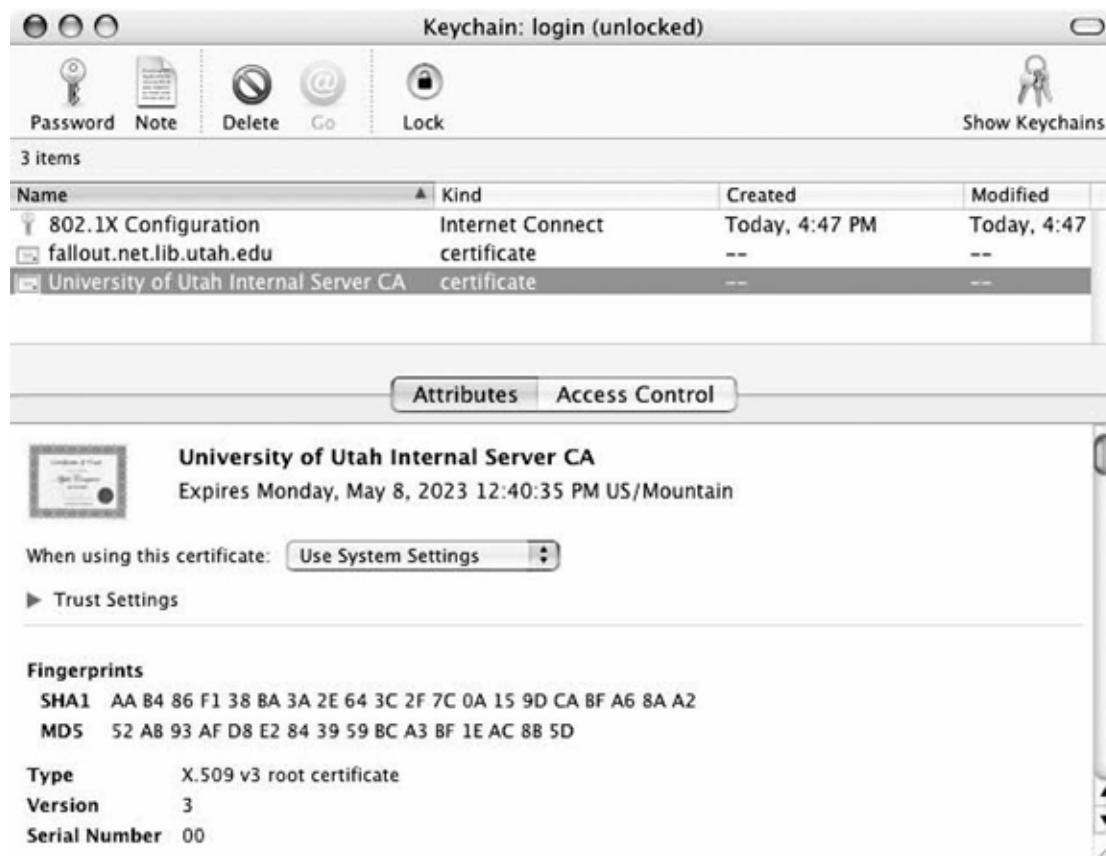


图 18-14: 密钥链检视器

幸好，`supplicant`可以提供额外的排错纪录。如果`/var/log/eapolclient`目录不存在，请先手动建立。如果此目录已经存在，而且 Internet Connect 执行时已经设置`NSDebugEnabled`环境变数，使用者所发送的 EAPOL 帧就会被记录在`/var/log/eapolclient/uid(number)-(network interface).log`文档中。举例而言，如果 UID 501 试图在 AirPort（通常为 en1）使用 802.1X，该纪录档即为`uid501-en1.log`。Internet Connect 必须从命令列执行，这样才能自终端机中取得环境变数。

```
Mac: ~$ sudo mkdir /var / log/eapolclient
```

```
Mac: ~$ NSDebugEnabled=YES; export NSDebugEnabled
```

```
Mac: ~$ /Applications / Internet \ Connect. app/Contents / MacOS / Internet \ Connect
```

对于所收送的每个帧，排错纪录档会同时以 ASCII 与十六进制（hexadecimal）两种格式加以记录。至于经过加密的 EAP 方法，则不会列印出相应的解密帧。举例而言，802.1X 身份认证成功后，会收到两个如下的 EAPOL-Key 帧：

Authentication failed because the server certificate is not trusted. Select and verify the certificates below. If you accept these certificates, they will be added to your keychain and trusted.

If you do not understand or recognize the contents of the certificate, and are unable to verify the server's identity, do not click Accept.

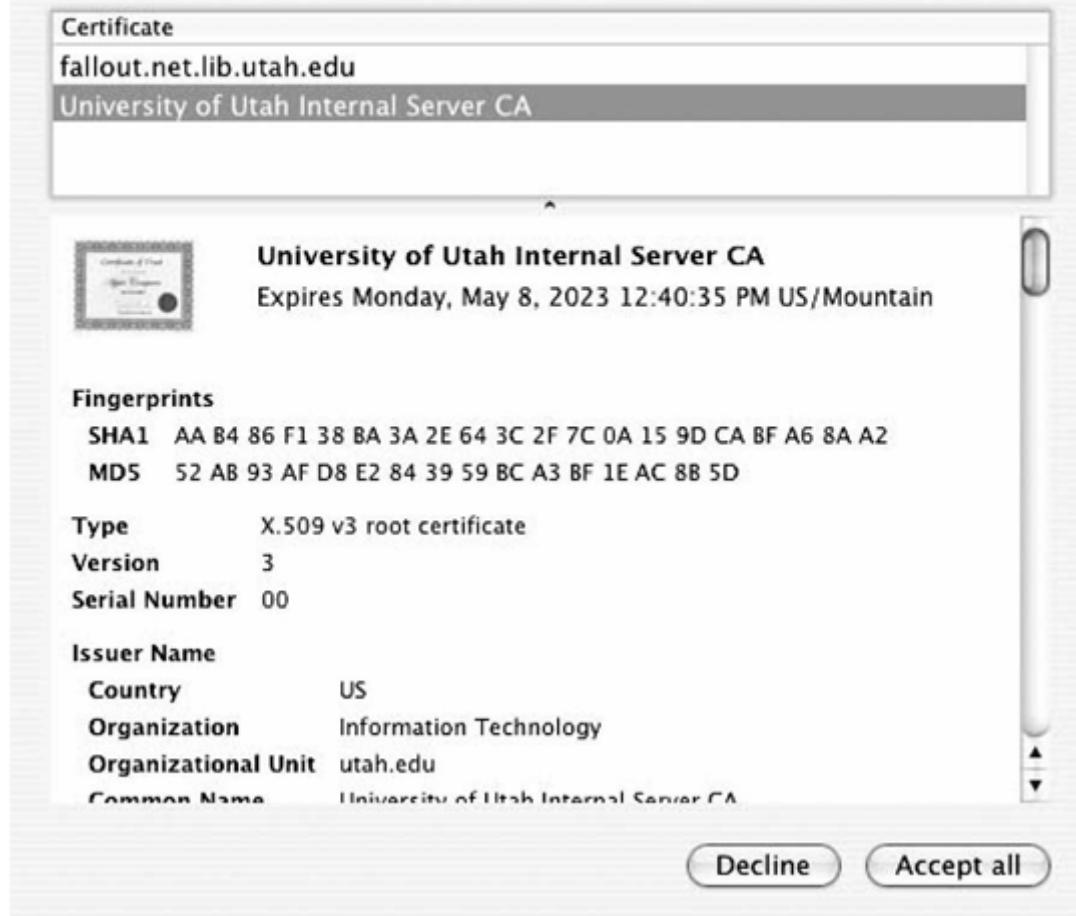


图 18-15: 将凭证汇入密钥链



图 18-16: 身份认证失败对话框

2005/02/15 17:00:42.903841 Receive Packet Size: 75

```
Ether packet: dest 0:30:65:2:e7:36 source 0:b:e:a:70:2 type 0x888e
EAPOL: proto version 0x1 type Key (3) length 57
Signature: 6c 08 b3 97 b1 74 f2 ec 0e 2c 1f 66 ff 40 78 42 is valid
EAPOL Key Descriptor: type RC4 (1) length 13 Broadcast index 2
replay_counter: 42 11 48 e2 00 00 00 18
key_IV: ca 7e d9 ff d4 47 80 ba 9e eb 33 c8 82 17 02 7c
key_signature: 6c 08 b3 97 b1 74 f2 ec 0e 2c 1f 66 ff 40 78 42
key: fc 7a 7c 67 f6 f6 f5 7d a5 94 cb 49 1a
```

2005/02/15 17:00:42.960436 Receive Packet Size: 64

```
Ether packet: dest 0:30:65:2:e7:36 source 0:b:e:a:70:2 type 0x888e
EAPOL: proto version 0x1 type Key (3) length 44
Signature: ce b3 45 05 47 72 5a 98 7c 64 0c d8 52 0d 8f 78 is valid
EAPOL Key Descriptor: type RC4 (1) length 13 Unicast index 0
replay_counter: 42 11 48 e2 00 00 00 19
key_IV: 45 e5 2a ad 1c 9c ea 8f 3c 58 a4 c4 6a e0 fa 82
key_signature: ce b3 45 05 47 72 5a 98 7c 64 0c d8 52 0d 8f 78
EAPOL: 2 bytes follow body:
0000 00 00
```

在 Mac 上同时使用 WEP 与 WPA

本书即将付印之际、Mac **supplicant** 当中依然存在一个攸关互通性的瑕疵，无法同时使用两种加响方式。同时会用到动态 WEP 与 TKIP (WPA) 的情况十分普遍。支持 TKIP 的工作站通常会以之传送单点传播 (unicast) 数据，而以动态 WEP 来加于广播 (broadcast) 数据。只支持动态 WEP 的工作站则同时以之加密单点传播与广播数据。

在混用 WEP/TKIP 的环境中，Macintosh 便无法连接至网络。**supplicant** 可以在连接的过程中得知网络同时支持 WEP 不过在进行密钥磋商 (key handshake) 与 TKIP，并且接受相关的安全参数时，**supplicant** 坚持只能使用 TKIP。既然连接程序与配钥程序所使用的安全参数有所差异，依照标准规定，彼地台应该认足密钥磋商失败，以及将工作站踢出网络。

欲解决此问题，你可以降低网络的安全等级，只使用动态 WEP；或是设置两组无线网络（一组使用 WEP，另一组使用 TKIP），让 Mac 使用 TKIP 网络；或是强迫使用动态 WEP 的所有设备退出网络完全使用 TKIP。

第19 章 802.11 与 Linux

写作本书第一版时，802.11 才刚走向 Linux。当时能够完整支持无线网卡的开放原始码驱动程序很少，也跟不上 Linux 核心（kernel）的更新脚步，因此在选购时必须特别小心。如今支持 Linux 已经成为主流，许多厂商开始主动赞助驱动程序开护专案，至少也会提供协助给那些针对自家硬件所做的努力。Broadcom 算是少见的例外。

大多数 802.11 设备是由 PCMCIA 系统提供支持。和 Windows 驱动程序一样，在 Linux 安装无线网卡就会产生 Ethernet 界面。有些 Linux 驱动程序会通过核心提供 Ethernet 界面。大多数驱动程序甚至会以 eth 为字首来替这些界面命名。应用程序将会通过 Ethernet 界面在链路层收发数据，并由驱动程序负责处理 Ethernet 与 802.11 之间的转换作业。【注 1】其中有许多事情和大家对 Ethernet 界面的期待相当 ARP 的作业方式相同，IP 的配置设置也可以利用作业系统发行套件所提供的相同工具程序。Ifconfig 甚至可以用来监控界面状态以及检视数据的收发。

19.1 Linux 所支持的 CIA

起初，无线网卡大多是 PC Card 规格的外接卡（add-on card）。【注 2】PC Card 通过在 8 MHz 时脉操作的 16 位元控制器与系统汇流排介接。虽然效能受限于和 16 位元 ISA 相当的汇流排，不过 PC Card 已经足够应付相对较慢的 802.11b 无线局域网络。至于效能较高的 802.11a 与 802.11g 网卡，就必须用到 CardBus 界面（操作在 33MHz 时脉的 32 位元汇流排）。CardBus 提供大幅提升的效能，可以满足频宽需求较高的网络界面。外观上，CardBus 和 PC Card 网卡看起来没什么两样，而且使用同样的插槽。可想而知，两者均可使用 Linux PCMCIA 工具程序进行配置设置与管理。

附带天线的外接式网卡通常会有部分凸出膝上型电脑的机壳，外观上并不讨喜。因此膝上型电脑厂商另外替“内建”（built-in）的无线设备选择了一种截然不同的造型，称为 Mini-PCI。Mini-PCI 是 PCI 界面的缩小版，长度只有几英寸。Mini-PCI 界面卡可以内建各种不同功能，不过目前 Mini-PCI 插槽最常见的用途，就是用来替膝上型电脑添加无线网络功能。大多数 Mini-PCI 无线网卡是由 PCI-to-Cardbus 桥接器与 CardBus wireless LAN 界面所组成。因此可以通过 Linux PCMCIA 系统进行配置设置与管理。

19.1.1 PCMCIA Card Services 概观

Card Services（卡片服务）的由来，主要是为了简化系统配置。也就是说，主机系统为 PC Card 维护一组资源，必要时才加以配置，而不是为个别设备提供专属的系统资源。图 19-1 显示了每张卡片在 Linux 作业系统上的配置设置程序。

卡片插入时，cardmgr 系统程序负责指挥整个设备的配置设置过程，如图 19-1 所示。整个过程中，会将系统资源、核心元件以及核心驱动程序模组通过储存于/etc pcmcia 的配置档兜在一起。大致而言，主机会采取下列步骤：

1. 某张卡片被插入一个空的 PC Card 插槽，cardmgr 会被被告知此一事件。除了一些硬件上的作业（例如，为该插槽提供电源），cardmgr 会查询该卡片的卡片信息结构（card information structure，简称 CIS），判断所插入的卡片种类以及所需要的资源。关于 CIS 的进一步数据，请参阅附文〈卡片信息结构〉。

2. `cardmgr` 接下来会尝试辨识该张卡片，以及载入适当的核心模组做为支持。位于 `/etc/pcmcia/config` 的 PCMCIA 卡片数据库主要用来把 CIS 数据库对映到驱动程序。驱动程序也可以通过硬件识别表（hardware identification list）自动载入。硬件识别表属于模组的一部分，存放在模组对映表中（`/lib/modules/(kernel version)/module.*map`）。辨识卡片的主要目的是为了将卡片归类。就设置网卡的目的而言，重点在于网络类别（network class）后续还需要一些额外设置作业。卡片的种类会在步骤 1 藉由 CIS 加以辨识，而网络类别的设置则是在主要系统配置档中加以设置。至此，`cardmgr` 会发出一声哔响。如果辨识成功，所发出的哔声音阶较高，否则所发出的哔声音阶较低。

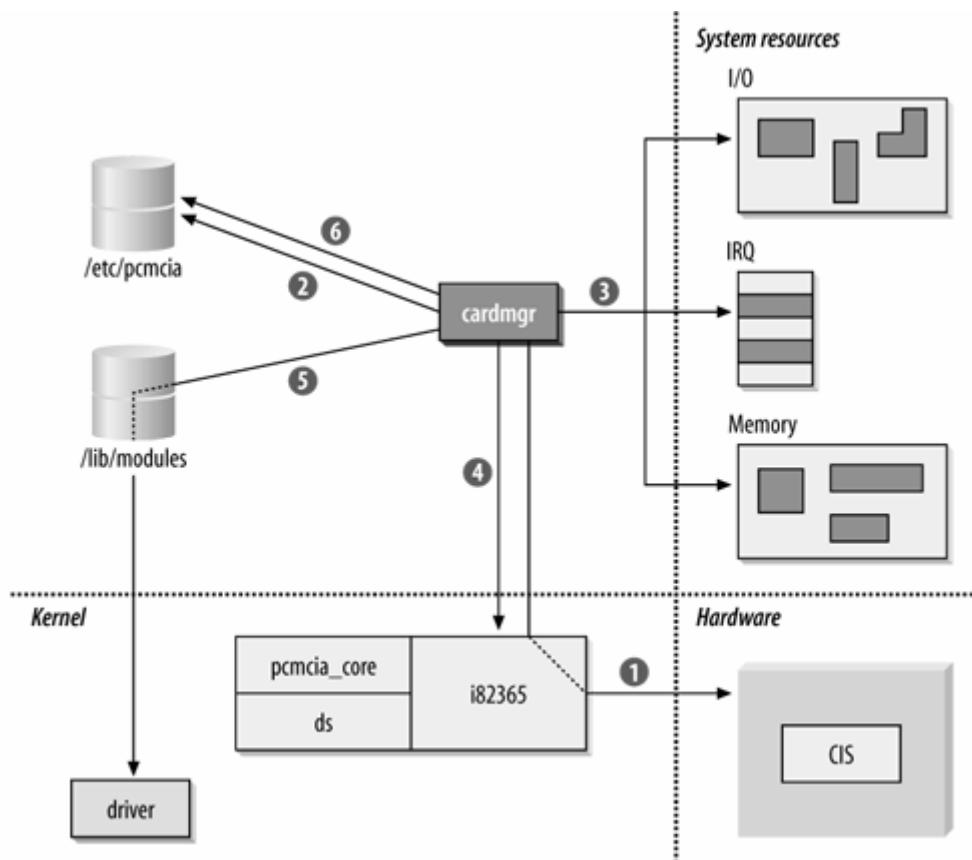


图 19-1: Linux PCMCIA 系统配置

3. `Cardmgr` 判断有哪些资源可以配置给卡片，在主要配置档中会保留系统资源区块给 PCMCIA 卡使用，而且 `cardmgr` 会将所需要的资源发放给卡片。`I/O` 埸编号以及记忆体大小是由 CIS 取得。

4. `Cardmgr` 所配置的资源会在 PCMCIA 控制芯片加以设置，如图 19-1 所示，该控制芯片会与设备驱动程序互动。Intel 的 i82365SL PCMCIA 控制器是目前市面上最常见的芯片，这就是为什么此核心模组会标示为 i82365。新的 PCMCIA 系统采用的是 yenta-socket（而非特定芯片组）的驱动程序。PCMCIA 控制芯片负责将卡片所需要的资源对映到可用的系统资源。卡片或许会要求中断，但实际指派的中断与此无关。在作业过程中，卡片仅会要求 PCMCIA 控制芯片发出中断信号，而控制芯片的回应则是找出指派给插槽的中断，以及触发正确的 中断线路。

5. 在步骤 2 所搜寻来的配置信息中，有一部分是使用刚插入卡片时应该载入之设备驱动程序的名称。PCMCIA 卡片的驱动程序被实作成了核心模组。插入卡片的过程中，驱动程序会在步骤 4 被告知所分配到的资源。只要正确设置模组的依存关系，即可使用模组堆叠载入多个模组。

6. 进一步的使用者空间配置，系根据设备类别（device class）加以设置。举例而言，网卡可额外以/etc/pcmcia/network 命令稿（script）加以设置，只要编辑/etc/pcmcia/network.opts 即可。如果设置成功，就会发出一声高音哔响，否则发出一声低音哔响。此外，Linux 的热插拔系统（hotplug system）也可能会进行一些额外的配置设置。

19.1.1.1 Linux 所使用的界面名称

驱动程序产生网络界面之后，就会赋予它一个由字首(prefix)与数字(number)所组成的名称。有些驱动程序会以 ethX 做为新增网络界面的命名格式，其中 X 代表卡片的顺序。目前大多数膝上型电脑均已内建 Ethernet 界面，开机时即启用为 eth0，因此无线界面通常从 eth1 开始命名。旧版的 WaveLAN 驱动程序是以 wlan 为字首，不过目前的版本已经改用 eth。采用 Atheros 芯片组的网卡则使用 ath 字首。

19.1.1.2 以热插拔系统进行自动配置设置

Linux 采用“hotplug configuration”专案的工作成果来进行自动配置设置，该专案的网址为 <http://linux-hotplug.sourceforge.net/>。插入设备时，热插拔系统在为界面进行配置设置之前，会先呼叫必要的 PCI 配置命令。如果有不少网络界面需要设置，或是希望进行自订的配置设置作业，就可以使用 Hotplug 命令稿完成系统的自动配置设置。有些实作较新标准的无线设备在产品推出后，开发工作仍然持续进行。更换新韧体后，卡片就可以支持新的协议，或者修正已发行版本的错误。设置上可以要求 Hotplug 在插入特定网卡时自动更新韧体。

19.1.2 PCMCIA Card Services 的安装

2.4 版以后，PCMCIA 功能被整合到了核心，各位所使用的发行套件（distribution）或许早已安装这项功能。升级核心的 PCMCIA 功能并非必要。虽然不能没有网卡驱动程序，但是 PCMCIA 功能也要够新，方能支持各位手上的无线界面卡。（较旧的发行套件可以通过发行维护单位（distribution maintainer）的软件套件（package）来更新 PCMCIA 软件，或者使用 <http://pcmcia-cs.sourceforge.net/> 的原始码自行编译。）

卡片信息结构

为了能够自动进行配置设置，每片 PC Card 都内含了一段数据，让卡片得以向主机系统交待本身所具备的功能。这段数据区块称为卡片信息结构（card information structure，简称 CIS），其所具备的格式为 link-list（链结串列）。CIS 的基本建构单位称为 tuple，因为它们具有三项组成元件：用以表示 tuple 类型的类型码、长度栏位，以及一系列数据位元组。tuple 格式可以十分简单，也可能相当复杂，这就是为什么本书并未试图进一步为之分类的原因。勇于求知的读者可以向 PCMCIA 协会订购一份规格书，以及利用 Linux 平台上的 dump_cis 工具读出卡片的 CIS。

在自动配置设置程序中，CIS 会向主机作业系统描述本身所具备的功能。举例而言，

网络界面卡会表明身份，其中的 CIS 可以让 Card Services（卡片服务）较体配置适当的资源，例如 I/O 埠以及中断要求线路（IRQ）。在 Linux 作业系统中，系统管理员可以使用配置档来匹配 CIS 数据与驱动程序。

大多数的配置设置信息不难从环境自动检测得知。根据所使用的岭行套件以及安装选项，或许必须在系统配置档中设置 PCIC 变数，告诉 PCMCIA 软件目前 PCMCIA 插槽使用何种控制器。核心的 PCMCIA 软件会将这个变数值设置为 yenta-socket。使用独立 PCMCIA 模组的系统，如果将此变数设为 tcic，代表使用 Databook TCIC-2 芯片组，如果设为 i82365，代表使用 Intel i82365SL 芯片组。Slackware 提供了一个 probe 选项，可以自动检测并载入相关模组。

19.1.3 监控网卡

用来控制 PCMCIA 子系统的主要工具是 cardctl 命令。它具有一些副命令(subcommand)可用来检视信息或配置设置状态。每个引数(argument)也可以指定插槽编号。有些膝上型电脑配备两个 PCMCIA 插槽，编号分别是 0 与 1。为了携带方便，有些笔记型电脑只配备一个插槽，因此只有插槽 0。

除了以硬件方式退出卡片，也可以用 cardctl 来移除驱动程序，只要送出“卡片已经移除”(card is removed) 的告知讯息即可。移除相关驱动程序以及关闭插槽电源之后，可以传送一个“插入卡片”的软件告知讯息重新启动网卡。通过软件进行控制，不需要实际插拔即可重新启动网卡。

```
[root@bloodhound] # cardctl eject 0
[root@bloodhound] # cardctl insert 0
```

选择使用何种驱动程序主要是根据 CIS 数据。要检视卡片的 CIS 内容，可以插入卡片等它启动，然后使用 info 或 ident 副命令来检视识别信息。以下是 Proxim 8480 Gold card 的数据。它和其他 802.11a 网卡一样，所采用的是 Atheros 芯片组。你甚至可以看到这张卡片采用了 Atheros 的公版设计：

```
root@bloodhound: ~# cardctl info 0
PRODID_1="Atheros Communications, Inc. "
PRODID_2="AR5001-0000-0000"
PRODID_3="Wireless LAN Reference Card"
PRODID_4="00"
MANFID=0271, 0012
FUNCID=6
root@bloodhound: ~# cardctl ident 0
product info: "Atheros Communications, Inc. ", "AR5001-0000-0000",
"Wireless LAN Reference Card", "00"
manfid: 0x0271, 0x0012
function: 6 (network)
```

除了以 cardctl 检视 CIS 信息，也可以使用 dump_cis 命令列出完整的 CIS 结构。除了卡片识别信息，CIS 中也包含支持速率的相关信息。以 Proxim 8480 为例，虽然它也相容于 802.11b，不过却只显示出了所支持的 802.11a 速度：

```
root@bloodhound: ~# dump_cis
Socket 0:
manfid 0x0271, 0x0012
config_cb base 0x0000 last_index 0x01
cftable_entry_cb 0x01 [default]
[master] [parity] [serr] [fast back]
Vcc Vnom 3300mV Istatic 25mA Iavg 450mA Ipeak 500mA
IRQ mask 0xffff [level]
mem_base 1
BAR 1 size 64kb [mem]
Vers_1 7.1, "Atheros Communications, Inc. ", "AR5001-0000-0000",
"Wireless LAN Reference Card", "00"
funcid network_adapter [post]
lan_speed 6 mb/sec
lan_speed 9 mb/sec
lan_speed 12 mb/sec
lan_speed 18 mb/sec
lan_speed 24 mb/sec
lan speed 36 mb/sec
lan-speed 48 mb/sec
lan_speed 54 mb/sec
lan_speed 72 mb/sec
lan_media 5.4_GHz
lan_node_id 20 00 4d a6 d4 0a
lan_connector Closed connector standard
Socket 1:
no CIS present
```

将卡片插入系统后，就可以使用 **status** 副命令进行检视。**Config** 副命令也会显示系统所赋予的系统中断。以我为例，我的膝上型电脑使用 PCI 转 Cardbus 的桥接器，因此卡片沿用 PCI 汇流排的 IRQ。

```
root@bloodhound: ~# cardctl status 0
3.3V CardBus card
function 0; [ready]
root@bloodhound: ~# cardctl config 0
Vcc 3.3V Vpp1 3.3V Vpp2 3.3V
interface type is "cardbus"
irq 11 [exclusive] [level]
function 0:
```

19.1.3.1 没有用的灯号显示

有些驱动程序同时支持好几种硬件，而且各家厂商对于卡片灯号的数量与用途，定义上并不相同。通常会有一个灯号表示卡片已经启动，第二个灯号闪动时表示卡片正在进行传输。至于回应来自其他工作站的数据时，可闪可不闪。少数网卡会有第三个灯号显示连接状态。

Linux 驱动程序通常不会以厂商所定义的方式来控制网卡灯号，内建的网卡也许根本没有灯号显示。如果你的卡片灯号显示方式异常，请勿惊慌。请先检查与基站是否已经建立连接；若已连接，则卡片的运作即为正常，只不过灯号的显示方式不同。

19.1.4 排除资源的冲突

PCIMCIA 卡片厂商所宣称的神话之一是，在 IBM PC 相容的硬件中，使用者再也不必负责维护低价的硬件设置。就某些方面而言，这项神话有点过度吹嘘，因为使用者还是必须负责维护 PCMCIA Card Services 所使用的资源，所以使用者仍然必须熟悉硬件配置。Card Services 为使用者管理三种资源：IRQ 线路、I/O 埠，以及 DMA（直接记忆体访问）通道。不过，网卡并不需要用到 DMA 通道，因此本节将略过不谈。

19.1.4.1 IRQ

必须周期性用到 CPU 的设备就会用到 IRQ。界面卡之所以会使用 IRQ，是因为一旦缓冲区已满，必须通知系统 CPU 清空缓冲区。PC 架构的限制之一是，只有 15 个 IRQ 可用，而且其中已经有些被标准硬件所占用。表 19-1 显示了 IRQ 的一般用途，这或许可以帮助读者判断有哪些 IRQ 可供 PCMCIA 卡使用。停用额外的元件可以释出 IRQ。表 19-1 同时显示了 PC 硬件上一般的 IRQ 设置。依经验法则，在大部分机器上，IRQ 3、5 与 10 通常是空闲可用的。

表 19-1：常见的 IRQ 设置

IRQ 编号	一般用途	使用目的
0	系统计时器	每秒钟振荡 18 次，以保持粗略的计时。
1	键盘	让作业系统得以监测使用者是否按下任何键。
2	串联 (Cascade)	使用两颗中断控制芯片；第二颗控制芯片主要负责控制 IRQ 8 到 15，并与第一颗控制芯片的 IRQ 2 相串联。
3	第二 / 第四序列埠 (serial port)	第二与第四序列埠(在 Windows 中为 COM2 与 COM4)均使用 IRQ 3。如果只用到一个序列埠，那么 IRQ 3 即可供其他扩充设备使用。
4	第一/第三序列埠	第一与第三序列埠(在 Windows 中为 COM1 与 COM3)均使用 IRQ 4。通常，提供 IRQ 4 给其他扩充设备使用并不恰当，因为如此一来就无法使用终端机模拟软件了。
5	第二并列埠 (parallel port)	大部分系统均只配备一个并列埠，不过 IRQ 5 通常保留给音效卡使用。

IRQ 编号	一般用途	使用目的
6	软碟机控制器	所有系统均配备软碟机，对可携式电脑而言尤其重要。
7	第一并列埠	膝上型电脑通常可以将此并列埠停用，而不致产生任何问题，除非此并列埠用于列印。
8	RTC	RTC 负责维持较精确的计时。
9	显示卡（旧式系统）	旧式系统必须为显示卡保留一个 IRQ，通常使用 IRQ 9。如今大部分显示卡均使用 PCI 汇流排，因此不需要特别配置一个 IRQ。
10		通常用于扩充设备。
11	通常供 PCI 汇流排或 SCSI 控制器使用	扩充设备一般无法使用此 IRQ。
12	通常供 PS/2 滑鼠连接埠使用	一般无法移作他用。
13	FPU	浮点运算单元的 IRO，专供数值数据处理器使用，就算 CPU 本身已经内建数值数据处理器，如 Pentium 系列。
14	主要 IDE 通道	第一 IDE 通道主要供主系统硬碟机使用，因此在可携式系统中 IRQ 14 通常无法移作他用
15	次要 IDE 通道	可携式系统通常将 IRQ 15 供 CD-ROM 使用，因此无法移作他用。

19.1.4.2 I/O 埠

I/O 位址主要用于系统与周边设备之间的双向沟通。它们的设计通常不怎么样，何况有些设备的预设值会彼此重叠。每个 I/O 埠可以在周边设备与 CPU 之间传送一个位元组的数据。大部分的设备都需要具备一次传递多个位元组的能力，因此需要为设备指派一组 I/O 埠。最小的埠号也称为 I/O 基底位址 (base I/O address)。另外一个参数则用来描述 I/O 范围的大小。表 19-2 列出了一些常见的 I/O 埠设置值。1R 埠、USB 控制器・PCMCIA 控制器，以及其他需要用到主机版资源的设备，请参阅硬件厂商所提供的文件。

表 19-2：常见 I/O 埠

设备名称	I/O 范围 (大小)
传输埠	
第一并列埠	0x3bc-0x3bf (4)
第一序列埠	0x3f8-0x3ff (8)
第二序列埠	0x2f8-0x2ff (8)
磁碟机	
主要 IDE 通道	master: 0x1f0-0x1f7 (8) slave: 0x3f6-0x3f7 (2)
次要 IDE 通道	master: 0x170-0x177 (8) slave: 0x376 (1)
软碟机控制器	0x3f0-0x3f5 (6)

设备名称	I/O 范围 (大小)
输入设备	
键盘	0x060 (1) 0x064 (t)
多介质/游戏	
音效卡	0x220-0x22f (16) FM Synth: 0x388-0x38b (4) MIDI: 0x330-0x331 (2)
摇杆/游戏埠	0x200-0x207 (8)
系统设备	
中断控制器	0x020-0x021 (2) 0X0a0-0x0a1 (2)
DMA 控制器	DMA 通道 0-3: 0x000-0x00f (16) 分页暂存器: 0x080-0x08f (16) DMA 通道 4-7: 0x0c0-0x0df
CMOs/即时时钟	0x070-0x073 (4)
喇叭	0x061
数值数据处理器	0x0f0-0x0ff (16)

19.2 Linux 无线延伸功能与工具

802.11 界面一旦启动，它们的行为表现跟 Ethernet 界面没什么不同，不过它们比 Ethernet 界面多出一些配置设置选项，因为底层使用无线电技术。为了让所有驱动程序实作相同的功能以及使用相同的配置设置命令，而不必各自实作本身的配置设置工具与回报机制，因此有 Extension API 的开发。无线延伸功能（Wireless extensions）对需要通过此界面取得详细信息的应用程序开发人员也相当有帮助，因为如此一来，信息的取得与设备无关（device-independent）。例如，`xsupplicant` 将会利用无线延伸功能来设置界面上的 WEP 密钥，因此你就不必了解各家驱动程序设置密钥的方式。（本书付印时，WPA 产生密钥的系统呼叫尚未纳入官方发行的无线延伸功能。）

19.2.1 编译与安装

无线局域网络延伸功能系通过 `CONFIG_NET_RADIO` 核心配置选项来启用。启用了 `CONFIG_NET_RADIO` 功能的核心会搜集无线统计数据，并且提供大多数驱动程序所使用的额外数据结构。大多数 Linux 发行套件所包含的核心如果具备无线延伸功能，通常也会包含无线工具。如果需要最新的版本，可以从 http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux 下载，不过等候 Linux 发行套件将最新版本纳入核心原始码再予以重建可能会比较简单。

19.2.2 以无线工具和 iwconfig 来设置界面

管理具备无线延伸功能的驱动程序，主要是通过 `iwconfig` 这个命令列工具，它原本就是设计来做为“无线网络的 `ifconfig`”。使用 `ifconfig` 设置传统网络参数前，可以用它来设置无线电波界面参数。

不带任何参数时，`iwconfig` 会列出所有系统界面。非无线界面将会显示它们没有无线方面的数据，无线界面则会显示所有数据。并非所有驱动程序均会实作完整功能。例如，在使用旧式 Orinoco 网卡以及 Atheros CardBus 网卡的系统上执行 `iwconfig`，其结果可能会像这个样子：

```
[root@bloodhound] # iwconfig
lo no wireless extensions.

eth0 no wireless extensions.

eth1 IEEE 802.11-DS ESSID: "lib-is-slow" Nickname: "HERMES I"
    Mode:Managed Frequency: 2.457GHz Access Point: 00: E0: 03: 04: 18: 1c
    Bit Rate: 2Mb/s Tx-Power=15 dBm Sensitivity:1/3
    RTS thr: off Fragment thr: off
    Encryption key: off
    Power Management: off
    Link Quality: 46/92 Signal level: -51 dBm Noise level: -94 dBm
    Rx invalid nwid: 0 invalid crypt: 0 invalid misc: 0

ath0 IEEE 802.11 ESS ID: "lla-is-very-fast"
    Mode: Managed Frequency: 5.28GHz Access Point: 00: 0B: 0E: 00: F0: 43
    Bit Rate: 36Mb/s Tx-Power: off Sensitivity=0/3
    Retry: off RTS thr: off Fragment thr: off
    Encryption key: E452-94AC-09DB-2200-1256-6D7D-74 Security mode: open
    Power Management: off
    Link Quality: 31/94 Signal level: -64 dBm Noise level: -95 dBm
    Rx invalid nwid: 0 Rx invalid crypt: 0 Rx invalid frag: 0
    Tx excessive retries: 0 Invalid misc: 0 Missed beacon: 0
```

这两张网卡均会回报作业频率，以及与接收品质相关的统计数据。Atheros 网卡并未显示 Orinoco 网卡所列的“nickname”（昵称），因为 Atheros 驱动程序并未实作此项功能。（此昵称预设为“HERMES I”，这是以 Orinoco 网卡所使用的 Lucent 芯片组来命名的。）

无线延伸功能将会以两种方式来报告链路品质(`link quality`)信息。它会列出杂讯基准(`noise floor`)以及信号准位(`signal level`)，两者均由驱动程序所提供。这两种方式之间的差异在于讯噪比(`signal to noise ratio`)。上例中，`eth1` 的 SNR 为 43dB，`ath0` 的 SNR 则是 31 dB。驱动程序所提供的 `Link Quality` 统计数据会显示出 RSSI(相对信号强度)以及杂讯基准。上例中，`ath0` 的 RSSI 为 31 dB，杂讯基准为 -94 dBm。

19.2.2.1 搜寻可用网络

有些驱动程序支持列出该区所有网络的无线延伸功能。设置之前，可以使用 `iwlist` 命令从网卡取得相关信息。使用 `iwlist` 时需要指定界面以及一个副命令。`scan` 这个副命令将会印出该区所发现的可用网络信息。要取得扫描数据必须具备 `root` 权限。

```
root@bloodhound: ~# iwlist eth1 scan
eth1 Scan completed:
Cell 01 - Address: 00: 07: 50: D5: CE: 88
```

ESSID: "LuminiferousEther"

Mode: Master

Frequency: 2.417GHz

Quality: 0/10 Signal level: -70 dBm Noise level: -256 dBm

Encryption key: on

Bit Rate: 1Mb/s

Bit Rate: 2Mb/s

Bit Rate: 5.5Mb/s

Bit Rate: 11Mb/s

Cell 02 - Address: 00: 09: 5B: 72: 12: 58

ESSID: "Mom's House"

Mode: Master

Frequency: 2.467GHz

Quality: 0/10 Signal level: -22 dBm Noise level: -256 dBm

Encryption key: on

Bit Rate: 1Mb/s

Bit Rate: 2Mb/s

Bit Rate: 5.5Mb/s

Bit Rate: 11Mb/s

Cell 03 - Address: 00: 0D: 72: 9B: FE: 69

ESSID: "2WIRE086"

Mode: Master

Frequency: 2.442GHz

Quality: 0/10 Signal level: -28 dBm Noise level: -256 dBm

Encryption key: on

Bit Rate: 1Mb/s

Bit Rate: 2Mb/s

Bit Rate: 5.5Mb/s

Bit Rate: 11Mb/s

Bit Rate: 22Mb/s

Bit Rate: 6Mb/s

Bit Rate: 9Mb/s

Bit Rate: 12Mb/s

19.2.2.2 设置网络名称

要与网络连接，首先必须选择打算加入的网络。做法是以 **essid【注】** 参数来设置 SSID。如果网络名称中包含空白，则必须在前后加上引号。此时网络界面或许尚未启动，因此必须先以

ifconfig 命令启动之后方能进行网络搜寻。要检视扫描的进度，可以连续执行几次 iwconfig，然后查看扫描至哪个频率。例如，要搜寻使用频道 56 的基站，你可以这么做：

```
[root@bloodhound] # iwconfig ath0 essid "Space Cadet"
[root@bloodhound] # ifconfig ath0 up
[root@bloodhound] # iwconfig ath0
...
Mode: Managed Frequency: 2.412GHz Access Point: 00: 00: 00: 00: 00: 00
...
[root@bloodhound] # iwconfig ath0
...
Mode: Managed Frequency: 2.447HZ Access Point: 00: 00: 00: 00: 00: 00
...
[root@bloodhound] # iwconfig ath0
...
Mode: Managed Frequency: 5.17GHz Access Point: 00: 00: 00: 00: 00: 00
...
[root@bloodhound] # iwconfig ath0
...
Mode: Managed Frequency: 5.28GHz Access Point: 00: 0B: 0E: 00: F0: 43
...
```

一旦网卡发现网络，就会与基站连接，然后在 iwconfig 的输出中显示基站的 MAC 位址。与网络连接只是第一步骤。在进行逻辑网络连接之前，也许还需要进行其他配置设置。

如果频道已经通过自动配置方式设置完成(automatically configured)，则会对某些驱动程序造成问题。如果频道已经设死(hard set)，驱动程序可能就不会进行搜寻。要解决驱动程序卡死在特定频道的问题，可以先以 cardctl eject 命令停用网卡、重新设置 SSID，然后以 ifconfig 重新启用界面。

19.2.2.3 设置网络频道

不同网卡支持不同的作业频率。采用 Atheros 芯片组的网卡支持整个 ISM 频段，最高至第 14 频道，以及三个 5 GHz 频段。驱动程序如果支持此项作业，就可以使用 iwlist 命令列出受到支持的频道：

```
root@bloodhound: ~ # iwlist ath0 channel
ath0 255 channels in total; available frequencies:
    Channel 01: 2.412 GHz
    Channel 02: 2.417 GHz
    Channel 03: 2.422 GHz
    Channel 04: 2.427 GHz
    Channel 05: 2.432 GHz
```



Channel 06: 2.437 GHz
Channel 07: 2.442 GHz
Channel 08: 2.447 GHz
Channel 09: 2.452 GHz
Channel 10: 2.457 GHz
Channel 11: 2.462 GHz
Channel 12: 2.467 GHz
Channel 13: 2.472 GHz
Channel 14: 2.484 GHz
Channel 34: 5.17 GHz
Channel 36: 5.18 GHz
Channel 38: 5.19 GHz
Channel 40: 5.2 GHz
Channel 42: 5.21 GHz
Channel 44: 5.22 GHz
Channel 46: 5.23 GHz
Channel 48: 5.24 GHz
Channel 50: 5.25 GHz
Channel 52: 5.26 GHz
Channel 56: 5.28 GHz
Channel 58: 5.29 GHz
Channel 60: 5.3 GHz
Channel 64: 5.32 GHz
Channel 100: 5.5 GHz
Channel 104: 5.52 GHz
Channel 108: 5.54 GHz
Channel 112: 5.56 GHz
Current Frequency: 5.28GHz (channel 56)

作业频率有三种选择方式。如果以之前所描述的方式进行，大多数网卡就会开始搜寻 SSID。至于不支持扫描功能的网卡，可以使用 freq 参数直接设置作业频率，或者使用 channel 参数指定适当的频道编号，驱动程序会将频道编号自动转换为相应的频率。以下两道命令可以达到相同的目的：

```
[root@bloodhound] iwconfig ath0 freq 2.4326
[root@bloodhound] iwconfig ath0 channel 4
```

19.2.2.4 设置网络模式以及连接基站

通常 802.11 工作站若不是处于 ad hoc 网络，就是处于 infrastructure 网络。iwconfig 将这两种模式分别命名为 Ad-hoc 与 Managed。你可以使用 mode 参数从中挑选一种模式：

```
[root@bloodhound] # iwconfig ath0 mode Ad-hoc
[root@bloodhound] # iwconfig ath0 mode Managed
```

处于 infrastructure 网络的工作站，可以使用 aP 参数要求与所指定的 MAC 位址连接。不过，工作站并不是非得一直与所指定的基站保持连接，如果信号强度衰减过多，也可以选择漫游至其他基站：

```
[root@bloodhound] # iwconfig ath0 ap 01: 02: 03: 04: 05: 06
```

19.2.2.5 设置买料传输率

大部分网卡均支持几种不同的位元传输率。iwconfig 允许管理人员以 rate 参数从中挑选。位元传输率可以在 rate 参数之后指定，或者使用 auto 这个关键字，如此一来，在信号品质较差的频道中，网卡就会自动降速至较低的位元传输率。如果 auto 和某种位元传输率合并使用，驱动程序就会使用低于所指定速率的任何传输率：

```
[root@bloodhound] # iwconfig ath0 rate auto
```

19.2.2.6 设置静态 WEP 密钥

Key 这个参数用来控制驱动程序的 WEP 功能。密钥的键入可以使用十六进制数字所构成的字串。所键入的字串可以不带任何分隔字符，也可以每四个数字一组，每组数字以破折号隔开，或是以冒号区隔每个位元组：

```
[root@bloodhound] # iwconfig ath0 key 0123456789
[root@bloodhound] # iwconfig ath0 key 0123-4567-89
[root@bloodhound] # iwconfig ath0 key 01: 23: 45: 67: 89
```

许多驱动程序也支持 104 个位元的 WEY 密钥。104 个位元刚好是 13 个位元组，或者 26 个十六进制字符：

```
[root@bloodhound] # iwconfig ath0 key 12345678901234567890123456
[root@bloodhound] # iwconfig ath0 key 1234-5678-9012-3456-7890-1234-56
[root@bloodhound] # iwconfig ath0 key 12: 34: 56: 78: 90: 12: 34: 56: 78: 90:
12: 34: 56
```

虽然可以在中括号里指定编号来输入多把密钥，但并不是所有网络均会使用这项功能。通过 802.1X 来指定动态 WEP 密钥是比较简单的做法，不但可以使用多组密钥，也比较安全。

```
[root@bloodhound] # iwconfig ath0 key 0123-4567 - 89
[root@bloodhound] # iwconfig ath0 key 9876 - 5432-01 [2]
[root@bloodhound] # iwconfig ath0 key 5432 - 1678 - 90 [3]
```

一旦键入多组密钥后，可以直接以索引编号来选用特定的密钥，而无须使用密钥值：

```
[root@bloodhound] # iwconfig ath0 key [2]
```

要启动或停用 WEP 作业，可分别以 key on 与 key off 参数加以指定。这些参数可以在选取新的 WEP 密钥时，与索引编号搭配使用：

```
[root@bloodhound] # iwconfig ath0 key [3] on
[root@bloodhound] # iwconfig ath0 key off
```

最后, WEP 的作业方式可以区分为两种。Open (开放) 系统接受以明文方式传递的数据帧, 而 restricted (受限) 系统会将明文形式的数据帧加以丢弃。这两个参数均可与索引编号搭配使用:

```
[root@bloodhound] # iwconfig ath0 key [4] open
[root@bloodhound] # iwconfig ath0 key [3] restricted
```

key 这个参数也可以用 encryption (可缩写为 enc) 参数来替代。我比较喜欢使用 key 这个参数, 因为对我而言比较清楚, 不过你可以选择自己喜欢的方式。

19.2.2.7 调校 802.11 参数

iwconfig 允许使用者调校 RTS 与 fragmentation 门槛。大多数驱动程序将 RTS 门槛设为 2,347, 这个值可以有效停用 RTS 净空功能。在可能有隐藏节点的环境里, 可以使用 **iwconfig** 设置 rts_threshold (可缩写为 rts) 参数。

```
[root@bloodhound] # iwconfig wvlan0 rts 500
```

fragmentation 门槛的预设值是 2.346。在杂讯较多的环境里, 降低 fragmentation 门槛以减少数据量是值得的, 因为当帧漏失或因碰撞损毁时, 就必须加以重传。可以使用 **iwconfig** 配合 fragmentation_threshold (可缩写为 frag) 参数来指定此门槛。其值可介于 256 到 2,356 之间, 不过必须是偶数值。

```
[root@bloodhound] # iwconfig ath0 frag 500
```

802.11 工作站本身维护了几个重传计数器。当帧重传“太多”次, 或等候传输“太久”, 就会被弃置不用。工作站所维护的重传计数器有两种。长帧重传计数器以 **retry** 参数来指定, 代表比 RTS 门槛长之帧的重传次数。短帧重传计数器以 **retry min** 参数来设置, 代表比 RTS 门槛短之帧的重传次数。和一些驱动程序不同的是, **iwconfig** 也允许以 **retry lifetime** 参数来设置每个帧的最长存活时间。要以毫秒(milliseconds) 或微秒(microseconds) 指定时间值, 可以分别在时间值后加上 m 或 u:

```
[root@bloodhound] # iwconfig ath0 retry 4
[root@bloodhound] # iwconfig ath0 retry min 7
[root@bloodhound] # iwconfig ath0 retry lifetime 400m
```

19.3 Agere (Lucent) Orinoco

无线网络的历史远比 802.11 标准悠久。一些专属系统在 1990 年代初期就已经发表, 并且在市场上取得一定的占有率。其中最值得注意的产品是 NCR 的 WaveLAN, 发表当时, NCR 还是 AT&T 的一个部门。【注】Lucent 在 1996 年由 AT&T 独立出来当时, WaveLAN 部门和其他 AT&T 所生产的通讯产品一样被划归为 Lucent 所有。

早期的 WaveLAN 硬件完全是封闭的专属系统。802.11 在 1997 年正式成为标准后, 符合标准的新硬件才以 WaveLAN 品牌对外销售。为了区别两者, 符合标准的卡片称为 WaveLAN IEEE 网卡。专属系统则只称为 WaveLAN 网卡。

当 802.11 硬件的市场逐渐发展, Lucent 决定将 WaveLAN 部门以其他品牌重新命名。Orinoco (奥利诺科) 这个新名称来自于全世界第三大河流。由于南美的多雨气候, Orinoco 汇

集了两百条以上支流的水量。在河水高涨时，该河会膨胀为 10 英里宽，水深达 300 英尺。1,300 英里长的 Orinoco 河有将近 1,000 英里可以航行，难怪这条河的名称原意为“可划船之地”。

在开放原始码平台上，Lucent 原本采取的策略是，提供不同的驱动程序方案。Lucent 提供了两种驱动程序。`wavelan2_cs` 是封闭专属的二元驱动程序，此驱动程序提供完整功能。此外，功能较少的开放原始码驱动程序 `wvlan_cs` 以 GPL 方式授权使用。`Wvlan_cs` 驱动程序是以封闭原始码驱动程序所提供的低价程序库为基础，不过已经面临发展的死胡同。放弃延续传统路线之后，`wvlan_cs` 的低价控制层经过重新改写，成为 Linux 2.4 版核心中的 `Orinoco_cs`。（`Orinoco_sc` 原本称为 `dldwd_cs`，代表 David's Less Dodgy WaveLAN Driver!）



注 创办于 1884 年的 NCR (National Cash Register Company) 在 1991 年被 AT&T 所并购。一家收银机公司会对无线网络产生兴趣。以我推论大概是因为如此一来收银机就可以任意摆设不必拉线了。

除了 WaveLAN 以及其他 OEM 版本的 WaveLAN 网卡，`orinoco_cs` 对一些使用 PRISM-2 芯片组的网卡，以及使用相同 MAC 控制芯片的 Symbol 网卡，提供了基本的功能。2.4.3 版以后，`orinoco_cs` 成为了 Linux 发行套件的一部分。

19.3.1 编译与安装

所有采用 2.4 版以上核心的 Linux 发行套件均随附 `orinoc_CS` 驱动程序。在某些情况下，可以直接使用核心所附的驱动程序。如果打算执行 `xsupplicant` 或是需要修补密钥管理功能则另当别论，这些议题将于稍后探讨。

19.3.1.1 PCMCIA 的配置设置

许多随附 `wvlan_cs` 驱动程序的老旧发行套件仍然还在使用中。要更换发行套件所使用的驱动程序，只要换掉系统 PCMCIA 配置的模组即可。`orinoco_cs` 的作者提供了一个名为 `hermes.conf` 的文档，其中包含 `orinoco_cs` 所支持网卡的卡片定义。因为 `hermes.conf` 属于 `.conf` 档。因此可以在负责读取所有 `.conf` 档的 `/etc/pcmcia/config` 档尾处被汇入。不过为了避免系统上有所冲突，你必须注销掉所有 `wvlan_cs` 所使用的部分，以防其与新插入的卡片系统结在一块。另一种做法是先以 `duamp_cis` 读出卡片的辨识数据，然后编辑无线网卡的定义以便与 `orinoc_CS` 系统结：

```
# in hermes.conf
#
card "Lucent Technologies Wavelan/IEEE"
version "Lucent Technologies", "WaveLAN/IEEE"
bind "Orinoco_cs"

# from standard/etc/pcmcia/config
#
# card "Lucent Technologies WaveLAN/IEEE"
# version "Lucent Technologies", "WaveLAN/IEEE"
# bind "wvlan_cs"
```

19.3.1.2 自行编译

这部分涵盖在核心当中，因此通常无须进行安装，除非是为了修复特定的错误或者补强某些功能。之所以要重新编译驱动程序，通常是为了支持动态 WEP 以及 802.1X 身份认证。`xsupplicant` 发行了一个修补程序用来产生动态密钥。韧体或许也得更新才有办法支持动态密钥。我所使用的韧体版本为 8.42。8.42 以上的版本确定可以正常运作，较旧的版本就不见得了。

自行编译的方法十分简单。程序码本身可以从 <http://ozlabs.org/people/dgibson/dldwd/> 下载。请确定手上的修补程序可以修补所有你感兴趣的功能（0.15rc2 版不需要 rekey 修补档）：

```

gast@bloodhound: ~$ cd orinoco-0.13e
gast@bloodhound: ~/orinoco-0.13e$ patch -pl<../rekey_patch_orinoco-0.13e
patching file orinoco.c
patching file orinoco.h
msg@bloodhound: ~/orinoco-0.13e$ make
(省略组讯息)
root@bloodhound: /home/msg/orinoco-0.13e # make install
if [-d /etc/pcmcia] ; then install -m 644 -o 0 -g 0 hermes.conf
    /etc/pcmcia/hermes.conf ; fi
mkdir -p /lib/modules/2.4.26/kernel/drivers/net/wireless
for f in hermes.o orinoco.o orinoco_cs.o orinoco_plx.o orinoco_tmd.o
    orinoco_pci.o ; do \
if test -e /lib/modules/2.4.26/pcmcia/$f ; then \
install -m 644 -o 0 -g 0 $f /lib/modules/2.4.26/pcmcia/$f ; \
else \
install -m 644 -o 0 -g 0 $f /lib/modules/2.4.26/kernel/drivers/net/wireless/$0f ; \
fi ; \
done
depmod -a

```

编译完成后，系统将会产生几个系统核心模组：`orinoco_cs.o`（PCMCIA 界面）、`orinoco.o`（硬件驱动程序）以及 `hermes.o`（MAC 芯片驱动程序）。

19.3.2 设置 orinoco_cs 界面的配置

`orinoco_cs` 的配置与 `wvlan_cs` 的配置相同。插入卡片之后，就会执行`/etc/pcmcia/wireless` 命令稿，同时会用到`/etc/pcmcia/wireless.opts` 档中所记载的配置选项。`wireless` 命令稿其实不过是 `iwconfig` 程序的前端。编辑 `wireless.opts` 档中的栏位，实际上就是在设置 `iwconfig` 的参数。为 `iwconfig` 设置选项的细节，请参阅上一节论及 `wvlan_cs` 驱动程序的部分。

安装 WEP 密钥后的重置动作

在 Linux 上使用动态 WEP 时，802AX supplicant 会从认证程序中产生 WEP 密钥，然后将之载入驱动程序。1999 年之前，有些网卡并不支持动态密钥，必须重置（reset）网卡中的微控制器方能让新的密钥生效。当初编写驱动程序时通常会以此为前提，因此更新密钥的程序码会负责重置硬件。

对动态 WEP 而言，每次更换新的密钥便重置硬件是无法接受的。一旦身份认证完成，说必须进行全钥的安装。如果驱动程序在密钥安装完成后即进行重置，连接就会中断。塞地台注意到连接中断后会要求重新进行身份认证。一旦申请者检测到连接状态改变，将重新进行身份认证以产生新的密钥。“当身份认证再度完成，supplicant 又会重置网卡以便安装新的密钥，就这样陷入没完没了的循环。

大多数界面卡目前都已提供韧体更新，解决安装密钥后必须重置硬件的问题。韧体更新为正确版本后，也必须将驱动程序一并更新成不会送出重置命令・具备动态 WEP 能力的版本。

如果动态 WEP 无法正常运作是因为网卡在身份认证后的重置动作，除了检视原始码，也可以到线上论坛确定网卡驱动程序是否有更新版本，或者需要进行修补。

19.4 采用 Atheros 芯片组的网卡与 MADwifi

802.11a 是高速/高密度之 802.11 网络的最佳选择，市面上大多数的 802.11a 设备均会采用 Atheros 芯片组。【注】它的驱动程序专案称为“Multiband Atheros Driver for WiFi”，简称为 MADwifi，网址为 <http://sourceforge.net/projects/madwifi/>。

虽然以 802.11a 著称，Atheros 其实推出了好几款不同的芯片组。该公司的芯片组分为三代。第一代芯片组称为 5210，只具备 802.11a 功能。之后就是第一套双频芯片组 5211，加入了 802.11b 功能。目前市面上大多数设备均使用 5212，它属于双频/三模芯片组，同时支持 802.11a、802.11b 以及 802.11g。此外，下一代的产品将能够处理更复杂的安全防护作业。MADwifi 支持上述所有芯片组。

19.4.1 驱动程序架构与硬件访问层

MADwifi 分为两部分：其一是开放原始码驱动程序，其二是称为“硬件访问层”（Hardware Access Layer，简称 HAL）的封闭原始码程序库。Atheros 芯片组相当有弹性，经过调校后也可以使用非免照频段，因为它们使用了某种特定型式的软件定义无线电。

对于 FCC 的管制规定，Atheros 的解读是不得公开硬件访问层（HAL）。（在市场上推出类似芯片组的 Broadcom 也采取同样的解释。）FCC 规定要求 SDR（软件定义的无线电）不得让使用者自行将其变更成，运作在非 FCC 核准的频段。违反 FCC 认证条款的设备就可能受罚。如果原本用于免照频谱的设备突然能够干扰有照（licensed）通讯，设备的供应厂商也将一并受罚。

对商业产品而言，要确保软件不致逾越免照频谱的范围并不困难，只要编译与散布的程序码不会破坏规定即可。使用者无法更动编译后的程序码，也就无从破坏规定。开放原始码改变了整个游戏。发行合乎规定的程序码，不见得可以防止有心人士的恶意篡改。

Atheros 面临一项抉择：是要释出完整的驱动程序原始码，并且承担可能遭管制当局禁止销售芯片的风险，或是找出某种可以保护无线电频谱的方式。Atheros 最后显然采取了后者。它通过 HAL 的 API 来访问无线电波，而不让开放原始码驱动程序直接访问无线芯片组。HAL 是相当普遍的做法，其他作业系统也经常以之开发开放原始码驱动程序；它们完全独立于主机系统软件，虽然还是离不开主机硬件的指令集。HAL 支持 X86 架构（32 与 64 位元）、ARM、MIPS、PowerPC

以及 Xscale。虽然开放原始码社群对封闭原始码通常怀有疑虑，我认为 Atheros 此举已经表达了他们对于 Linux 平台的承诺，亦即该公司愿意支持驱动程序的开发。

19.4.2 先决条件

MADwifi 广泛使用了无线延伸功能，而且通常以最近的版本进行开发。你可以使用支持最新版本的发行套件，或者将核心升级至最新版本。

驱动程序通常会用到其他的核心功能，MADwifi 自不例外。组建 MADwifi 需要用到一些核心标头档，以及执行核心所需要的配置档。如果核心是你针对所使用的硬件平台自行打造的，你手上应该已经有核心原始码以及相关的配置设置。不过核心原始码与配置设置并非所有发行套件的预设安装选项，有时候可能必须自行找出正确的软件套件。

要取得 HAL，你还需要用到 UUCP 工具。为了能够在网络上安全地传输 HAL 程序码，因此该程序码经过 uuencode 的编码。MADwifi 的 make 命令稿会叫用 uudecode。uudecode 可能属于 shell archive utilities 软件套件 (sharutils)，或者属于 UUCP tool 软件套件，这取决于你所使用的发行套件。

19.4.3 组建驱动程序

MADwifi 仍然在持续进行开发，而且经常更新。它是以 CVS 进行维护，而不是定期发行更新套件。要取得最新版本，可以通过 CVS：

```
root@bloodhound: ~# cvs -z3 -d: pserver: anonymous@cvs.sourceforge.net:  
/cvsroot/madwifi co madwifi
```

这道命令执行后，原始码以及编码过的 HAL 文档便会被下载至 madwifi 目录。要组建驱动程序，可以键入下列开放原始码常用的标准命令：

```
root@bloodhound: ~# cd madwifi  
root@bloodhound: ~/bloodhound # make  
中略  
root@bloodhound: ~/bloodhound # make install
```

主要的模组有 wlan.o、ath_pci.o 以及 ath_hal.o。一些其他的加密模组会在需要时被载入，以支持特定的加密格式。如果 MADwifi 组建系统无法在文档系统中检测到正确的安装位置，你就必须手动将这些必要的模组置于正确的地点，然后执行 depmod -a 来更新模组。

19.4.4 驱动程序的使用

最新版的 MADwifi 驱动程序会将所支持的网卡列表提供给核心，在检查模组相依性时就可以看见。此列表包含了一些厂商识别码为 0x168c 的设备，这个识别码即属 Atheros 所有。如果模组相依性正确无误，就没有必要修改 PCMCIA 配置设置命令稿。

载入驱动程序会产生一个字首为 ath 的界面。如果系统中只有一张 Atheros 网卡的话，通常命名为 ath0。旧版的 MADwifi 使用 wlan 做为字首。如果界面名称为 wlan0，请更新驱动程序。

MADwifi 已经与 Linux 热插拔系统整合无误。插入网卡模组时，热插拔系统会尝试登录该界面。几乎可以确定的是，发行套件所使用的启动命令稿 (start-up script) 必然需要修改；使用

开放系统的无线网络可能只需稍作修改；使用 802.1X 则需要大幅修改，因为在 DHCP 程序进行之前，界面必须已经通过验证。

在 Linux 中使用 Windows 驱动程序

并非所有网卡厂商均承诺支持 Linux。释出驱动程序原始码可能泄露智慧财产权是主要的考虑。必须提供额外人力来撰写、维护与支持释出给使用者社群的驱动程序则是另外的考量。

针对 Linux 量身订作的驱动程序通常比较受到欢迎。不过，即使网卡厂商尚未提供 Linux 驱动程序，还是可以通过包装程序（wrapper program）来使用 Windows 驱动程序。目前有两种软件套件可以执行 Windows NDIS 驱动程序，居中将 Windows 系统呼叫转换为 Linux 系统呼叫。NDISWrapper 专案(<http://ndiswrapper.sourceforge.net/>)提供了完整的开放原始码实作。另外一家名为 Linuxant 的公司则开发出了一套称为 DriverLoader 的商业程序(<http://www.linuxant.com/driverloader/>)，提供相同的功能。试用版是免费的，如要持续使用就必须付费。

19.5 在 Linux 中使用 xsuplicant

过去几年，我有幸担任 Interop Labs 无线安全制定小组的志工，可以就近体验互通性的运作。2004 年，Open1X 专案的开发人员参加了互通性测试大会，将开放原始码带到之前只有产品制造商能够参加的会议。当无线网络逐渐普及，众人也愈来愈有兴趣为 Linux 系统提供安全的无线局域网络解决方案。xsuplicant 算是这些 802.1X 实作中的佼佼者。

19.5.1 先决条件

考虑使用 xsuplicant 之前，最重要的工作是确定 802.11 已经运作无误。有些“无线”问题是 PC Card 的问题。当然，除非你已经建构与设置好 xsuplicant，否则就无法连上已经验证的网络，但是插入无线网卡时，系统应该要能够辨识得出。辨认出网卡时，Card Service 通常会发出一个高音哔声，代表资源已经成功配置，驱动程序也已经载入。（后续或许会出现一个低音哔声，代表配置设置失败，不过这并没有关系。有可能你希望最后再使用自己的配置设置来执行 xsuplicant，因此一开始没有配置设置的支持是可以接受的。）成功载入驱动程序后就可以执行 iwconfig，以便从驱动程序取得相关的统计信息。

不过就算可以驱动网卡，最好还要确认一下能否支持动态 WEP。虽然动态产生密钥的 WEP 系统其绝对安全性尚有争论，它的安全性比单一密钥 WEP 系统来得高是毫无疑问的。要使用 xsuplicant 的话，网卡必定得支持动态密钥功能。2003 年初以后发行的网卡均已提供支持动态 WEP 的驱动程序，不过一些较旧的网卡就需要进行修补。常见的 Orinoco 802.11b 网卡（使用 Hermes 芯片组）即属后者。编译驱动程序时，你可能还需要重新建构核心（或者至少取得一份核心的配置设置），视驱动程序而定。

最后，xsuplicant 还需要用到一个程序库。如前所述，大多数的 EAP 认证方式均以 TLS 为基础。xsuplicant 使用的是 OpenSSL TLS 实作。请安装 0.97 或者之后的版本。从 openssl.org 取得原始码之前，请确定你的发行套件是否提供该软件套件。

19.5.2 编译与安装 xsuplicant

xsuplicant 的编译与安装仍是遵循开放原始码套件的标准程序。你可以从 <http://sourceforge.net/projects/openlx/> 取得已发行的原始码，并以标准的 Unix 程序进行编译：

```
root@bloodhound: ~# tar -xzvf xsuplicant-1.0.1.tar.gz
```

```
root@bloodhound: ~# cd xsupplicant
root@bloodhound: ~/ xsupplicant# ./configure
root@bloodhound: ~/ xsupplicant# make
root@bloodhound: ~/ xsupplicant# make install
```

本书即将付印时，`xsupplicant` 1.0.1 已经发行好几个月，CVS 版本中已经累积不少修正。（本节所使用的是 200 缠最新的 CVS 版本。）除了一些修正，这个 CVS 版本初步支持 WPA。CVS 版本可以从任何匿名 CVS 服务器取得，同样是以标准的 Unix 程序进行编译：

```
root@bloodhound: ~# cvs -z3 -d:pserver: anonymous@cvs. sourceforge.net:
/cvsroot/xsupplicant co xsupplicant
root@bloodhound: ~# cd xsupplicant
root@bloodhound: ~/xsupplicant# ./configure
root@bloodhound: ~/xsupplicant# make
root@bloodhound: ~/xsupplicant# make install
```

建构完成之后，会在系统中安装三个可执行档；其中最可能用到的就是 `/usr/local/sbin/xsupplicant`。

19.5.3 xsupplicant 的配置设置

执行时，`xsupplicant` 会在 `etc` 目录中搜寻配置档。预设上并不会安装`/etc/xsupplicant.conf` 这个配置档，请自行将它复制到定位。

```
root@bloodhound: ~/xsupplicant# cp etc/xsupplicant.conf/etc/
```

配置档中指定了身份认证方式、使用者识别码，有时也会指定密码以及凭证所在位置，以便进行网络验证。网络的凭证验证也可以停用，只要将凭证位置设为 `NONE` 即可，但是不建议这么做。设置网络时，你或许需要将凭证转换为其他格式。`OpenSSL` 可以轻易转换各种不同的格式，只要在命令列指定所需格式即可。

`root@bloodhound: ~# openssl x509 -inform DER -outform PEM -in MyCA.der -out MyCa.pem` 密码系以未加的密格式存放在配置档中，但是你或许希望系统提示你输入密码，而不要将敏感的数据摆在配置档里。如果配置档中没有所要连接网络的密码，`xsupplicant` 就会提示使用者输入密码。

配置档中，每个 `SSID` 都可以拥有一份自己的设置描述。在下面的配置档范例中，一个名为 `batnet` 的网络上，使用了 `PEAP` 以及 `EAP-MSCHAP-V2` 内层验证方式。`xsupplicant` 可以被设置成，在认证完成之后执行命令，或是让作业系统的命令稿来执行。

```
### GLOBAL SECTION
logfile=/var/log/xsupplicant.log
network_1ist=all
default_netname=batnet
first_auth_command=dhcpcd %i
### NETWORK SECTION
```

```
batnet {
    # allow_types=eap_tls, eap_md5, eap_gtc, eap-otp
    allow_types=eap_peap
    # Phase 1 ("outer") identity
    identity=msg
    # Alternative, but common specification is to not reveal username
    # identity=anonymous
    eap-peap {
        # It is a good idea to validate the certificate and not do "none"
        # root_cert=NONE
        root_cert=rootCA.pem
        root_dir=/etc/xsupplicant.d
        chunk_size=1398
        random_file=/dev/random

        # ** Inner method configuration
        allow_types=eap_mschapv2

        # Inner method configuration
        eap-mschapv2 {
            username=msg
            password=imnottelling
        }
    }
}
```

19.5.3.1 产生准随机数

和其他安全性协议一样，EAP 验证方式需要有好的随机数来源。Linux 提供两种随机数设备：`/dev/random` 与 `/dev/u random`。前者所传回的随机位元是从系统的乱数集区(**entropy pool**)取得。如果目前没有足够的乱数可用，读取的动作就会一直等候。后者则会立即传回目前可用数据，代价是牺牲数据的品质。

19.5.4 网络连接与身份认证

要访问经 802.1X 防护的网络，首要步骤就是与之连接。**xsupplicant** 进行连接的方式与系统有关。初始的配置设置应该告诉网卡必须使用加密帧，虽然密钥本身并不重要。设置一个假密钥，告诉驱动程序应该使用加密模式。**xsupplicant** 将在身份认证成功后，呼叫 **wireless extension** 程序库，以便替换密钥。最常见的连接设置方式，就是利用 **iwconfig** 设置密钥及网络，然后以

ifconfig 启用网络界面及搜寻网络。当然，这些命令可以在插入无线网卡时，由命令稿加以执行。

```
root@bloodhound: ~#iwconfig ath0 key 12345678901234567890123456  
root@bloodhound: ~# iwconfig essid "batnet"  
root@bloodhound: ~# ifconfig ath0 up
```

系统与网络连接之后，就可以执行二 **suplicant -i** 选项用来指定所要执行的界面。排错功能可以通过一 **d** 选项启动，后续选项则是用来指定要印出多少信息。**-f** 选项可以将 **log** 信号显示在操控台（**console**）。接下来是经过删节的原始封包倾印。

```
root@bloodhound: ~# /usr/local/sbin/xsupplicant -i ath0 -dasic -f  
Using default config!  
Network_list: all  
Default network: "default"  
Startup command: "echo" some command" "  
First_Auth command: "dhclient of"  
Reauth command: "echo" authenticated user of ""  
LogFile: "/var/log/xsupplicant.log"  
Allow Types: ALL  
ID: "msg"  
peap root cert: "NONE"  
peap chunk: 1398  
peap rand: "/dev/random"  
PEAP Allow Types: ALL  
mschapv2 username: "msg"  
mschapv2 password: "imnottelling"  
Interface ath0 initialized!
```

至此，**xsupplicant** 已经读取了配置档，并且检视无线界面是否已经与基站连接。若已连接，则开始进行身份认证程序。

```
[INT] Interface ath0 is wireless!  
[INT] The card reported that the destination MAC address is now 00 0B 0E 00 F0 40  
[INT] Working with ESSID: batnet  
[CONFIG] Working from config file /etc/xsupplicant.conf.  
[STATE] (global) ->DISCONNECTED  
[STATE] Processing DISCONNECTED state.  
[STATE] DISCONNECTED->CONNECTING  
[STATE] CONNECTING->ACQUIRED  
[STATE] Processing ACQUIRED state.
```

一旦系统已经与基站连接，就会开始进行身份认证。

Connection established, authenticating...

[STATE] Sending EAPOL-Response-Identification

[STATE] ACQUIRED->AUTHENT (CATING)

[STATE] Processing AUTHENTIGATING state.

[STATE] Sending EAPOL-Response-Authentication

****WARNING**** Turning off certificate verification is a *VERY* bad idea !

You should not use this mode outside of basic testing, as it will compromise
the security of your connection !

[AUTH TYPE] Packet in (1) :

20

[AUTH TYPE] Setting Key Constant for PEAP v0 !

[INT] Interface eth0 is NOT wireless !

Userdata is NULL ! We will probably have problems !

[STATEE] (global) ->DISCONNECTED

[STATE] Processing DISCONNECTED state.

[STATE] DISCONNECTED->CONNECTING

[STATE] Processing AUTHENTICATING state.

[STATE] Sending EAPOL-Response-Authentication

当双方开始对话，并且来回交换与验证凭证，就会出现一堆排错讯息。一旦建立起 TSL 管道，排错讯息就会显示内层身份认证。以 EAP-MSCHAP-V2 为例，RADIUS 服务器会送出一个盘查讯息。有了盘查讯息与共享密码，就可以产生回应讯息。

[AUTH TYPE] (EAP-MSCHAPv2) Challenge

[RUTH TYPE] (EAP-MS-CHAPv2) ID: 2F

[AUTH TYPE] Authenticator Challenge: C6 02 26 BE C3 E0 44 03 13 6E 1F BA F0
B3 1D 5A

[AUTH TYPE] Generated PeerChallenge: 28 62 AA A2 8C 8E EB 82 D1 9B 2F 9A 54
67 93 2C

[AUTH TYPE] PeerChallenge: 28 62 AA A2 8C 8E EB 82

[AUTH TYPE] AuthenticatorChallenge: C6 02 26 BE C3 E0 44 03

[AUTH TYPE] Username: msg

[AUTH TYPE] Challenge: 48 E7 AA 53 54 52 98 62

[AUTH TYPE] PasswordHash: C5 A2 37 B7 E9 D8 E7 08 D8 43 6B 61 48 A2 5F A1

[AUTH TYPE] Response: 4D 96 51 8C 18 3A F7 C7 70 15 47 13 19 D8 D6 9B 36 00
AD E8 FA 9A 0F 28

[AUTH TYPE] myvars->NtResponse=4D 96 51 8C 18 3A F7 C7 70 15 47 13 19 D8
D6 9B 36 00 AD E8 FA 9A OF 28

```
[AUTH TYPE] response->NT-Response=4D 96 51 8C 18 3A F7 C7 70 15 47 13 19
D8 D6 9B 36 00 AD E8 FA 9A 0F 28
[AUTH TYPE] (EAP-MSCHAPv2) Success!
[AUTH TYPE] Server authentication check success! Sending phase 2 success!
```

一旦通过身份认证，基站将提供密钥给系统。密钥本身会被“来自第一阶段 TLS 交换的共享加密密钥”所加密与验证。总共会送出两笔密钥讯息，其中一笔讯息包含工作站所使用的单点传播密钥（unicast key），另外一笔讯息包含所有工作站共享的广播密钥（broadcast key）。xsupplicant 会使用 wireless extensions API 来设置驱动程序中的密钥，这些密钥可以使用 iwconfig 来检视。

```
Processing EAPoL-Key!
[INT] Key Descriptor=1
[INT] Key Length=13
[INT] Replay Counter=41 2F BB 2D 00 00 00 D5
[INT] Key IV=69 4C 45 D7 CF C3 DD CD 2A 3A F3 CB 04 7A F4 A3
[INT] Key Index (RAW) =01
[INT] Key Signature=C2 05 6C 3A EB 25 E9 B9 8E FC 60 D6 77 44 57 22
[INT] EAPoL Key processed: broadcast [2] 13 bytes.
[INT] Key before decryption: ED 5D 03 D2 7A DE B4 60 29 FD FD F5 42
[INT] Key after decryption: FB BB AC D3 6F 7D OA 3F FF 2A CF 33 4E
[INT] Successfully set WEP key [2]
Processing EAPoL-Key!
[INT] Key Descriptor=1
[INT] Key Length=13
[INT] Replay Counter=41 2F BB 2D 00 00 00 D6
[INT] Key IV=66 15 69 E2 B2 8C OE 89 7C D3 94 8C 93 25 43 1B
[INT] Key Index (RAW) =80
[INT] Key Signature=49 C1 15 B8 E9 D0 87 53 A6 FD 5D 76 CB 51 9D 65
[INT] EAPoL Key Processed: unicast [1] 13 bytes.
[INT] Using peer key!
[INT] Successfully set WEP key [1]
[INT] Successfully set the WEP transmit key [1]
```

有些驱动程序实作了自己的系统呼叫来显示密钥。使用 MADwifi 驱动程序的 Atheros 网卡，可以用 iwlist ath0 key 命令列出密钥；有些驱动程序也会在 iwconfig 中显示单点传播密钥。

Linux 上的 802.1X 商用软件

除了 xsupplicant，市面上还有一套由 Meetinghouse Data Communications 公司所发行的商业软件。Meetinghouse 的 AEGIS 用户端程序支持相当多的 EAP 认证方式 (MD5, TLS, TTLS, PEAP 及 LEAP)。不过因为很难跟得上发行套件的脚步，因此只为 RedHat 8 与 9 两个版本提供官方支持。Linux 版的



Meetinghouse supplicant 并未支持 WPA, 理由和 *xsupplicant* 所抱持的一样: 缺乏标准的 WPA keying API (WPA 动态密钥应用程序开发界面)。

19.5.5 Linux 上的 WPA

通常 Linux 之上并无 WPA 功能, 因为没有一种标准的方式可以取得“进行四道磋商”所需要的信息。*xsupplicant* 在使用者空间执行, 然而计算四道磋商所需要的数据却必须从驱动程序取得。每一种驱动程序各自定义了访问这些数据的系统呼叫, 如此一来申请者就必须追踪个别驱动程序所定义之系统呼叫的后续发展。未来发行的 wireless extensions API 将会支持必要的系统呼叫, 到时 WPA 就会出现在开放原始码以及商业产品中。

第20 章 使用 802.11 基站

就算是最简单的 802.11 网络，能够正确设置基站（access point）也是一件重要的事。网络界面没设置好，根本就不会有任何数据被桥接至有线网络。

早期的 802.11 基站十分简单。通过基站内建的一组界面，可以将无线设备连接到既存的有线局域网络。早期的基站相当于无线与有线领域的桥梁，另外附带一些其他的功能。第一代无线局域网络产品刚上市时，粗略区分为便宜的家用闸道器与昂贵的商用产品。这些产品具备同样的功能。不过后者通常采用比较高档的元件，除了保障升级的弹性与设备的投资，也提供大规模部署所需要的管理工具。

802.11 刚问世时，通常将基站设计成独立的设备。早期无线局域网络虽然提供无线访问的功能，但是缺乏牢靠的安全性以及管理方面的能力。虽然这些网络中的孤岛偶尔互相往来，但因为所需要的协议尚未开发完成或未经大规模测试，所以通常不被视为大规模网络系统的一部分。当无线网络逐渐普及且规模逐渐扩大，传统上将基站设计为独立设备的做法，开始浮现缺点。

察觉到这股商机，有些厂商开始打造第二代的无线网络硬件。新式的做法是将基站的管理与支持功能，整合到具备 Ethernet 交换器基本功能的机器中，如此一来就只需要搭配具备电波界面的傻瓜型（dumbed-down）基站。虽然做法不同，业界通常将这种以「轻量级」（lightweight）或者「精简型」（thin）基站搭配中央控制系统的做法称为无线交换器（wireless switch）。自从 2002 年底开始流行之后，这种交换式（switch-based）架构就引起各方的兴趣，不过基本上还是必须提供等同第一代基站的功能。

本章主要在探讨如何使用基站。除了检视 Cisco 1200 系列的基站，本章也会提到 Apple 的 Airport Express } Cisco 1200 属于全功能的独立设备，因为功能很多，设置上并不容易。

20.1 基站的基本功能

大致而言，市面上的基站可以分为两种价位。家用低价机种通过零售管道，直接销售给一般使用者。这些低价设备属于特殊运算平台，其记忆体与储存能力有限。【注】高价机种内建一些额外的功能，可以支持较大规模的部署；通常，这些机种配备额外的记忆体与储存能力，并且使用更多通用型（general-purpose）硬件。这两种价位产品之间的差异，在于高价机种能够协同运作自成系统，建构出更加可靠、安全与可管理的网络。举一个稍嫌简单的类比，逐渐蔓延到家庭或小型办公室的小型无线局域网络就像无线电话（cordless phone）。它们可以在有限的距离内延伸网络的使用范围，但仅止于此。大型无线局域网络则像移动电话（cellular telephony），可以在更严苛的环境下维持连接品质。应付经常移动的使用者以及基站间的换手（hand-off）作业只是起码的要求，其所使用的管理与障碍排除工具也比较高档。

然而不论市场如何区隔，这些设备还是必须提供一组通用的功能，以达成 802.11 标准对这些服务所做的承诺。虽然每家厂商设置配置的方式各有不同，不过各家产品在功能与设计上其实极泻相似。

最明显的是，基站乃是扮演无线与有线之间的桥梁。既然如此，基站也就具备网络桥接器所有的功能。基站至少具备两个网络界面：其中的无线界面通晓 802.11 相板细节，而另一个界面则是连接至有线网络。我还未曾见过不以 Ethernet 做为有线后端（wired back-end）的基站，虽然标准的确不曾这样规范。当无线局域网络逐渐普及，一些高价机种开始在网络上链功能

(uplink) 方面支持 VLAN。有些低价基站会提供第二个 Ethernet 埠做为 WAN 埠，供缆线数据机 (cable modem) 或 DSL 使用，不过有少数产品只提供支持拨接数据机的 RS-232 口序列埠。

所有无线界面都必须支持 802.11 频道访问的基本规则，不过它们之间的共同点仅止于此。早期的基站是在网络的边陲地带实现所有 802.11 协议；新式设备则是把一些 802.11 功能自网络边陲地带移开，将 802.11 MAC 分解为跨系统的元件。大多数基站均可以加装外接天线，微调传输距离与覆盖范围。

桥接器中内建了一些缓冲记忆体。可容纳行经两界面间的帧，此外亦会将每个埠所对应的 MAC address 储存于内部的对照表。当然，桥接对照表 (bridging table) 的实现方式各有不同，业界并无一套放诸四海皆准的做法。功能最阳春或价格最便宜的机种，通常认为自己是网络中独一无二的基站或桥接器。如果基站支持漫游功能，有时候必须在基站间进行连接或使用者数据的转移。比较高档的基站或许需要新增一份基本的桥接对照表，用来记录有线界面上的 VLAN 信息，以及使用者如何进行身份认证的相关信息。

商用等级的产品在设计上会考虑到设备间的交互运作；最常见的功能是各厂商专属的漫游方式，可在基站间转移连接关系，同时维持链路层的连通性。商用等级的产品在网管功能方面通常较为复杂，好让网络工程人员得以管理涵盖范围相当大的数十甚至数百台设备。

起初，通过 TCP/IP 网络界面管理基站属于基本功能。过去几年，一项重大的创举是，开发出了所谓的[精简型] (thin) 基站解决方案，将基站的管理功能集中交由特定设备负责。

根据其所针对的目标市场，基站可能为无线用户提供不同的服务。其中最受欢迎的服务要算是 DHCP；无线工作站在连接后会被自动赋予一个位址。大型网络中，设备通常使用现有的 DHCP 服务器以确保基站间的一致性。有些基站也提供网络位址转换 (network address translation, 简称 NAT)，特别是可以连接数据机及拨接到 ISP 的[家用闸道器]之类的产品。

早在 802.11 取得成功之前，安全问题一直是无线网络管理人员关切的焦点。就安全的考虑，基站本身占据了相当特殊的地位。既然基站位居有线网络的闸道，在此实施安全政策再理想不过。除了第一代的安全防护（像是 MAC 位址过滤），目前大多数产品均已实现较坚固的使用者身份认证 (user-based authentication)。大多数家用产品可以使用预设共享密钥来执行 [Wi-Fi 访问防护] (Wi-Fi Protected Access, 简称 WPA)，大型企业也可以部署身份认证服务器与之搭配。目前，有些高价机种已能完美地整合到既存的有线网络。如何使用这些功能来延伸有线网络的最佳做法，将留待下一章探讨。

管理界面通常无法尽如人意。设置基地之所以具有挑战性，主要是因为基站在生产上必须尽可能便宜，而低价设备所具备的处理能力，通常难以支持易于设置的引擎所需要的条件。大部分厂商会使用轻量级的过程系统，执行于能力较低的硬件上，然而这种做法的缺点是，无法提供足以支持更多功能的程序设计环境。早期的基站通常会同时提供命令列以及网页管理界面。近来「Wi-Fi 交换器」(Wi-Fi switch) 的发展，为网管人员带来不少希望。所谓傻瓜型 (stripped-down) 或精简型 (thin) 基站是通过少数中央控管交换器来管理，不像过去必须分别管理每一部独立的基站。这些交换器具备较强的运算能力与功能，可以提供更多功能与更完善的管理界面。

排错与问题排除工具如同管理工具一般先进，不幸的是，这意味着，它们通常留给网络管理人员一堆难以判别，或者毫不相关的信息。理想上，这些产品必须维护网络活动的详细日志，不过时常会见到一些无用的纪录，难以让人洞察问题所在。除非维护得当，否则计数器也帮不上什么忙 ping 与 traceroute 之类的工具程序十分常见，不过网络分析软件及封包捕捉工具则不然。

20.1.1 基站的种类

大致而言，基站可以分为三种。知名的基站中有许多是通过各主要消费性电子产品卖场进行销售的低价产品。虽然此类基站占市场大宗，不过并不适合用于大规模的网络部署。就像消费性电子产品等级的 **Ethernet** 交换器不适合用来建构主要网络，便宜的基站也无法提供组建主要无线网络所需要的功能。高价机种具备许多重要的功能，主要是针对企业市场。

20.1.1.1 家用机种：家用闸道器

低价机种包含一般所谓的家用闸道器(**residential gateway**)。家用闸道器在设计上尽可能节省成本，因此只提供一些小型或家庭办公室所需要的基本功能。为了进一步降低成本，大多数家用机种均采用 802.11 芯片制造商所提供的「参考设计」（俗称公版）。设备制造商也许会（或许不会）更改公版或外壳，贴上自家品牌后便开始销售。

家用闸道器通常具备如下特点：

- 大部分机种均内建 DHCP 服务器，便于 plug-and-play（随插即用）的配置设置。
- 使用者通常会被配置一个可绕送（**routable**）的 IP 位址，因此使用 NAT 的做法十分常见。
【注】有些机种使用 PPPoE 或 DHCP 动态指定可绕送的外部位址（**routable external address**）。
- 依据家用闸道器主推的客户不同，其所配备的 WAN 界面有可能是数据机。序歹 J 埠，甚至是 DSL。（有些家用闸道器产品会使用 Ethernet 埠做为连接埠，以便与缆线数据机或者 DSL 数据机转接。）
- 它们通常自成一个独立的单元，并且内建天线。如果找不到适合的放置地点通常必须重新摆放。
- 有些产品宣称具备 IPSec 透通(**pass-through**)的功能，允许在 NAT 情况下使用 IPSec。根据所选用的 IPSec VPN 解决方案的不同，支持的程度会有差异。
- 家用闸道器的配置设置，通常是通过预设的私用 IP 位址。首次开机时，可以通过 web 浏览器指定预设位址，然后输入使用者名称和密码。有时候，同一家厂商所生产的设备会使用相同的预设位址。常见的预设网址是 192.168.0.1，亦即 RFC 1918 在传统的 class C 所保留的第一个私用位址。不过随着无线局域网络逐渐普及，有些厂商考虑到设备的共存性，就会任意挑选一个位址，或者检测该位址是否已被占用。
- 这些产品通常会直接销售给一般使用者，因此在设计上极尽美观之能事。不过对一些使用者而言，这些眩目的视觉设计，反而使他们无法将家用闸道器与其他网络设备堆叠在一起使用。不过，有些厂商刻意设计出只能与自家产品堆叠使用的产品。
- 小型网络设备的安全性设置选项通常有限。较旧的家用闸道器通常只提供 MAC 位址过滤或静态 WEP，因此购买二手设备时必须特别小心。目前，几乎所有市售产品均已使用 WPA 的预设共享密钥身份认证，搭配动态加密密钥。
- 大多数家用型无线电系统都很简单。它们通常只配备单一无线界面，使用 802.11b 或 802.11a。前者在家用产品上比较常见，因为 802.11g 所使用的 2.4 GHz 频段覆盖范围较广。家用网络通常受限于 Internet 的上行频宽 1 因此没有必要缩小覆盖范围，增加基站数目来提升频宽。

写作本书当时，家用闸道器的价格大约介于 35 至 100 美元之间。常见的厂商有 D-Link、Linksys 与 Netgear。Apple 的 Airport 有时候也被归于此类，不过它的价格显然较高，也具备较多功能。

20 . 1 . 1.2 一般商用机种：企业基站

尽管有各种不同的称谓，企业闸道器（enterprise gateway）这个名词意味着，使用者比较侧重产品的功能，而非产品的价格。除了提供家用闸道器（residential gateway）所具备的功能，企业闸道器还具备一些大规模环境所需要的额外功能。企业闸道器通常具备如下特点：

- 需要在较大的范围提供移动性，必须有几部基站彼此合作。企业级产品支持某种协议，可以在基站间转移连接。
- 企业级产品着重可升级性，目的是尽可能延长产品的使用年限。它们通常采用功能较强的通用型硬件，并以软件实现大部分的高价功能，因此相当容易升级。它们也可能采用抽换方便的无线界面。早期企业级基站使用的是 PC Card 界面，因此要从 802.11b 切换到 802.11a 只要更换网卡即可，顶多搭配软件的升级。随着零件价格不断滑落，无线网卡通常已经无法升级，不过软件可以。
- 以高价软件控制企业级基站的好处之一，就是可以随时通过软件更新的方式，将最新的安全功能加入基站。任何称得上企业等级的基站均支个 WPA，有些厂商承诺可以通过软件，轻易升级至 802.11i。当新的安全功能成为标准，不必更换硬件就可以将它们添加到既有网络。企业级基站通常是以逐层添加的方式新增安全功能，如此一来，新旧安全机制便可并存共用。通祈论只有更高档的产品，才会抢先以硬件更新安全功能。当初芯片组开始以硬件支持更快的 AES 加密，就是高档产品最先采用。有些企业级基站可以同时支持多种安全标准。
- 企业级的部署，通常是在相当大的区域内提供地毯式（coverage blanket）的服务。基站所在之处不见得方便供电，但集线槽（wiring closet）的电力供应通常不虞匮乏。所有企业级基站均支持 IEEE 802.3af 标准，可以通过 Ethernet 汲取所需要的电源。
- 高价产品所使用的无线界面，通常比低价产品来得复杂。大多数企业级基站均提供天线接头，可以加装各式外部天线，根据实际需要来调整覆盖范围或信号品质。有些基站已经开始采用相当先进的天线技术，允许以非常精密的方式控制传输样式，或者让好几颗 MAC 芯片共用单一天线。传输功率通常可以任意调整，以便扩大或缩小覆盖范围。有些企业级基站甚至可以使用单一天线支持多组虚拟无线网络。
- 除了可以调整无线电波，企业级基站也支持某种型式的虚拟基站。只要设置多组 SSID，就可以指定个别 SSID 的身份认证与加密配置。这项功能通常用来建立安全层级不同的平行网络，除了可以容纳老旧设备，也可以为新式设备提供最高的安全性。
- 企业级基站原本就是设计来整合到现有网络。在安全性方面，意味着它们必须整合到既有的安全架构，通常是安插到现有的使用者数据库。当使用者成功通过网络的身份认证，就可以充份利用网络所提供的服务。第二个整合点，就是企业级基站用来延伸有线网络既有访问控制与使用者权限的方式。
- 整合到既有网络的同时，也扩展了整个数据平面（data plane）。大多数企业级基站可以根据身份认证服务器所提供的使用者属性，动态指定虚拟局域网络（VLAN）。

- 通常，企业级产品会附带 **site survey**（实地探勘）工具，网络管理人员可以根据涵盖范围的信号品质来规划大型的部署计划。这些工具的复杂程度不一。有些只能提供一些历史统计数据，有些则是十分先进，可以从实际环境中勾勒出网络分布图。
- 为符合管理上的需要，企业级设备的配置设置，通常是通过简易的命令列界面或 **SNMP**，而其监控与管理机制也较家用闸道器来得完备。有些产品也可以整合到大型管理架构当中，如此一来，只需要一位网管人员就能够监控与设置数以百计甚至数以千计的基站。
- 企业闸道器通常是整批部署。任何摆设都必须符合办公空间对于美观上的要求，因此这些设备通常提供较具弹性的摆设方式。有些是设计成附挂于天花板之上，而且符合防火等级（**plenum rated**）【注】。为了安全上的考虑，安装于气流导管（**air ducts**）与空调场所（**air-handling spaces**）的设备均得符合严格的排烟规定。防火等级的基站几乎可以安装在任何场所，未取得相关认证的产品就只能安装在某些特定区域。

不过，天下没有白吃的午餐。大多数企业级基站的价格通常介于 500 至 1,000 美元之间，虽然通常会有不少折扣。过去一段时间，高档基站的价格的确有所滑落，但不像家用产品一般有降价压力。**Cisco 1200** 与 **Cisco 1100** 是企业级基站中比较经典的款式。两者均使用比较通用的硬件，搭载完整版的 **Internetwork Operating System**，每隔一段时间就会加入新的功能。**Proxim**、**Symbol**、**3Com** 以及 **HP** 均提供具备类似功能的竞争性产品。

20.1 .1.3 大型商用机种：无线交换器

本书第一版问世以来，最大的变化就是「无线交换器」（**wireless switch**）或「精简型基站」（**thin AP**）架构的出现。在此架构中，功能比较简单的几部轻量级基站由一部中央交换器加以控制。之所以会发展精简型基站或无线交换器架构，是为了提供比第一代产品更好的效率。更好的效率，部分来自所使用的技术本身。精简型基站架构将处理过程从基站抽离，交由专职设备全权负责。从基站移除处理过程意味着移除基站的零件，因此降低了基站的成本，也增加了基站的使用年限。如果一并移除基站的配置设置，就可以进一步减少需要管理的网络设备。

将功能集中在控制器也同时提高了弹性。以同样的成本，将硬件集中于控制器可以提供更强大的处理能力，何必将资源分散给基站处理。通过各基站间的协调，网管人员可以平衡各基站的流量负载。集中监控无线电波的运作情形以及轻易扩充现有的网络功能。

以无线交换器做为解决方案的成本，绝大部分取决于网络规模的大小。大多数厂商斗出各种不同款式的控制器，能够控管几部甚至数百部基站。最早推出的解决方案众州 **Symbol** 的 **Mobius** 无线交换器。后续推出解决方案的厂商，包括 **Airespace**、**Aruba**、以及 **Trapeze**。

20.2 以 Ethernet 供电（PoE）

如果希望网络的规模可大可小，以 **Ethernet** 供电（**PoE over Ethernet**，简称 **PoE**）就极为重要。设计无线网络时应该以无线电波传播（而不是以电源供应）的角度来考量基站的摆设位置。

第一波销售的基站与其他计算设备采用同样的供电方式，亦即将电源线插入最近的 **AC** 电源插座。糟糕的是，有些产品所使用的变压器居然会挡到隔壁的插座。基站的摆设受制于附近是否有电源插座，而不是考虑哪些地点能够提供最佳的服务。如果限制必须靠近电源，基站的位置变更就不是那么容易。

由于电气方面的过程有其危险性，有些地方的法律规定必须聘请合格的技师。有些机构也会与工会协商，要求提供有经验的电工。这时候，变更基站的摆设位置就可能所费不菲。有些地方，Ethernet 之类的数据线由网络技术人员拆装即可，因此基站可以由非工会成员进行安装或变更摆设地点。【注】

20.2.1 PoE 的种类

市面上有各种不同的电源设备，其中有许多符合 IEEE 802.3af 标准。8023.af 所定义的传输标准，可以在整段 Ethernet 缆线中供应 48 伏特的直流电，最高可达 15 瓦。这份标准可以从 IEEE Get802 网站下载，进一步的信息可至 <http://www.poweroverethernetcom/> 取得。

最基本的差别在于，通过 Ethernet 缆线中的哪几对线供电。数据通常是通过数据线传送（第 1、2 对和第 3、6 对线）。标准中，A 版本以数据线供电，而 B 版本则是通过其他未使用的（第 4、5 对和第 7、8 对）线供电。以数据线供电时，正负极有两种配置方式，如图 20-1 所示。脚位的安排如表 20-1 所示。以非数据线供电必须使用特定的极性。并非所有厂商均使用第一对线当作正极，值得一提的是除了 Cisco 早期的专属电源设备，其所定义的极性只供自家设备使用。

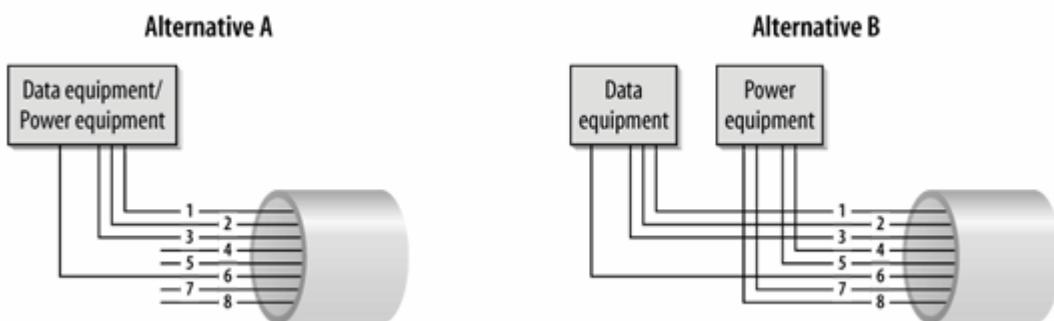


图 20-1：电源线路图

Wire number	Pair mapping	Alternative A (MDI-X)	Alternative A (MDI)	Alternative B
1	1 - data	-	+	
2	1 - data	-	+	
3	2 - data	+	-	
4	3 (unused)			+
5	3 (unused)			+
6	2 - data	+	-	
7	4 (unused)			-
8	4 (unused)			-

表 20-1 802.3af 的线路定义

电源设备的种类，可以根据电源供应的角度做进一步区分。电源设备如果内建于交换器，就称为终端（endpoint）电源。另一种方式，使用灌电器（power injector）来提供电力，称作中介

(mid-span) 设备。目前大多数 802.11 网络部署均使用灌电器或所谓的中介设备。如果交换器厂商所生产的电源设备(power blade)得到更广泛的使用，终端供电就会更加普及。图 20-2 显示了两种不同的选项。中介式选项的灌电器可以是独立设备，也可以是具有好几个供电埠的「电源插线面板」(power patchpanel)。Gigabit 数据链路只能使用终端供电，虽然这对 802.11 而言尚无重大影响。

802.3af 提供电源检测机制，可避免烧毁插入供电埠的设备。早期的 PoE 设备随时提供满载电压，规格不符的设备可能因此烧毁。为了顾及安全，802.3af 提供了一种磋商机制，可以逐步提升电压。如果初次检测得不到任何反应，就会停止供电以保护终端设备。

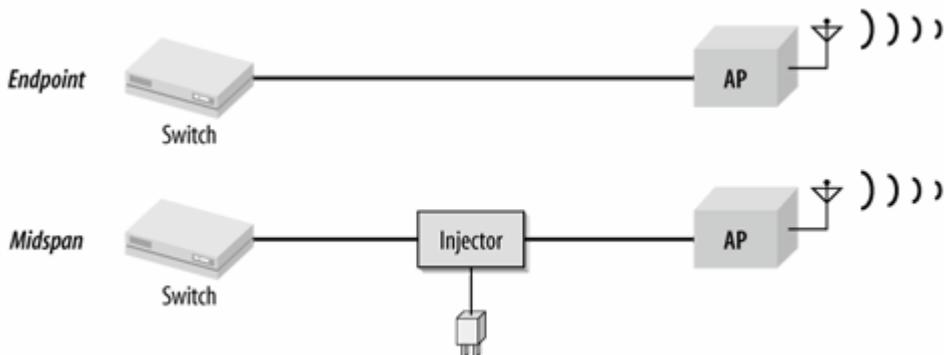


图 20-2：终端电源与中介灌电器

灌电器通常配备两个 Ethernet 埠以及一条电源线。其中一个 Ethernet 埠连接网络，第二个 Ethernet 埠则为之供电。值得一提的例外是 Cisco 的 AIR-PWRINJ-FIB，它使用 Ethernet 埠供电，但以 100BASE-FX 光纤做为网络连接。

20.3 选购基站

选购基站时，必须将一些因素纳入考虑。随着 802.11 成为主要标准，是否符合标准已经不再是主要考虑因素。任何打算组建大型网络的厂商都必须提供符合目前所有标准的相容性，而且通常需要承诺支持未来制定的重要标准。有些机构已经推出测试方案来验证互通性。其中最著名的就是 Wi-Fi 联盟的 Wi-Fi 认证，虽然其他机构眼见无线局域网络逐渐普及，也推出类似方案与之争食这块大饼。目前业界最严谨的测试方案是由 New Hampshire 大学的互通性实验室 (Inter-Operability Lab，简称 IOL) 所推行。IOL 的测试方案不如其他商业性测试方案出名，因为它的目的是协助开发更好的产品，而不是提供行销上的「认可标章」(seal of approval) 给厂商。如同以往，研究认证方案时，最好确定厂商已经通过你所感兴趣的相关测试。

部署无线网络时，安全性通常是主要的考虑重点。既然 WEP 已遭彻底破解，在选购基站时最好确定它支持 802.1X 与 802.11i 安全功能。小型网络部署可以使用预设共享密钥身份认证，不过比较侧重安全性的网络部署就应该采用完整的 RADIUS 整合方案。在比较大型的环境中，选用能够提供多部虚拟基站，同时允许不同加密与身份认证组合的产品，或许比较值得。

有时候，如何供电给基站是部署时会遇到的头痛问题。为了涵盖较大的范围，通常必须将基站置于电源所不及之处。使用较长的天线可能使信号品质降至可接受的水准以下，因此最好还是就地提供电源。安装新的电源插座通常十分昂贵。这些工作必须由合格的技师完成，况且建筑消防法规也有额外的限制。有些产品可以通过 Ethernet 缆线提供电力。较便宜的产品通常使用

专属的电源设备，价格较高的产品则是使用符合标准的电源设备。网线没有电源线那么多限制，网管人员可以自行布线。

有时候，使用环境同时包含室内与户外场所。要在一个区域提供密度较高的覆盖率，外接天线通常可以派上用场。不过并非所有基站均可外接天线，因为必须付出额外的成本。就算基站配备外接天线接头，也无法保证可以找到适合的天线。**802.11** 只规范外接天线的转接头必须具备 **50 ohms** 的标准阻抗。如果外接天线对整个部署计划而言十分重要，最好确定有足够类型的天线可供使用，不论其来自 **802.11** 厂商或其他来源。户外安装通常需要使用「耐候：**(environmental** 寸"hardened") 的基站，或同时以耐候材料包覆。

检验基站需要符合哪些条件时，也必须将环境因素纳入考虑。安装于空调场所的设备必须符合防火等级。认证时会在受测设备上点火，然后检测所产生的烟雾浓度。浓烟可能会通过通风系统与管线弥漫到整座建筑物，遮蔽紧急出口标示且造成伤亡。防火等级设备所采用的材料不会产生浓烟。而烟雾通常容易造成危险。防火等级的基站之所以比较安全，是因为不致于产生浓烟遮蔽出口，而不是因为它的烟雾不具毒性。安装在天花板上面的设备通常不需符合防火等级，除非天花板上方就是换气口。配备气流导管的建筑物通常不必使用防火等级的基站 **1** 但有些建筑检验单位可能会误认有此必要。有些地区的建筑法规的确有此要求。

如果漫游十分重要，就必须从不同技术与做法中挑选合适的解决方案，因为不同厂商提供的产品之间或许无法顺利漫游。确保各家产品互通性的最佳方式，就是选购以「动态 **VLAN** 指定：**(dynamic VLAN assignment)** 做为漫游与换手（**handoff**）基础的系统・工作站进行身份认证时，将可以通过相同的「逻辑附接点：**(logical point of attachment)** 连接至网络。

802.11 在标准中包含了一些省电功能。这些功能绝大部分不具强制性。如果在部署上，主要是使用以电池供电的设备，最好评估一下该设备提供了哪些省电功能。此外，最好先试试看，如果启用省电功能，电池可以持续多久时间。

设备管理也必须加以考虑。无线网络属于新的服务，对于新的硬件，网络人员必须加以规划、评估、采购、部署以及维护。大型部署可能会用到数十甚至数百部基站，若无适当工具，对网络管理而言将是一项头痛的问题。厂商是否提供基站管理工具，可以批次设置许多设备？基站的管理，是否能够整合到现有的网管基础架构中，以便使用已部署完成的工具？这些管理工具是否够安全？许多产品只能够以明文临定（**clear-text protocols**）加以管理，这无疑会危及或违反目前既定的安全政策・经验显示，网络设备软件升级十分频繁。那么，软件该如何升级，升级又可以提供多少功能？新的协议功能是否能够通过韧体加以升级？在采购之前，可以根据部署的规模加以评估。看看自己是否可以承受每部基站所能覆盖的范围，使用一些常见的网卡加以测试。**802.11** 网络的负载能力完全取决于无线链路，不过你或许希望确定是否有其他的负载限制。如果败用安全性协议，基站是否能够提供最大的负载能力？有些产品针对所有协议提供加密加速机制(**cryptographic acceleration**)，有些则无。仅靠单一加密处理器执行安全系统的产品，在升级至较快的物理层标准后，或许会不敷使用，也有可能受限于上链频宽。目前 **Fast Ethernet** 虽然能够应付 **802.11a/g** 网络所需，不过未来就可能成为 **802.11n** 标准的瓶颈・试着架设一个测试网络，感受一下如果要将基站整合至现有网络，应该如何配置。

和所有采购决策一样，有些「软件：因素是不容易量化的。产品的保证。与厂商的关系，以及技术支持的品质，种种因素都会影响到购买的决策。软件因素既不属于技术层面，也不容易量化，在此不予以置评。

20.3.1 真的需要基站吗？

无线网络不见得需要配置基站。无线工作站可以彼此形成独立型网络，根本用不着基站·组建一部 Unix 机器，做为 Ethernet 与无线网络间的路由，并不困难，况且所需要的硬件可以从旧机器堆中回收使用。那么，为什么要用基站呢？

既然家用闸道器的价格已经跌破 100 美元，对只需单一基站的网络而言，组建一台 Unix 路由器已经不符成本效益·只要想想必须花费多少工时成本，就知道组建一部 Unix 路由器算不算是浪费·何况，基站的硬件与通用型平台相比亦有其优点。基站设备较小，' 但无其他琐碎零件。‘因此，它们所耗费的电力较少，也不会产生多少热量。Apple 所提供的「软件基站」(software base station) 算是例外，它可以将任何桌上型电脑转变为桥接用的基站。只要稍加设置，一部桌上型电脑摇身一变就可以成为基站。

以 Unix 主机充当路由器，在较大型的部署上不具效率，主要是因为无法支持移动性。有效的漫游需要通过桥接（而非路由）来访问不同地理位置的链路层。不过，在 802.11 中，除非基站之间能够彼此沟通，藉此追踪无线工作站的行踪，否则也无法提供漫游。未来，或许会出现开放源码的 Unix 套件，可以提供基站所有功能：访问 802.11 网卡之基本参数的低价能力。Ethernet 桥接能力，以及 IAPP。在此之前，商用等级产品还是无可替代的。

Unix-Based 基站

打造一部 Unix-based 塞地台的先决条件之一。就是放动无线网卡上的基站功能。其中一项困难所在，就是必须重写 802.11 标头。在基础型网络(infrastructure network) 上，所有流量均会流经塞地台。基站必须重写 802.11 标头中的传送端与接收端的位址。此外，可能还会用到其他的管理功能。举例而万，802.11 规格包含了基础型网络所使用的一些省电机制。不过必须通过基站实现，方能使用这些功能。

此外，还有一些非技术性的障碍。有些厂商会十分积极，相当支持自家网卡之 Unix 开放源码驱动程序的阁香工作。毕竟，厂商是通过销售硬件获利，可以将网卡销售给所有的用户系统当然是件好事，就算使用在闭放源码的 Unix 平台上亦然。不过，基站则不然。厂商们通常不鼓励支持将网卡变更为塞地台模式的界面。基站比较有利可图。如果为网卡提供驱动程序界面，使之可以支持塞地台的功能，无疑会妨碍塞地台的销售。

就某些方面而言，要将采用 Intersil 品片组的网卡转变为塞地台，惟一的方式是向 Intersil 购买公版。（此公版附带具备选地台功能的韧体，而该韧体并未分闭销售。）Intersil 所销售的工作站韧体，当中的确包含所谓的「Host APMode：（仿 AP 模式）。在此模式下，PRISM-2 品片组会自动处理一些，低价的 J 工作，例如传送 Beacon 帧及回应 Beacon 帧。Jouni Malinen 所闭发的驱动程序，可以在 Linux kernel 2.4 中使用 Host AP Mode。连同核心所实现的 Ethernet 桥接功能，此驱动程序可用来建构一部基站该驱动程序可自 <http://www.epitest.fi/Prism2/> 下载。

以驱动程序目前的现况而言，建构一部 Unix-based 路由器不无可能。（在此，我学术性地称 h 路由器：为「第三层网络设备」。）其中一个界面可像以往般连接至有线网络，而第二个无线界面可用 IBSS 模式执行。Ross Finlayson 利用一部 FreeBSD-based 的路由器，已经在加州 Mountain View 一家咖啡馆中组建了一套社区网络。该专案的网址为 <http://www.dive.co/mldanastreet/>，该路由器也有专属的网页 <http://www.lave.co/m/u,iredess/unax-base-station.html>。

20.4 Cisco 1200 基站

Cisco 1200 系列基站是独立式 (standalone) 基站的典型代表。它所执行的是 Cisco 的 IOS 过程系统。1200 系列原本采用的是基于 VxWorks 的系统，不过后来 Cisco 岭行了 IOS，可用来

升级 1200。升级工具可以从 Cisco 的网站下载。目前 VxWorks 的版本已经停止开岭，也不再增加新的功能。

Cisco 1200 可以通过 web 界面或 LOS 命令列界面单独设置。设备数较多的话，则可以通过 Wireless LAN Solutions Engine（简称 WLSE）进行管理。通过一条使用 Cisco RJ-45 脚位的序列缆线，就可以进入命令列界面，或者等到网络界面就绪后，以 telnet 或 et 或 SSH 登入。

20.4.1 设置 1200 基站

1200 的硬件设置十分简单。它可以使用本身的电源供应器（power supply）或者 Cisco 专用的灌电器（power injector），两者的电路相同。电源供应器的输出为 48 伏特，和灌电器一样。

1200 使用了一个「桥接一群组虚拟界面」（Bridge-group Virtual Interface，简称 BVI）。BVI 是 IOS 所使用的一种软件功能（construct），可以通过同一个界面绕送（routing）与桥接（bridging）不同协议。基站需要将 802.11 帧桥送到 802.3，但也需要绕送 IP 封包进行管理过程，因此 BVI 就成为理所当然的选择。必须在全域配置提示符号（global configuration prompt）底下方能设置 BVI 的 IP 位址。基站的 IP 位址可以手动指定，也可以通过内建的 DHCP 用户端程序取得：

```
ap1200# configure terminal
ap1200 (config) # interface BVI1
ap1200 (config-if) # ip address 192. 168. 1. 5 255. 255. 255. 0
ap1200(config-if)# ip address dhcp client-id FastEthernet0
```

要检查界面的状态以及确认是否已经指定位址，可以使用 show ip interface 命令：

```
ap1200# show ip interface brief
Interface IP-Address OK? Method Status Protocol
Dot1Radio0 unassigned YES TFTP up up
FastEthernet0 unassigned YES NVRAM up up
Virtual-Dot1IRadio0 unassigned YES TFTP down down
BVI 192 . 168.5 ‘191 YES DHCP up up
```

20.4.2 无线界面的配置设置

1200 配备两个无线界面。Radio 0 为 2.4 GHz，通常使用 802.11b，不过较旧的机种可能还是使用 802.11b。Radio 1 则是 5 GHz。每个界面均可使用界面配置设置命令分别加以设置。“数据率（传输率）”可以只用 speed 命令来设置，或者加上 basic 一前置词。在下面的范例中，第一个 speed 命令允许使用所有数据率。第二个命令指定 1Mbps 与 2 Mbps 过程为必要，但也允许 5.5 Mbps 与 11 Mbps 过程。最后两个命令比较特别。speed range 允许使用所有数据率，不过只有最低速率必要。speedthroughput 会将所有数据率设为必要。

```
ap1200# configure terminal
ap1200 (config) # interface dot1IRadio 0
ap1200 (config-if) # speed 1, 0 2, 0 5. 5 11. 0
ap1200 (config-if) # speed basic-1. 0 basic-2. 0 5. 5 11. 0
ap1200(config-if)# speed range
ap1200 (config-if) # speed throughput
```

以 milliwatts (毫瓦) 为单位设置「本网最大功率」 (local maximum power) 即可为每个界面进行传输功率配置设置。和传输率一样, power 这个命令会因界面而异。802.11 b/g 界面最高只允许使用 100 MW 的功率。由于 OPDM 芯片设计上的限制, 802.11a 界面最高只能够设置到搜 0 MW。

```
ap1200# configure terminal  
ap1200 (config) # interface dot1radio 0  
ap1200 (config-if) # power local 100
```

除了功率设置, 还可以使用 channel 命令为每个界面设置过程频道。channel 之后必须提供以 MHz 为单位的频率做为参数。另外一种做法, 是在 channel 命令之后键入 least-congested 关键字, 让基站自行挑选最干净的频道。

```
ap1200# configure terminal  
ap1200 (config-if) # interface dot1radio 0  
ap1200 (config-if) # channel 2412  
ap1200 (config-if) # channel least-congested
```

基站可以使用两种 802.11b 同步信号。长同步信号相容性较高, 不过短同步信号效能较佳。一般而言, 应该将这个选项设为 short, 除非网络中存在一些老旧设备。要停用短同步信号, 可以使用 no preamble-short 界面命令。

```
ap1200# configure terminal  
ap1200 (config) # interface dot1radio 0  
ap1200 (config-if) # no preamble-short
```

Beacon 帧系用来宣告网络的存在, DTIM 信息元素则是用来宣告有暂存帧。透巡 Beacon 帧间隔的微调, 可以在暂存帧的传送与电池的消耗之间找出平衡点, beacon period 与 beacon dtim-period 命令的用法如下:

```
ap1200# configure terminal  
ap1200 (config) # interface dot1radio 0  
ap1200 (config-if) # beacon period 100  
ap1200 (config-if) # beacon dtim-period 5
```

除了 Beacon 帧间隔, 也可以设置 RTS/CTS 门槛值。较低的设置值将导致 RTS/CTS 碰商程序开始进行。根据所处的环境, 以下面的命令来调整帧的重传次数或是进行帧切割的门槛值, 可能会有所帮助:

```
ap1200# configure terminal  
ap1200 (config) # interface dot1radio 0  
ap1200 (config-if) # its threshold 2000  
ap1200 (config-if) # its retries 2  
ap1200 (config-if) # packet retries 8  
ap1200 (config-if) # fragment-threshold 1500
```

20.4.2.1 网络互连

不同用户端将会以不同的方式封装帧。到目前为止，最常被使用的是 RFC 1042 所规范的 SNAP 分封格式，这是本基站的预设值。IOS 也允许使用 802.1H。这个设置只能针对无线界面做全域设置，无法针对个别协议。

```
ap1200# configure terminal
ap1200 (config) # interface dot1lradi0 0
ap1200 (config-if) # payload-encapsulation snap
ap1200 (config-if) # payload-encapsulation dot1h
```

随着「动态 VLAN 指定」(dynamic VLAN assignment) 的出现，在有线网络使用 VLAN 已经日渐普遍。1200 的 IOS 同时支持原生 (native) 与标记式 (tagged) VLAN。重点在于必须在相同的 IP 网络中，将 VLAN 1 (即 native VLAN) 指定给网络上其他设备，以确保能够通过所谓的 native VLAN 进行传输。要指定 nativeVLAN，可以在子界面的 encapsulation 命令之后加上 native 关键字。

```
ap1200# configure terminal
ap1200 (config) # interface dot1lradi0 0. 1
ap1200 (config-subif) # encapsulation dot1q 1 native
ap1200 (config-subif) # interface fastethernet 0. 1
ap1200 (config-subif) # encapsulation dot1q 1 native
```

其他的 VLAN 可以用同样的方式来设置，但省略掉 native 这个关键字。常见的做法是使用子界面编号做为 VLAN tag 举例而言，要设置 VLAN 70 可以用下面的命令。要设置 VLAN 20，只要将 10 置换成 20 即可。

```
ap1200# configure terminal
ap1200 (config) # interface dot1lradi0 0. 10
ap1200 (config-subif) # encapsulation dot1q 10
ap1200 (config-subif) # interface fastethernet 0. 10
ap1200 (config-subif) # encapsulation dot1q 10
```

20.4.3 安全性的配置设置

基站所广播的 SSID，代表无线网络。在 1200 中，每个 SSID 就代表一部独立运作的虚拟基站。每个 SSID 均有自己的安全性配置设置，以及自己的 VLAN 对映方式(VLAN mapping)。值得注意的是，这些 VLAN 的对映方式显得有些拖泥带水。预设的 VLAN 可以被指派给 SSID。如果所使用的 RADIUS 服务器传回不同的 VLAN，用户端设备将会被重新对映到所指定的 VLAN。

【注】不过，只有当 RADIUS 服务器完全不提供任何 VLAN 时，才会使用这种指派给每个 SSID 的预设值。(这种做法不如市面上其他产品来得乾淨，亦即若非使用预设 VLAN，就是由 RADIUS 服务器提供。)

每个 SSID 的身份认证系使用 authentication 命令进行配置设置。一般而言，这个命令会将身份认证的方式设置为「开放」(open)，但可能会加上 EAP 做为认证方式选项。下列命令会把名为 babefish 的 SSID 对映到 VLAN 42，并且要求对服务器群组 rad_eap 进行 EAP 身份认证。

```

ap1200# configure terminal
ap1200 (config) # interface dot11radio 0
ap1200 (config-if) # ssid babelfish
ap1200 (config-ssid) # vlan 42
ap1200(config-ssid)# authentication open eap rad eap

```

要定义用来进行 EAP 身份认证的 RADIUS 服务器，首先得指定有哪些服务器，然后将它们加入一个群组。预设上，如果没有指定 UDP 埠，RADIUS 服务器就会使用旧式的 RADIUS 埠(1645 与 1646)，因此必须加以指定，才能使用新的埠号。

```

ap1200# configure terminal
ap1200(config)# radius-server host 192.168.200.187 auth-port 1645 acct-port 1646
key MySecret
ap1200(config)# radius-server host 192.168.200.188 auth-port 1812 acct-port 1813
key MySecret
ap1200 (config)# aaa group server radius rad_eap
ap1200 (config-sg-radius) # server 192. 168. 200. 187 1645 acct-port 1646
ap1200 (config-sg-radius) # server 192. 168. 200. 188 1812 acct-port 1813

```

20.4.3.1 WPA-PSK 的配置设置

WPA 预设共享密钥系通过 SSID 命令来设置。以 SSID 命令设置好 WPA 密钥管理以能后，就可以指定 WPA 所使用的 ASCII 或十六进制预设共享密钥。

```

ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid-LuminiferousEther
ap1200 (config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii Thisisaverylongsecretsharedkey!

```

20.4.4 监控

欲列出所有已连接的工作站，可以在一般提示符号之下键入如下的命令（这是一项基本的监控工具）：

```

ap1200> show dot11 association
802.11 Client Stations on Dot11Radio0:
SSID 「LuminiferousEther」 :
MAC Address IP address Device Name Parent State
0002.2d6e.abda 192.168.200.150 — self Assoc

```

要查看特定连接的详细数据，可以指定对方的 MAC 位址。如此就会列出完整的连接纪录，包括所使用的加密方式。下面这部已连接的工作站，以 TKIP 做为加密的方式：

```

ap1200>show dot11 association 0002.2d6e.abda
Address: 0002.2d6e.abda Name:
IP Address: 192 . 168. 200. 150 Interface: Dot11Radio 0
Device: — Software Version:

```



CCX Version:
State: Assoc Parent: self
SSID: LuminiferousEther VLAN: 0
Hops to Infra: 1 Association Id: 120
Clients Associated: 0 Repeaters associated: 0
Tunnel Address: 0 . 0 . 0 . 0
Key Mgmt type: WPA PSK Encryption: TKIP
Current Rate: 11 . 0 Capability:
Supported Rates: 1.0 2.0 5, 5 11.0
Signal Strength: -39 dBm Connected for: 1463 seconds
Signal Quality: 79% Activity Timeout: 55 seconds
Power-save: Off Last Activity: 4 seconds ago
Packets Input: 535 Packets Output: 245
Bytes Input: 61629 Bytes Output: 137018
Duplicates Rcvd: 0 Data Retries: 18
Decryption Failed: 0 RTS Retries: 0
MIC Failed: 0
MIC Missing: 0

20.4.5 障碍排除

IDS 提供了一些额外的排错工具，可用来排除问题。**debug** 命令用来启用追踪功能，其后可以指定所要追踪的对象。追踪讯息预设会被送到操控台（console）。如果通过网络连上基站，就必须以如下的命令将排错讯息导向目前的登入画面：

```
ap1200# terminal monitor
```

采取安全防护措施的 802.11 网络最容易出现问题的地方，就是一开始的连接与密钥传递阶段。这些问题的障碍排除可以通过 **debug dot11** 以及相关副命令来达成。一些常用的「障碍排除」排错命令如表 20-2 所示。

Debug area	Commands	Remarks
EAP authentication	debug radius authentication	
	debug dot11 aaa authenticator process	Prints out RADIUS packets; decodes attributes; explains actions
	debug dot11 aaa authenticator state-machine	May show servers timeout or fail
MAC filtering	debug dot11 aaa authenticator mac-authen	Shows MAC addresses and response from authentication system
	debug dot11 aaa authenticator process	
	debug dot11 aaa authenticator state-machine	Shows key exchange
WPA	debug dot11 aaa manager keys	

表 20-2: Cisco 1200 排错命令

关闭排错功能十分简单。只要键入如下命令即可：

```
ap1200# undebug all
```

20.5 Apple AirPort 基站

目前 Apple 在市面上推出了 **AirPort Express** 与 **AirPort Extreme** 两款基站，两州均采用 802.11g 规格。**AirPort Extreme** 在设计上比较像是家用闸道器，而且具有个数据机埠与外部天线接头。虽然价格比市面上其他产品高出不少，但它的功能较多，得到许多小型办公室的青睐。

20.5.1 初次设置

和设置新的无线界面配置一样，初次设置也是使用同一套 **AirPort Setup Assistant** 应用程序线参数。**AirPort** 基站会对外宣告本身的存在，因此 **Mac OS** 用户端可据以设置迎。连接到 **AirPort** 基站并且点选配置设置画面后，网络安全性设置画面。图中的配置设置画面显示目前采用性设置。如要设置 **WEP** 配置，同样是通过这个画面。



图 20-3：网络安全设置

20.5.2 管理界面

一旦以 **Setup Assistant** 完成初次配置设置, **AirPort** 基站便会在网络上, 此时必须以 **AirPort Utility** (图 20-4) 加以设置。这是另外一套设置工具, 如果看过 **Lucent** 的 **AP Manager**, 必然会感到相当熟悉。程序开始执行后, **AirPort AdminUtility** 会搜寻网络中所有 **AirPort** 基站, 并且以列表方式显示。只要挑选个别的基站, 就可以进一步加以设置或配置变更之后, 基站必须重新启动, 变更才会生效。上方所显示的 **Other** 按钮可用来设置任何的 **AirPort** 基站, 只要管理人员能够送出 IP 封包至该基站。距离较远的基站可能不会出现在列表中, 不过只要点选 **Other** 按钮同时键入 IP 位址, 即可设置任何以 IP 相连的基站。

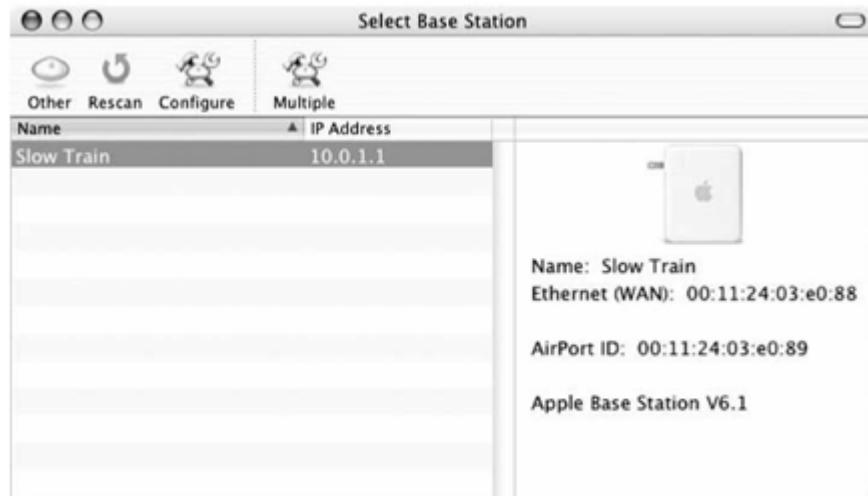


图 20-4：AirPort Admin Utility 主画面

2 0.5.2.1 设置无线界面

为所选定的基站进行配置设置时，就会出现配置设置画面。配置信息以标签页（tab）区分为各种逻辑单元，预设会选用无线界面配置设置（wireless interface configuration）标签页。画面上方，有一些按钮可用来重新启动基站（Restart）、更新韧体（Upload）、还原出厂设置（Default）以及更改密码（Password）。 （新韧体通常随 Admin Utility 套件一起发行，如果管理软件发现有新的版本，就会自动进行韧体升级。）

AirPort 的配置设置程序如图 20-5 所示。安全性设置类似之前图 20-3 所显示的画面。“closed network”选项会移除 Beacon 帧中的 SSID 信息元素，想要连接到网络的工作站必须自行指定。这个有点像是消遣性质的安全性选项（toy security option），因为它并无法提供真正的封闭式网络。既然同时支持 802.11b 与 802.1，因此可以将它设置为 b/g 相容模式，或者禁止使用 802.11b 设备以避免防护机制所带来的负担。



图 20-5：无线界面的配置设置

20.5.2.2 设置 LAN 界面的配置

AirPort 可以当做 NAT 设备使用，这时候它会把来自无线设备的 IP 数据转译为它的 Ethernet 界面位址。管理人员可以手动为其他工作站设置静态位址，或以内建的 DHCP 服务器，将特定范围中的位址分配给其他工作站。当 NAT 被用来让多部电脑使用同一个 IP 位址时，Internet 选

项所指定的位址就会被当做对外的公开位址。有线局域网络界面的位址会被设置为不对外公开的私有位址 10.0.1.1，而 DHCP 所释出的私有位址介于 10.0.1.2 与 10.0.1.200 之间（在这种情况下，无法手动指定 DHCP 服务器所分配的位址范围）。如果不使用 DHCP 服务器，AirPort 基站可以使用内建的 Fast Ethernet LAN 埠连接至有线网络。

如图 20-6 所示的 Port Mapping 标签页可用来新增内送(inbound)的静态连接埠对映关系。公开的埠号会被转译至私有 IP 位址与相应的埠号。本图所显示的位址转换，是将内送的 web 服务转送至 10.0.1.201 主机上的 80 埠。

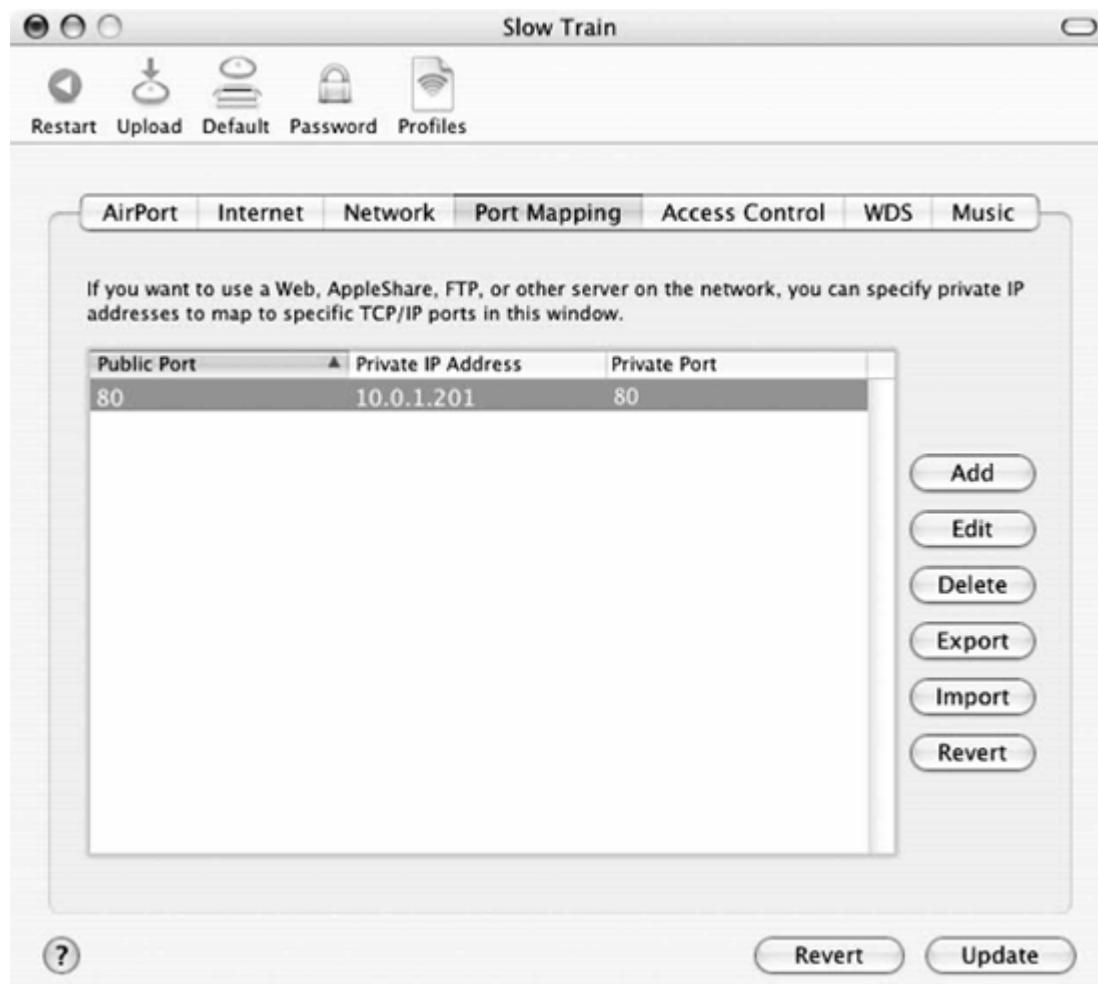


图 20-6：Port Mapping 标签页

20.5.2.3 访问控制

和大部分其他的产品一样，AirPort 基站也支持 MAC 位址过滤的功能。AccessControl 标签页可通过 Airport ID (MAC 位址) 来辨认工作站，请将之列入允许访问的工作站列表，并且填入工作站相关描述。

第21 章 无线网络逻辑架构

无线局域网络的安装规划并不简单，因为横跨许多原本毫不相干的学科。本章会先从网络架构的角度探讨无线局域网络的部署。网络设计就是在几个因素之间作取舍，包括成本 (cost)、可管理性 (manageability)、可用性 (availability) 与性能 (performance)。至于无线网络，另外得将移动性 mobility) 纳入考虑。

无线网络通常是通常是现存有线基础设施的延伸。有线基础设施或许十分复杂，特别是幅员涵盖工作园区里好几座建筑时。无线网络必须以牢靠、稳定、设计完备的有线网络为基础。如果既有网络不够稳定，无线部分也必然岌岌可危。

本章主要探讨组建无线局域网络的四种做法。本章将从技术的观点，探讨足以影响网络设计的无线局域网络功能。无线局域网络的功能如何影响网络拓扑？除了 802.11 设备，部署网络时还需要哪些器材？如何让逻辑网络的移动性达到极致？

21.1 评估逻辑架构

详细列举各种网络拓扑之前，让我们先来探讨如何评估网络组建方案。本章所提到的网络拓扑各有其优缺点。网络拓扑的选择，取决于几个决定性因素。以下是我认为比较重要的评估因素。

21.1.1 移动性

可移动性 (portability) 能够提高生产力，因为方便使用者随处访问信息。不过，可移动性只免除了连接的实体限制。膝上型电脑方便带着四处游走，因此有很多人这么做。不过到达新地点后，仍然必须重新连接。实际连接的动作还是无可避免，何况设备一经移动，原本的网络连接就无法使用了。

举例而言，挂载远端的文档系统后，让膝上型电脑进入休眠状态。带至别处唤醒膝上型电脑后，该文档系统已经不存在。必须等到之前开启的文档或过程超时，才有办法重新取得电脑的控制权。DHCP 用户端可能造成更常见的限制。一般 DHCP 用户端在更新租期时，会尝试取得之前所使用的地址，因此可能要进行好几回合的 DHCP 交换程序，才有办法在新的 IP 子网络上取得地址。

相较之下，移动性就较具威力。移动性进一步移除了许多限制，主要是由逻辑网络架构着手。就算设备正在移动，网络连接也不会因此中断。这对需要一致而持续之连接的应用来说特别重要，例如数据库的应用。服务人员经常会访问登入了问题与解决方案的追踪数据库 (tracking database)。对于医疗院所使用的追踪软件而言亦然。通过无线网络访问数据库可以提高生产力。如此一来，位于不同地点的使用者均可就地新增信息，用不着每次都与数据库重新连接。另外一个例子是库存应用，这也是为什么零售业 (retail) 与物流业 (logistics) 是率先采用 802.11 的市场。以库存应用为例，就地计算产品或包装盒数量，然后将数据通过无线网络传回，比起先

将数据记录在纸上，然后再登入数据来得合理。【注】事实上，无线局域网络技术的早期使用者主要是行动医疗，物流与教育方面的机构。

传统的有线 Ethernet 只能够提供可移动性。使用者可以带着膝上型电脑至园区各地，然后插上网线。（如果愿意忍受低速连接，甚至可以从世界各地拨接回公司网络。）不过，每次访问网络时，都必须从头开始。就算只移动了几尺，也必须重新建立连接。然而使用者所期盼的是，每当走进会议室时，不需任何动作即可连上公司网络。

21.1.1.1 移动性的定义

无线网络与移动性密不可分。缺乏移动性，人们就不会对无线网络特别感兴趣。移动性意味着不论电脑位于何处，应用程序就是能够运作。遗憾的是，要组建不受空间限制的网络，需要具备相当多的知识以及设置不少与区位相关的配置。

要将移动性从高层的定义落实为技术细节，有几种不同的方式。有些技术可以为网络使用者提供移动性，但并非所有技术均能带来好处。要提供真正『不须人为介入』（transparent）与『不受应用限制』（independent of application）的网络传输，必须满足下列条件。

1、一致的链路层连接。要具备移动性，现有的数据链路层必须不受区位（location）的影响。通过若干额外的工程，便可以在 802.11 中提供链路层的移动性。

a. 基站间的自动换手（transparent handoff）。使用者或许还是必须设置一开始的配置并选择某个网络加入，但不必参与换手的决定。如果信号强度过低，内建的软件必须能够自动寻找更强的信号进行移转，不需要使用者介入。目前，几乎所有网卡均可在同一个网络的基站间进行切换。802.11 在设计之初即考虑到此项需求，各位所购买的任何无线局域网络设备，应该都能够符合这项要求。

b. 如果基站位于不同的广播领域（broadcast domain），基站间的换手过程就可能会失败。假设两部工作站正在交换信息帧，但其中一部工作站却移往另一部基站，此时 802.11 就无法保证这两部工作站位于相同的广播领域。如要改善这种情况，厂商可以为所有基站指定相同的 SSID，如此一来，无线局域网络中的工作站不论置身何处，均可位于相同的广播领域，就算这些基站各自连接至不同的区域广播领域。

c. 要在两部基站间漫游，必须为加密与完整性防护过程设置一组新的安全参数，或将安全性参数自原本的基站转移至新的基站。802.11 并未规范此种程序。取决于所使用的硬件，建立安全环境（security context）的程序可能相当费时。传送大批数据库时，影响或许并不明显；传送语言数据时，就很容易察觉。

2、对工作站而言，并没有必要变更网络堆叠（network stack）的配置设置。

通常，这意味着工作站移动时仍可保有相同的网络地址。在大多数网络中，此地址即 IP 地址，虽然有些应用或许需要保留其他类型的网络地址。为了提供网络层的移动性，实际上需要一些额外的工程，特别是在 IP 领域，因为传统上 IP 并无法提供网络层的移动性。如何保有相同的网络地址乃是网络工程的主要挑战，特别是需要跨越不同的 IP 子网络时。

a. 论及如何保有相同的地址之前，工作站必须先取得一个地址。初次连接至无线局域网络时，工作站必须先取得一个地址，通常是通过 DHCP。连接过程中必

须使用同一个地址。对用户端而言，在网络中移动时，它仍可保有同一个 IP 地址，就算连接至其他基站，也无须更换地址或其他堆叠信息。

b. 当工作站跨越不同基站的覆盖区域，或者突然遇到电波链路问题，无线网络就可能会出现中断的情形。此时，基站必须掌握足够的连接信息，这样工作站总能够轻易地重新连接。基站也必须为工作站暂存信息帧，让工作站能够访问中断时所收到数据。

c. 同样重要的是，工作站必须能够维护本身的地位。如果工作站连接至某服务器，连接期间，工作站的地址必须维持不变。此外，网络系统所保存的状态信息通常与 IP 地址脱离不了关系。有许多网络会使用 NAT 来访问 Internet，每笔 NAT 记录相应于工作站的 IP 地址。

d. 视应用的不同，有时必须保存逻辑网络的路径。信息帧必须通过相同的路径传送，这样才有办法控管。不论位于网络何处，工作站都得像是连接到同一部基站才行。

没有任何单一技术能够同时满足所有移动性的要求。虽然 802.11 在链路层提供不少功能，但仍需要一些标准以外的功能。在基站间转移连接关系通常不难。在未使用链路层安全防护的网络中，将桥接信息转移给其他基站只需要几毫秒至数十毫秒的时间。重新建立链路层安全环境（link-layer security context）可能需要数百毫秒，这取决于身份认证服务器的反应速度。有些公司投入不少资源，希望打造出能够加速建立安全环境的产品。新型的『wi-fi 交换器』产品也可以加速整个漫游程序，将工作站的连接记录集中管理，如此一来就不必在基站间进行流转了。

有几种不同的做法可以提供网络层移动性。一些早期的设备使用 NAT。NAT 并非一种移动性协议。比较上层的协议做为网络的基本架构，只要转换过程失灵，应用就会无法运作。有些应用几乎无法与 NAT 相容，例如 H.323，有些则必须使用特殊的协议，例如 Ipsec 必须使用 NAT Traversal。有些设备极度依赖 NAT 来提供移动性，最好不要使用。

隧道协议（tunneling protocol）常用来提供与应用无关的移动性。用户端设备指定于某个网络，如果它无法直接访问指定网络（“home” network），基站间协议会自动将流量导回指定所在地。隧道协议必须定义于网络层，这样管道（tunnel）方能够跨网络传输信息。不过，隧道协议本身也可以运作于链路层（让 VLAN 附接点遍及全网络）或网络层（让 IP 地址可绕送至全网络）。目前，Mobile IP 隧道协议是业界唯一的开放标准（详见本章稍后的附文）。

网络设计人员经常面临的一项挑战是，究竟要提供多大范围的移动性。小规模的部署十分简单，有些技术已经可以支持 25 部基站。真正的挑战来自于如何为大规模部署，或者分散在不同区域的组织提供移动性。要设计成功的移动性解决方案，部分关键在于判断使用者的需求。有哪些过程需要 IP 地址维持不变？Telnet 与 SSH 这类具互动性的终端连接即属此类。有些应用在重新附接网络时，可以开始新的连接，而且重新连接的过程完全不需要使用者的介入。一般而言，大多数使用者并不希望，当他们搭乘汽车、火车或飞机时，IP 地址还能够维持不变。静态、大型、分散的园区，则需要高于一般的移动性支持。

Mobile IP

802.11 在 MAC 地址上耍了一套花招：工作站以 MAC 地址进行通讯，仿佛就像固定的 therent

工作站一般。然而，基站还会注意到附近的行动式工作站，并且会通过电波转送来自有线网络的数据给它。行动式工作站与哪部基站连接并无紧要，因为该负责的基站会进行必要的转送过程。有线网络上的工作站可以直接与无线工作站进行通讯，就好像它位于有线网络一般。

Mobile IP 对 IP 地址使用类似的花招。外部所使用的 IP 地址看似位于固定的地方，称为指定所在地（home location）。不过，位于指定所在地（指定所在地址）的 IP 地址是由所谓的 home agent（指定所在代理）提供服务，而非使用者的系统。和基站一样，home agent 负责追踪行动式节点目前所在的位置。当行动式节点『位于指定所在地区』（at home），就可以直接传送封包。如果行动式节点附接至不同网络（称为客籍网络『foreign network』或参访网络【Visited network】），就会向 home agent 登记所在的客籍位置，好让 home agent 知道如何传送数据给它。

举例而言，由两个无线局域网络分别位于不同的 IP 子网络。于指定所在子网络（home subnet），无线工作站可以“正常”收发数据。

如果无线工作站从『指定所在子网络』移动至另一个子网络，它会通过正常的程序附接至该网络。与基站连接的同时，该工作站或许还会从 DHCP 服务器取得一个 IP 地址。如果无线工作站无法使用 Mobile IP，由于 IP 地址突然改变，之前的连接必须因此中断，所有进行中的 TCP 连接均告无效。

不过，配备 Mobile IP 软件的无线工作站只要向 home agent 登记，就可以维持连接的状态。Home agent 可以为行动式工作站接收封包，检查登入表，然后将封包送至行动式工作站目前所在的位置。实际上，行动式工作站其实有两个地址。在指定所在网络，行动工作站可以使用 home address 进行连接。在客籍网络，则可以使用该网络所指派的地址。TCP 连接状态仍然有效，因为行动式工作站并未停止使用指定所在地址。

当然，系统管理人员通常不喜欢在终端使用者的系统上安装新的软件（这没有错）。另外的做法是使用『行动式 IP 代理』（proxy mobile IP），将代理软件的功能整合到基站设备。将 Mobile IP 功能移到基站，就不必安装用户端软件了，虽然这种做法会增加基站本身的复杂度。此处省略了许多协议过程的细节。要让工作站随时随地连接，又能够同时使用指定所在地址，在协议的设计上必须下相当的功夫。比较明显的还有安全问题，尤其是协议过程的认证，以及指定所在网络与客籍网络之间的封包转送安全问题。要维护传统之 Internet 闸道转送表及 Mobile IP 代理者之路由信息的正确性，已经是莫大的挑战。何况，该协议必须同时和 IPV4 与 IPV6 相容。想要对 Mobile IP 有更进一步的了解，我高度推荐 Charles Perkins 所著的《Mobile IP: Design Principles and Practices》（由 Prentice Hall 出版）。

21.1.2 安全性

当全世界的网络融合为盘踞全球的单一巨献，安全性就更重要。对一些较有安全意识的组织而言，无线局域网络曾是祸害的根源。随着新工具的出现，组建具备显着安全防护的网络已经变得比较简单。除了传统的安全性议题，例如使用者群组的流量区分与配置适当的访问权限，无线网络还带来新的挑战，例如私设基站与未经授权的工作站。

逻辑架构的安全性之所以错综复杂，和加密与身份认证协议的选择脱离不了关系。不过，架构本身还涉及其他安全因素，例如基站所使用的技术。

传统的基站是扮演独立网络元件的自主设备（autonomous device）。基站被设置于使用者所在地区，而且通常没有实体防护。不幸的是，随着 802.11 愈来愈受欢迎，设置于公共场所的基站很容易成为窃取的对象。传统的基站包括本身的软件与配置设置，攻击者能够从配置设置中取得敏感的安全信息（例如 RADIUS 共享密码），因此容易成为令人垂涎的目标。新式的『精简型』基地台移除了大部分的基站功能，并将这些功能置于可以被锁在集线槽的控制器上。

攻击者也有可能移除某些基站来取得额外的网络权限。在一些架构下，基站必须连接至权限较高的网络连接埠。举例而言，如果无线网络提供好几个 VLAN，有些基站要求与骨干连接的基站必须标记所有可用的 VLAN。在此种配置下，攻击者只要移除其中一部基站并取得连接埠，就可以直接访问骨干网络。

另外一个顾虑是，许多政府网络在设计上必须符合管制规定与最佳实务。美国国家标准与技术研究院（National Institute of Standards and Technology，简称 NIST）负责开发美国联邦政府所使用的 computing 标准；这些标准被称为『联邦信息处理标准』（Federal Information Processing Standards，简称 FIPS）。在 FIPS-140 这份标准中，列出了安全的网络设计必须符合哪些条件。FIPS-140 规定一些特定的数据必须经过加密。较不明显的是，FIPS-140 同时规定必须使用未经核准的加密模式与算法。并非所有安全性协议与标准都具备同等地位，只有某些网络设计符合 FIPS-140 的要求。除了大多数的联邦机构，FIPS 对联邦机构的供应商与合约商也有相当大的影响力。（FIPS 的要求将于第 22 章详细探讨。）

21.1.3 效能

虽然有移动性的好处，无线网络并非不用付出任何代价。简单来讲，不能期待无线网络提供类似有线网络的效能。相较于有线局域网络，无线网络的名目位元率（advertise bit rate）较低。更糟的是，华而不实的文宣所浮夸大数字，对协议所造成的沉重负担完全避而不提。**【注】**根据经验法则，表 21.1 列出了各种技术的最大传输率

表 21-1：各式 802.11 技术的最大传输率

Table 21-1. Maximum throughput for different 802.11 technologies

Technology	Advertised throughput	Estimated maximum continuous throughput	Estimated maximum perceived throughput with 5:1 multiplexing factor
Single radio systems			
802.11b	11 Mbps	6 Mbps	30 Mbps
802.11a	54 Mbps	30 Mbps	150 Mbps

Table 21-1. Maximum throughput for different 802.11 technologies (continued)

Technology	Advertised throughput	Estimated maximum continuous throughput	Estimated maximum perceived throughput with 5:1 multiplexing factor
802.11g, no protection	54 Mbps	30 Mbps	150 Mbps
802.11g, with protection	54 Mbps	15 Mbps	225 Mbps
Dual radio systems			
802.11a+802.11b	11+54 Mbps	36 Mbps	180 Mbps
802.11a+802.11g (without protection)	54+54 Mbps	60 Mbps	300 Mbps

不同于有线网络，无线网络的速度取决于其与最近的网络上链之间的距离。工作站离基站越远，信号就越微弱，过程速度就越慢。传输取决于距基站多远，以及设备所处的位置。对有线网络的使用者而言，这些都是陌生的概念。

信号必须够强，而且距基站不能太远，方能够达到表 21.1 所列的传输率。事实上，大多数无线局域网络则是以覆盖范围做为主要考虑。在边缘地带，只能达到最低的速率，而非最高的传输率。典型的情况如图 21.1 所示。距基站较近的工作站应用较高的数据率进行连接，距基站较远的工作站必须花费较长的时间，方能传送等量的数据。即使无线电波介质处于正常使用状态，图 21.1 中连接至基站的工作站，其最大传输率也将远低于 6Mbps。

虽然图 21.1 所显示的最大传输率不高，但可以通过神奇的多工技术（multiplexing），让数字看起来高一些。网络的基本原则是，使用者的流量通常时高时低（bursty）。虽然使用者通常希望能以每秒一百万位元以上的速率传送数据，实际上网络经常处于开置状态。网络只需要在使用者接收电子邮件或下载网页时提供最大速率；当连接处于开置状态，其他使用者就可以享受每秒一百万位元的服务。虽然 802.11b 网络的速率只有 6Mbps，但可以提供 20 至 30 个使用者每秒数百万位元的服务需求，因为很少有应用需要持续服务。（语音应用例外。）表 21-1 最后一栏显示多工数（multiplexing factor）为 5:1 时的有效传输量。取决于应用的方式与经验，有时你需要在网络上提高或降低此系数。

图 21-1 从定性的（qualitative）观点说明网络速度如何随距离而改变。从定量的（quantitative）观点，可以借助开放空间损耗（free-space loss）计算来掌握网络的传输距离与传播特性。开放空间损耗（或称路径损耗）是指没有障碍物的情况下，信号在空间中传输时的损耗。路径损耗（path loss）是一种“理想”值，用来描述电磁波随距离在信号强度方面的衰减，至于一些与组建 802.11 网络相关的因素则忽略不计。室内网络必须处理墙壁、门窗，以及大多数信号并非呈视线（line of sight）传送的问题。开放空间损耗计算的基本假设是：杂信基准（noise floor）低到某种程度时，接收器的灵敏度将成为限制因素。许多环境中，2.4 GHz ISM 频段存在过多的免照设备，以致于杂信基准超过许多接收器的最低限制。

开放空间损耗受到两种因素的影响：『信号的频率』与『涵盖的距离』。频率愈高，或距离愈长，衰减就愈严重。

开放空间损耗（以 DB 为单位）= $32.5 + 20 * [\lg(\text{频率, 以 GHz 为单位}) + \lg(\text{距离, 以公尺为单位})]$

表 21-1 所列的数值，是针对 2.4GHz 与 5GHz 无线局域网络所计算出的开放空间距离。在 ISM 频段，是以 2.437GHz 或第 6 频道的中心频率来计算。在 5GHz 频段，则是以 5.250GHz 或 U-NII 低中频段的中点来计算。（一些早期的 802.11 网卡只能够使用两种较低频段，因此有些

网络限制只能使用 802.11a 的前 8 个频道。)此表假定在 2.4GHz 频段是以最大功率 20dBm(100mW) 进行传输, 至于 802.11a 设备, 则是以 14dBm (25 mW) 的最大、实际功率进行传输。在接收器方面, 则是使用 Cisco CB-21 abg 无线网卡之规格表 (data sheet) 所列出的接收灵敏度。此表直接列出灵敏度, 是假设杂信基准远低于灵敏度栏位所列出的数值。不要期望能够得到此表所列的距离, 毕竟此处所计算出的最大距离纯属理想值。不过它可做为参考, 用来比较不同的调制速率以及不同的频段。

图 21-1: 效能与距离的关系

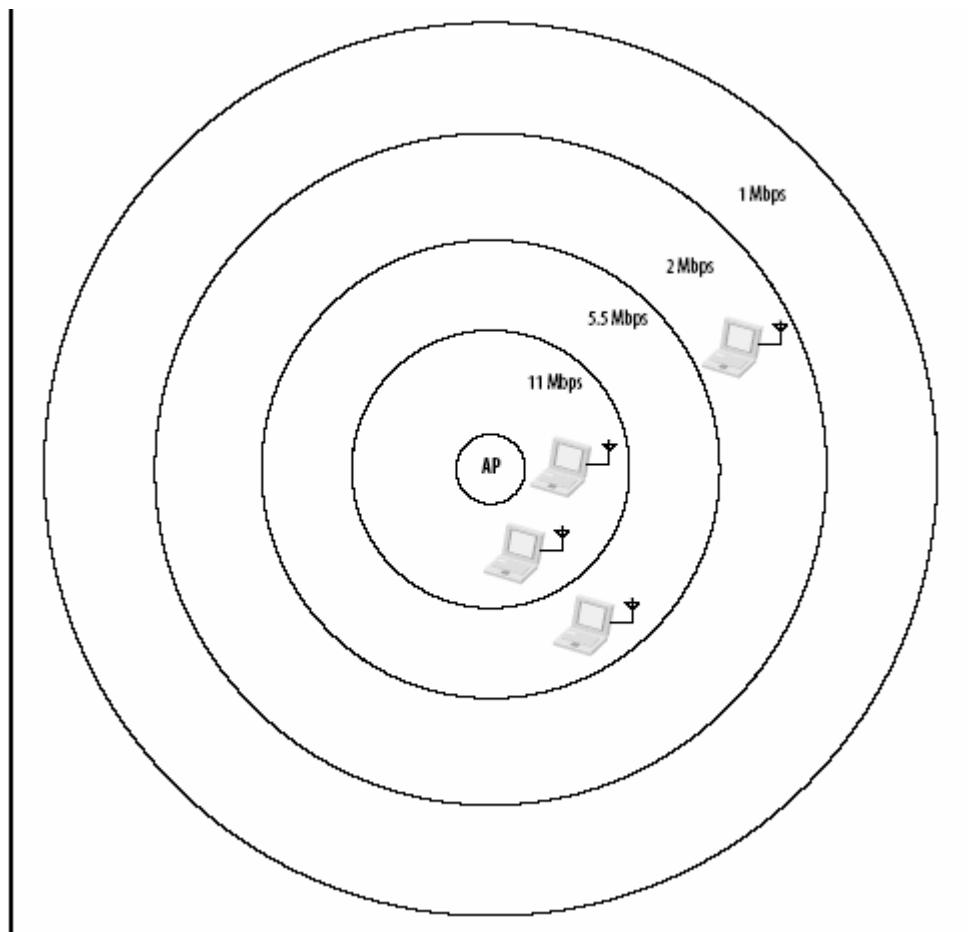


表 21-2: 开放空间中不同调制速度的传输距离

Table 21-2. Free-space range for different modulation speeds

Modulation type and speed	Sensitivity (Cisco 8-21)	Maximum free-space range (meters)	Free-space range relative to maximum speed	Percentage of maximum range modulation
2.4 GHz				
1 Mbps DSSS	-94	4,850	13.9	100%
2 Mbps DSSS	-93	4,300	12.3	89%
5.5 Mbps CCK	-92	3,850	11.0	79%
11 Mbps CCK	-90	3,050	8.7	63%
6 Mbps OFDM	-86	1,930	5.5	40%
9 Mbps OFDM	-86	1,930	5.5	40%
12 Mbps OFDM	-86	1,930	5.5	40%
18 Mbps OFDM	-86	1,930	5.5	40%
24 Mbps OFDM	-84	1,530	4.4	32%
36 Mbps OFDM	-80	970	2.8	20%
48 Mbps OFDM	-75	590	1.6	11%
54 Mbps OFDM	-71	350	1.0	7%
5 GHz				
6 Mbps OFDM	-89	630	7.0	100%
9 Mbps OFDM	-89	630	7.0	100%
12 Mbps OFDM	-89	630	7.0	100%
18 Mbps OFDM	-85	400	4.4	63%
24 Mbps OFDM	-82	280	3.1	44%
36 Mbps OFDM	-79	200	2.2	32%
48 Mbps OFDM	-74	110	1.2	18%
54 Mbps OFDM	-72	90	1.0	14%

另一个需要注意的地方是，无线网络的效能效能不同于有线网络。大多数有线网络是以交换器建构而成，因此可以独立交换不同的流量。无线网络基本上属于一种共享介质。在基站的覆盖范围内，同时只能有一部工作站进行传输。无线网络通常是以覆盖范围为主要考虑。当无线网络愈受欢迎，网管人员就必须限制每部基站的覆盖范围，以避免竞争频宽的情况出现。通过限缩覆盖范围来防止频宽竞争，乃是大多数『Wi-Fi 交换器』所采取的做法。

无线介质的实体特性对效能与服务品质有负面的影响。为了顾及可靠性，802.11 要求 MAC 层必须得到回应讯息，不过却因此造成信息帧的传输延迟。封包漏失与重传的可能性更增加了延迟的变动性，称为 jitter（抖动）。在某些应用上，使用者并不会察觉延迟的情况。可用频宽（available capacity）比服务品质（service quality）更容易影响大批数据的传输。不过，如果计划以无线网络提供语音服务，就得花费一些功夫才有办法提供可接受的服务品质。语音服务需要少量但稳定的流量，频宽高低反而不是重点。本章所探讨的架构中，有一些比较适用于需要高品质网络服务的应用。

传统服务品质的队列（queuing）与控制（control）之所以重要，不仅是因为符合无线信号少量而稳定的需求，也因为频宽有限。既然基站每秒只能传送数百万个位元，只要有一部素行不良的工作站，就可能榨干所有频宽。有些基站提供较佳的流量控制方式，让工程师自行配置稀少的无线介质资源。此外，有些逻辑架构较适合用于需要高频宽的应用。

如同许多其他网络工程，要建构符合预期效能的无线局域网络，必须分析打算在局域网络上执行的应用类型，并且尽量移除可能的瓶颈。有时候，组建足够的网络资源来满足使用者的需求的确可能。至于其他应用，可能必须使用流量管理工具来管理资源的配置。

21.1.4 骨干工程

基站位于不断扩张之网络的边陲。大多数情况下，它们并未提供新的网络服务，只是让现有服务更易于取得与使用。做为边陲设备，基站必须连至网络核心，方能够连紧使用者与资源。将无线网络加入局域网络边陲地带时，额外的配置设置势不可免。

在 802.11 刚成为标准且产品刚问世时，除了网络工程师所规划者，尚无法提供移动性，也没有针对流量加以区别。移动性完全是拜网络工程师所赐。将基地态置与单一链路层网络，才有所谓的移动性可言。否则，移动性纯粹是一种幻想。早期无线局域网络的要求是，网络的架构必须围绕着一个交换式核心，这样横跨整个园区的单一子网络便可用来连接所有基站。许多新型网络的架构也是围绕着一个交换式核心，但旧式网络通常有其限制，无法建构纯粹的交换式核心。

第一代产品问世后，业界开始生产可以将用户附接到 VLAN 的设备。虽然这些产品允许多个用户群同时存在与无线与有线骨干网络，但是较具影响力其实是骨干网络的配置。每个 VLAN 都必须延伸至园区所有基站，而不是 VLAN 来连接园区所有基站。Wi-Fi 控制器的目标之一，就是进一步减少骨干工程，允许使用较简单的基站连接配置。

21.1.4.1 Beacon、BSSID 以及 VLAN 整合

目前标准小组正在进行的一项主要工作，就是将现有的 VLAN 延伸至无线网络。针对这一点，不同厂商采取不同的做法。评估这些做法时，有一些基本的考虑。

802.11 是以所谓的『服务组合』(service set) 为基础，但并未明确定义何谓服务组合。此外，在 802.11 中有两种『服务组识别码』(SSID)。『延伸式服务组识别码』(ESSID) 就是『网络名称』。【注】这种说法有点简化，ESSID 只是基础型网络的网络名称，本书假定各位使用的是基础型网络而非独立型网络。

几部基站可以被设置为一组连接。当工作站打算连接至无线网络，就会发出探查讯息，找寻 ESSID 属于该 SSID 的基站就会加以回应。ESSID 可以随附在 Beacon 信息帧中，但并非必要。

(隐藏 ESSID 是通过隐瞒而达到安全性的做法；参考第九章，便可发现 Probe Response 信息帧中包含未经加密的 SSID。)

『基本服务组识别码』(BSSID) 是第二种类型的服务组识别码，亦即基站的 MAC 地址。它被用来做为传送于无线与有线网络间之信息帧的传送端或接收端地址。

一般而言，每个 ESSID 均具有本身的 BSSID。基站在单一 Beacon 信息帧中传送多组 ESSID，或是回应非 Beacon 信息帧中所记载的 ESSID，这种做法将导致许多问题，但却无从防范。例如 Windows Zero Configuration 软件通常不接受配置设置中出现第二个隐藏式 ESSID。它会试着连接到 Beacon 中所记载的 ESSID，而非试图搜寻隐藏式 ESSID。

当基站首度能够将使用者连接至不同的 VLAN，提供配置设置给使用者的一般做法，就是将 VLAN 命名成一个 SSID，然后让使用者自行选择。虽然这种做法十分有弹性，允许使用者自行选择如何连接至 VLAN，并且允许使用者在环境的考虑下切换 VLAN，此种弹性却如剑之双刃，当使用者选择了错误的配置设置时，容易造成使用者的混淆。为其他额外的 SSID 传送 Beacon 信息帧

不可避免要牺牲稀少的网络资源。在许多环境中，根据使用者设置档（user profile database）动态为使用者指定 VLAN 是比较有意义的做法。

21.1.4.2 IP 定位

IP 地址通常放映了实体网络的拓扑，无线网络也不例外。IP 地址的指定，算是附属于所选网络拓扑的一项决定。有些网络设计要求指定新的地址与路由配置，有些则否。试图以阶层方式配置地址空间的机构（或许是基于路由表大小的考虑），将会发现难以整合『逻辑地址的指定』与『底层的实体拓扑』。此外，使用实体 IP 地址空间的机构将发现这种做法较具优势。

21.1.5 网络服务

理想上，新的网络设备，只要附接到现有的基础设施并稍做设置，应该就可以运作。有网络服务对使用经验而言十分重要，应该仔细考虑。

21.1.5.1 DHCP

使用者的期待通常是，只要附接到网络就可以开始使用。无线网络也不例外，但却会让问题变得更糟。使用者希望只要附接到任何无线网络就可以开始使用。实际上，要让无线界面卡的 IP 堆叠自动取得适当的 IP，唯一方式就是通过 DHCP。

有些基站本身内建 DHCP 服务器。只有一两部基站的小型网络可以选择使用内建的 DHCP 服务，不过大型网络应该只使用单一来源。基站的 DHCP 服务器或许无法承担大量的负载，有些基准在连接结束后，随即会将地址收回。

任何 DHCP 服务都应该掌握所有可用的地址空间，这件事最好不要在基站中进行。基站的功能就象桥接器，将 DHCP 要求从无线网络传至有线网络，再由 DHCP 服务器予以回应。灵活运用 DHCP 代理（DHCP helper），只需要一部服务器就可以服务好几个 IP 网络，不论其为 VLAN 或无线子网络。

21.1.5.2 过程系统登入

无线网络所面临的挑战之一，就是验证使用者身份时，通常必须将网络连至身份认证服务器。例如，Windows 登入即是通过网络控制器（domain controller）来验证。这在有线网络并不困难，因为只要插上网线即可达到目的。不过在无线网络中，就回面临鸡生蛋、蛋生鸡的问题。验证网络连接时必须用到身份证明，但要验证使用者身份却得先有网络连接。并非所有过程系统厂商都会考虑这个问题。如果刚好碰上这个问题，就必须使用特别的登入功能，或是其他用户端软件来填补这个空隙。

21.1.6 用户端整合

不同的逻辑架构，需要不同用户端软件的支持。组建网络时很容易将安全性抛诸脑后，所谓用户端整合，不过是安装新的驱动程序了事。不过对任何网络而言，安全性都是不可或缺的。

使用静态 WEP 密钥可以提供最起码的安全性。有些老旧设备只支持静态 WEP，如果无法升级则别无选择。静态 WEP 的配置设置通常内建于驱动程序或用户端设置工具，不需要其他整合过程。不过为了顾及安全性，可能的话最好采用静态 WEP 以 的解决方案。

基于 802.1X 的链路层解决方案在安全性方面已有显着的进展，不过需要相当的用户端整合过程。用户端系统必须安装 802.1X 申请者软件，且必须正确设置。近来许多过程系统（Windows 2000、Windows XP 与 Mac OS X 10.3）已经整合了申请者软件。旧式系统可能需要另外安装用户端软件套件，方能支持 802.1X。

VPN 的解决方案各有不同，这取决于厂商与所采用的 VPN 技术。基于 SSL 的 VPN 是将用户端的访问导向某个安全的网站，以之做为应用的入口。由于此种技术是以安全的网站为基础，因此出了可能已经安装在过程系统上的网页浏览器，并不需要安装其他软件。不过，SSL VPN 的缺点是需要额外的工夫方能保护非网页式应用，使用者也需要经过训练。IPSec VPN 需要安装额外的软件，但比较能够处理任何以 IP 为基础的应用。VPN 用户端软件之所以愈来愈复杂，原因之一是大多数厂商希望在 VPN 用户端软件中塞进更多功能。

有些机构也许没有足够的能力为使用者安装用户端软件。例如，大学里的使用者通常必须开启 VPN 通道，方能访问外部的网站。在职进修的学生通常需要从教室连接到公司访问资源。一般而言，在 IPSec 管道中另开 IPSec 管道（IPSec tunnels inside IPSec tunnels）来执行多个用户端程序，并不是一个好的做法，如果有人这么做的话。

21.2 网络拓扑范例

重点确立之后，就可以勾勒出无线局域网络的面貌。大致上，无线局域网络的部署主要有两种方式，至于采用何种方式，取决于是否于链路层使用安全防护。本节将说明并分析无线局域网络的四种不同架构。本节所提到的四种范例，在某种程度上可说是相当严谨。等到无线局域网络硬件市场成熟，设备将会整合进这些拓扑所需要的功能，让使用者得以自行搭配符合需求的功能。

21.2.1 拓扑 1：单一子网络

起初只有一种拓扑形态。基站本身就是简单的桥接器，只能够将无线工作站附接至其所连接的有线网络。基站本身并没有什么智慧，因此设计无线网络时必须以基站当中的桥接引擎为核心。网络只支持简单的移动性。当基站只是简单的桥接器，无法处理复杂的 VLAN 或路由过程，就必须附接在相同的 IP 子网络。只要工作站位于相同的 IP 子网络，便不需要重新启动网络堆叠，并且能够维持本身的 TCP 连接。

设备本身的限制会影响到最终的网络架构。每部基站均连接至单一网络。虽然此种网络提供移动性，但通常很难组建，特别是在大型园区里。除了更改骨干网络配置，管理人员还必须指派新的 IP 地址区段以及适当地加以绕送。此种架构的开发，是在较牢靠的安全协议问世之前，用来防护有线网络免遭无线网络的波及。如今，打造两部平行网络的管理负担与成本，使得这种架构已经被大型网络排拒在外，除非网络中只有少数几部基站。

早期典型的无线局域网络部署拓扑如同 21-2 所示。此网络有单一链路层网域所构成，而且每部连接至网络的工作站均被赋予隶属该子网络的 IP 地址。因此，此种单一架构也被称为单一子网络的无线局域网络（single-subnet wireless LAN）、庭中花园架构（walled garden architecture）或 VPN 架构。（此外必须注意的是，大多数家用网络均采用此种单一子网络的做

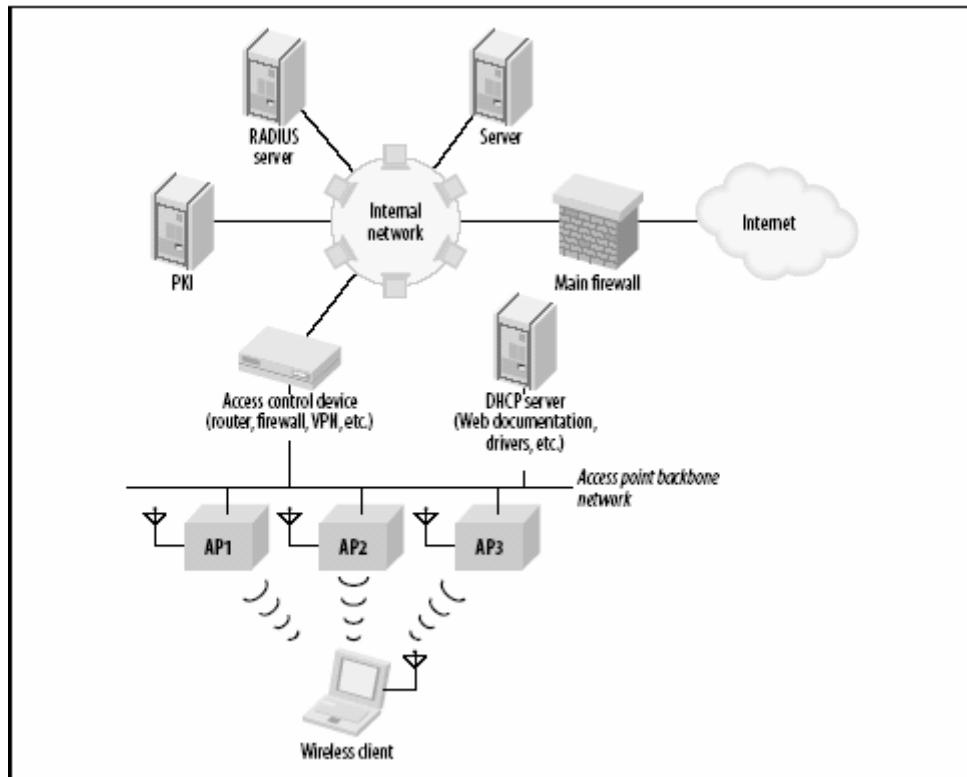
法，虽然通常只有一部基站。) 【注】图 21-2 的指导原则是，基站无法提供链路层移动性以外的服务，因此必须连接至相同的逻辑链路层。其他设计上的决定，有助于进行无线设备的访问控制，并可借助现有的服务来减轻管理上的负担，以下将逐一说明。

21.2.1.1 移动性

图 21-2 中串连所有基站的网络乃是单一 IP 网络，通常称为基站骨干。为了让使用者能够在基站间漫游。(Mobile IP 显然是此项规则的例外，参见本章的附文。) 网络层的移动性是由交换式基础设施所提供，由此基础设施将所有基站连接在一块，但使用 IP 定位机制，除了链路层的移动性，并不需要其他东西。

图 21-2 的骨干网络，实际的规模可以很大，不过并非毫无限制，亦即所有基站都必须以链路层直接连接到骨干路由器(以及其他基站)。802.11 工作站可以在网络中自由移动。不过，目前的 IP 并跨网段(子网络)。对于外部的 IP 工作站而言，图 21-2 的 VPN / 访问控制设备，乃是最后一站(last-hop)的路由器。要连紧位于此无线网络的工作站，必须通过此 IP 路由器。无线工作站究竟连接至第一或第三不基站并不重要，因为均可通过最后一站的路由器来连接。从外部来看，无线工作站无异于连接至 Ethernet 的工作站。

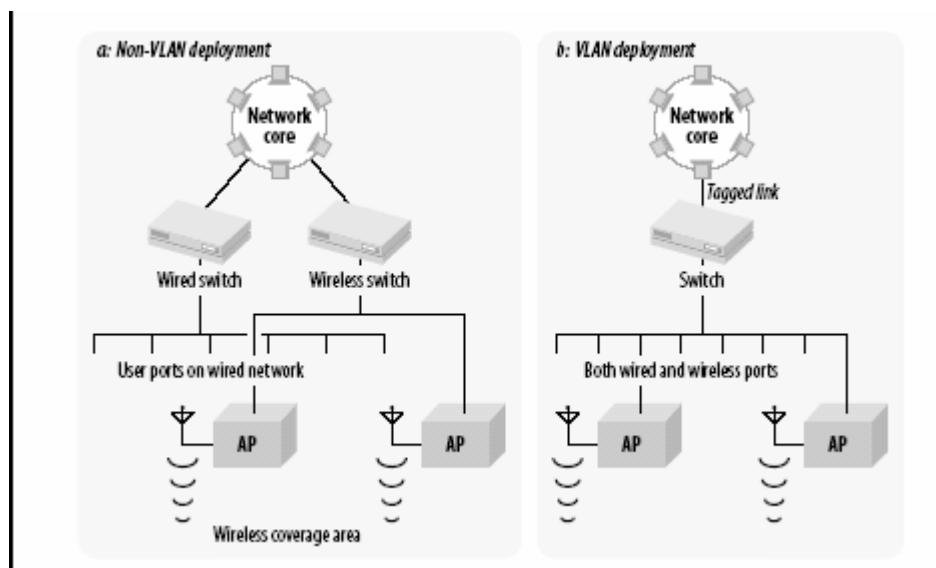
图 21-2：单一网络拓扑



不过，如果工作站离开子网络，就必须取得新的 IP 地址，然后重新建立连接。图 21-2 中，此种设计的目的，是为了将单一 IP 子网络指派给无线工作站使用，并允许它们在基站自由移动。在此并未禁用多个子网络，不过一旦使用多个子网络，就无法在子网络间提供无间隙的移动性。

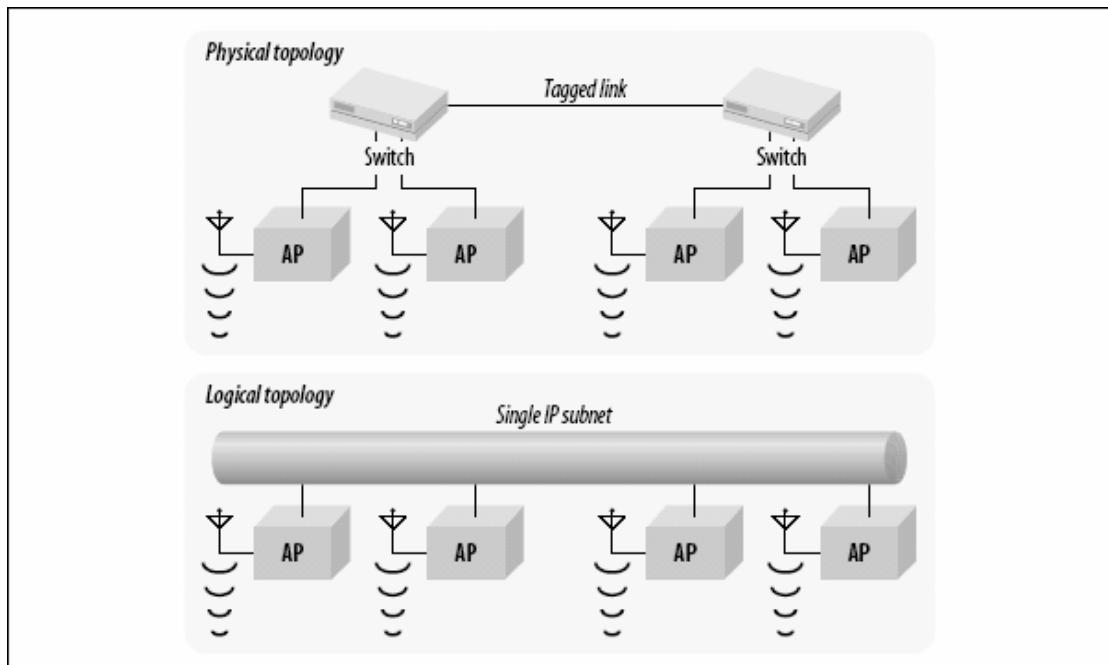
彼此合作提供移动性的基站必须在 layer2 相连。方式之一，如图 21-3 (a) 所示，就是在既存的有线基础建设外，另行组建一套如图 21-2 所示的无线基础建设。基站额外获得了一组交换器以及网络缆线的支持，并且上链 (uplink) 至核心网络。如要尽量缩减硬件，可以采用 VLAN（虚拟局域网络），如图 21-3 (b) 所示。图 21-3 (b) 中，交换器不仅扮演 layer-2 中继器 (repeater) 的角色，在逻辑上同时会将所有的连接埠划分为多组 layer-2 网络。基站可被置于其中一个 VLAN，这个 wireless VLAN（无限虚拟局域网络）可以拥有自己的 IP 子网络。从交换器流向网络核心的信息帧会加注 VLAN 代号，如此在逻辑上便能够有所区别，以便传送至不同目的地。多重子网络可以使用相同的上链链路，因为 VLAN 的标记功能允许以逻辑的方式区别信息帧。来自有线网络的信息帧会通过一个 VLAN 代号加以标记，来自无线虚拟局域网络的信息帧则以不同的 VLAN 代号标记。信息帧只会被传送至交换器中属于相同 VLAN 的连接埠，因此来自无线 VLAN 的信息帧只会送给基站。

图 21-3: 802.11 网络部署的实际拓扑



让基站骨干成为 VLAN，可以延伸相当长的距离。具备 VLAN 能力的交换器可以彼此串连，而这些经过标记的链路 (tagged link)，可以串连不同的地理区域而形成单一逻辑网络。图 21-4 中，两部交换器是以标记链路相连，四部基站均被指派给相同的 VLAN。这四部基站可被置于相同的 IP 子网络，有如连接至同一部集线器 (hub)。标记链路让两部交换器得以被隔开，实际的有效距离则取决于所使用的技术。如果采用光线链路，可以在好几栋建筑物间建构 VLAN，因此单一 IP 子网络可以涵盖好几栋建筑。

图 21-4: 利用 VLAN 来连接多部交换器



标记链路 (tagged link) 在成本与复杂度上程度不一。要连接同一栋建筑的不同区域，可以使用传统的 Ethernet 铜线。要在两栋建筑物间建立连接，则必须使用光线。建筑物之间的电压不尽相同。以铜线之类的导体连接两栋建筑，有可能让两部 Ethernet 交换器之间产生电流，因而导致严重的损坏。光纤缆线不会导电，在户外也不会受到电磁杂信的干扰，在顾虑电磁风暴的环境中，必须将此纳入考虑。另外，光线的优点是可以进行远距离高速的传输。如果有多部 Fast Ethernet 设备被连接到只配备单一FastEthernet 界面的交换器，那么上链时就会遇到瓶颈。为了在大型网络中提供较佳的传输品质，上链通常会使用 Gigabit Ethernet。

预算较为宽裕的大型机构，所使用的上链不必局限于 Ethernet。过去我所服务的一家公司就采用了都会型 (metro-area) ATM，于链路层连接市内几栋建筑。只要在 Ethernet 与 ATM 之间加上适当的转换机制，类似的服务即可做为交换器间的骨干。

21.2.1.2 以 DHCP 来指定地址

就图 21-2 而言，有两个位置适合摆设 DHCP 服务器。一个是在基站骨干子网络上。由一部独立的 DHCP 服务器，负责为无线子网络上的工作站提供可用地址。这种做法需要在每个子网络上提供一部 DHCP 服务器。另外，有能力进行路由转送的设备，通常包含 DHCP 中介机制 (relay)。如图 21-2 所示的安全设备（防火墙与 VPN）便具备路由转送的能力，并且提供 DHCP 中介机制。利用 DHCP 中介机制，来自无线网络的要求就会被基站桥接至基站骨干，然后通过访问控制设备转送至公司的主要 DHCP 服务器。如果组织以 DHCP 集中管理地址指定事宜，最好通过 DHCP 中介机制，利用现成、可靠的 DHCP 服务。使用 DHCP 中介机制的惟一缺点是，转送程序需要花费额外的时间，不过并非所有工作站均会耐心等候，此时就不该 DHCP 中介机制纳入考虑。

当然，静态定位是可以接受的做法。静态定位的缺点是需要准备较多的地址，因为不论使用与否，每个使用者均需要一个地址。为了减少使用者设置上的负担，可以考虑使用 DHCP 针对各个 MAC 地址指定固定的 IP 地址。

最后，地址指定与安全性之间有可能存在某种互动关系。如果采用 VPN 解决方案，可以在基础设施中使用 RFC1918 所规范的（私有）地址空间。DHCP 服务器所配发的私有地址，可以让

节点与 VPN 服务器连接上，当 VPN 身份确认无误，VPN 服务器即会配发可绕送的 (routable) 地址。

21.2.1.3 安全性

在本章所提出的架构中，这是最古老的架构，早在过去几年链路层安全性出现之前就已经存在。它通常用于链路层安全性并非考虑重点的场合，像是所提供的服务优先于安全性（例如 ISP），或是以上层 VPN 技术提供安全性的场合。无线网络设计时的安全性取舍，将于第 22 章详细探讨。

21.2.1.4 骨干工程

取决于现有的骨干，使用此种拓扑形态也许需要大幅修改，也许只要稍作更动。为了达到最大的移动性，每部基站均须附接至横跨整个园区的无线 VLAN。如果网络原本就组建在交换式核心之上，要建立一个横跨好几个无线槽与多部交换器的 VLAN 就相对比较简单。如果建筑物之间是以路由器串接，就无法建构延伸至整个园区的单一 VLAN，不相邻建筑物建的移动性就必须另行处置。更糟的是，有些旧式网络并非以交换器为核心，因此无法轻易延伸 VLAN 的范围。

此外 VLAN 的网络半径有实际上的限制。802.1D（桥接标准）建议 VLAN 最好不要超出七部交换器的服务半径。取决于实际的拓扑形态，或许无法将整个覆盖区域纳入单一 VLAN。就算可以，也必须大幅修改整个网络核心。

21.2.1.5 效能

此种设计的效能可能变动极大，因为当中包含一个关卡 (choke point)。此种设计若要得到良好的表现，最重要的是避免将所有流量导向单一逻辑路径。所有骨干设备必须有足够的能力处理来自整个无线网络的负载。

相较于使用碰撞检测协议的有线局域网络，基于碰撞避免原则的无线局域网络协议能够应付更高的负载。我们可以假定无线链路达到饱和，不过这取决于连接至特定基站的用户数。可使用的最大传输率依产品而异，6 Mbps 对 802.11b 而言应该算合理，至于 802.11a 与 802.11g 则可达到 27 至 30Mbps。

低速的 802.11b 比较容易避免拥塞。既然每部基站的潜在负载只有 6Mbps，基站骨干所配备的全双工 FastEthernet 链路，应该能够处理 30 部以上的基站。虽然 30 部基站还称不上大型网络，但足以提供相当大的覆盖范围，能够在相当大的开放空间提供低频宽的应用。如果将网卡设备升级为 Gigabit Ethernet，便能大幅提升可附接的基站数量。取决于上行与下行流量，或许可以连接 200 至 300 部基站，而不必担心造成骨干网络的拥塞。当然，gigabit 设备的成本远高于 Fast Ethernet 设备。

802.11a 与 802.11g 可以达到更高的速度，因此可能衍生更多问题。既然速度块了好几倍，因此 Fast Ethernet 设备只能服务几部基站。以最大的上行与下行传输而言，全双工 Fast Ethernet 可以连接 6 部基站，就算只是要覆盖中型的办公室都略嫌不足。同时具备 802.11a 与 802.11g 功能的双频基站更是雪上加霜，因为这两种电波界面均会造成高度负载。

表 21-3 列出了会让骨干技术达到饱和的基站数目。这只是粗略的估计。每一种骨干技术除以基站的负载，可估计出链路达到饱和将需要多少部基站。此表并未将协议所造成的负担，或

者上下行流量的区别纳入考虑。这只是让各位，在为无线子网络选择适当的上链技术时，有个概略的参考。

表 21-3：让骨干流量饱和所需要的基站数量

	802.11b (~6 Mbps)	802.11a or 802.11g (~30 Mbps)	Dual-band a/b (~36 Mbps)	Dual-band a/g (~60 Mbps)
Half-duplex Fast Ethernet (100 Mbps)	16	3	2	1
Full-duplex Fast Ethernet (200 Mbps)	33	6	5	3
Full-duplex Gigabit Ethernet (2,000 Mbps)	333	66	55	33

21.2.1.6 用户端整合

从用户端整合的观点，这种架构算是最多样化的。以服务供应商为例，用户端很少或几乎不需要任何调整。既然未进行任何安全防护，也就无须任何配置设置。不过，如果将较上层的安全性应用于此架构，用户端就需要额外的整合过程。

21.2.2 拓扑形态 2：E. T. Phone Home 或 Island Paradise

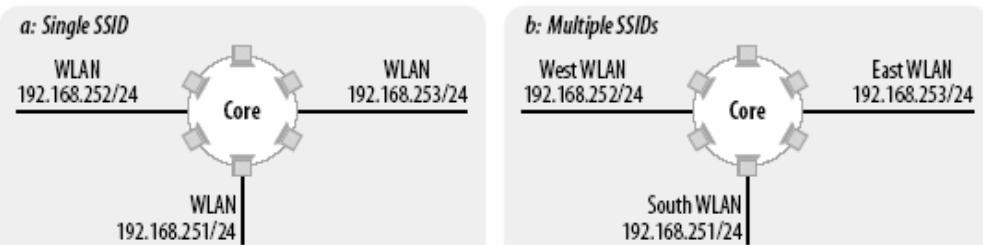
有些机构规模太大，无法组建单一基站网络。建筑物分布在方圆数里的大学就是最典型的例子。要让单一基站网络延伸至整个校园根本不可能，毕竟大型园区是以路由网络为基础。

妥协方案是由网管人员将无线网络切割为几个『孤岛』。以大学为例，一座孤岛相当于一栋建筑物或一个科系，使用本身的 IP 定位与路由信息。将无线局域网络切割为孤岛还可以满足某种有价值的政治目的。不同系所可以组建本身的无线网络，使用自己的安全政策，满足自己的网络服务目标。孤岛型网络在组建上也比较快速，因为无须与其他孤岛协调。而且各个孤岛的网络组建工作可以同时间进行。

此种拓扑形态可以在『连接至基站骨干网络的基站间』提供无间隙的移动性。在无法以单一 VLAN 做为基站骨干的网络中，常见的妥协方案是将移动性限制在某个最有用的特定区域。举例而言，在拥有多栋建筑物的园区，通常是在个别建筑物中提供无间隙移动性，但建筑物间无法漫游各栋建筑均配备如图 21-2 所示的无线局域网络，所有基站骨干网络最后串连至园区骨干。

图 21-5 (a) 中，有几个彼此相连的『孤岛』，每个孤岛各自提供本身的移动性。孤岛间的漫游无法由 802.11 本身来提供，需要类似 Mobile IP 或特殊的工作站软件。802.11 允许 ESS 跨网段，但不支持无间隙的漫游过程。

图 21-5：非连续空间的部署



如果必须将园区分割成几个不相连的覆盖区域，务必为你的用户保留最重要的移动性。大多数情况下，个别建筑物中的移动性是重要的。大多数建筑物是以交换器为核心，可以在整座大楼提供连接。

21.2.2.1 移动性

单一子网络架构是为所有基站建立单一子网络来提供移动性，并让所有用户位于相同的子网络。此种架构借用了相同的概念，但应用在无法建立单一子网络的网络上。

在最基本层次，此架构提供了可移动性。使用者可以在孤岛间自由移动，丝毫不受限制。不过跨越孤岛时，用户必须重新建立连接。重新建立连接有几种方式，有些根本不需要使用者的介入。许多大学只提供有条件的可移动性，要求使用者在离开之前，关闭用到网络资源的应用程序。如果可移动性的限制造成问题，可以利用用户端软件或隧道协议，达到 IP 网络间的移动性。

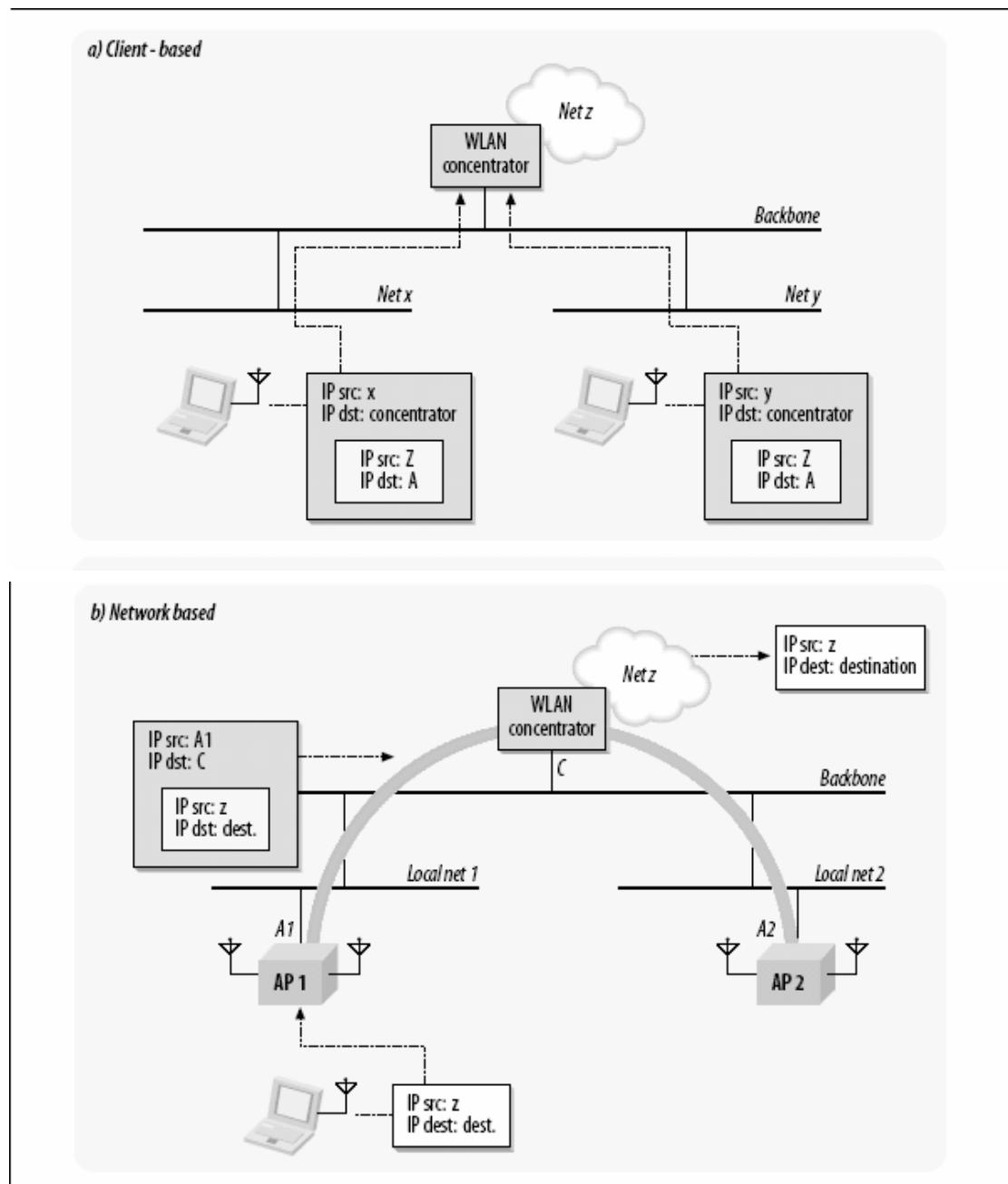
此种拓扑形态与第一种拓扑形态非常类似，只是被复制到多个不同的地区。此外，彼此相连的孤岛可以通过防火墙连接至核心网络。孤岛间的移动性可以借助隧道协议达成，确保用户不论身在何处，均能够连接至相同的逻辑位置。

图 21-6 显示了如何将移动性移植到一组分散式网络。图 21-6 (a) 中，两个工作站分属被赋予了一个 IP 地址，此 IP 地址来自工作站所连接的局域网络（图中标示为 Net X 与 Net Y 者）。连接之后，就会从『指定给 X 与 Y 网络的 IP 空间』中配发网址给工作站。不过，工作站还同时会连接至『集散中心』（central concentration point）。逻辑上，工作站所附接的是集线器（concentrator），工作站会被配发一个 IP 地址，此 IP 地址来自集线器逻辑上所附接的网络（图中标示为 Net Z 者）。工作站所发送的封包，将使用『集散中心』所配发的地址（Z）做为来源地址，但封包会被置于管道（tunnel）中进行传送。答复讯息会被绕送回 Z，不过集散器维护了一组对映关系，可将网络 Z 上的地址对映至各局域网络上的地址。注意，图 21-6 (a) 中并未指明使用何种通隧方式（tunneling method）。Mobile IP 的做法基本上类似，一些特殊的 IPSec 工作站亦然。

虽然图 21-6 (a) 的做法在概念上十分简单，但必须修改所有无线设备的软件。除了必须为所有无线设备安装新软件等管理方面的挑战，还得担负网络堆叠可能不稳定的风险，软件厂商也不见得支持所有过程系统平台。就算支持所有主要过程系统，也不见得支持一些嵌入式设备。图 21-6 (b) 提供另外一种做法：将通隧管道移至网络。图 21-6 (b) 中，基站并未直接连至骨干网络。骨干网络只用来将基站连接至流量集散中心（traffic concentration point）。所有来自工作站的信息帧或封包，均通过此一管道传送至集散设备，由集散中心分送到网络其他部分。工作站附接至哪个网络并不重要，因为任何数据均会被绕送至集散中心。

图 21-6 所举的两个例子中，重点在于工作站的 IP 地址变成与位置无关（location independent）。局域网上的 IP 地址只用于维持连通性，但逻辑上的网络附接点则是由集散中心来定义，就像上一个拓扑形态一样。

图 21-6 以通隧道提供移动性



通隧道管道的做法可以结合两个离散的覆盖区域。第一种拓扑形态中，移动性非有即无。以图 21-5 的离散覆盖区域为例，网络设计人员受限于局域网络的原本设计，只能针对最重要的区域为用户提供移动性。使用通隧道管道，可以将网络重组为单一的移动性区块，但不必翻修整个网络骨干。不过，通隧道管道的配置设置以及如何解决拓扑形式重叠的问题仍有其困难。

21.2.2.2 安全性

此种架构的一项优点，即是容易与 Ipsec 搭配使用。Ipsec 是一组坚固、值得信赖的加密协议，被广泛运用于不安全的网络环境，以及用来保护行经 Internet 的敏感数据。许多需要保护个人私密信息的机构也都在广泛使用 Ipsec。

网络层安全性的缺点在于，它为恶意的攻击者提供了一个立足点。如果网络连接未经保护，攻击者便可取得网络地址，然后开始攻击其他工作站，或者位于防火墙外的网络设施。坚固的防火墙防护绝对不可少，如此方能防范源自不可信赖网络的任何攻击。主机的安全性也极为重要，因为恶意攻击者也许会试图摧毁工作站的安全防范来劫持 VPN 管道，因此个人防火墙也是不可或缺的软件。

Ipsec 在设计上已经考虑到点对点架构。用于主要网站间时，基本上是以点对点进行传输。不过，局域网络本身并非点对点网络。（只要问那些曾经使用 ATM LAN Emulation 的人便明白！）若未经过修改或重新设置网络配置，使用组播的应用程序可能无法与 Ipsec 搭配使用。

21.2.2.3 效能

相较于第一种拓扑形态，为这些孤岛提供连接，使得这种拓扑形态具备前者所欠缺的优势。每个孤岛的闸道都必须能够转送该孤岛的流量，而不是有单一闸道来处理所有无线局域网络的流量。无线与有线网络间存在比较多的关卡（choke point），因此每个关卡可以较小，可以使用较为便宜的设备。

此种架构经常与 Ipsec 搭配使用，通常是搭配现有的 VPN 终端设备。可能发生的问题是，VPN 设备通常是做为远端的用户终端。如果局域网络的用户开始使用 Ipsec，现有的 VPN 终端设备也许会不敷使用。集中管理的 VPN 设备必须能够为所有无线局域网络上的流量负载提供加密。一部 802.11b 基站大约会造成 6Mbps 的流量负载，而 802.11a 或 02.11g 基站的流量负载可能高达 30Mbps。

针对此种拓扑形态，有几种不同的通隧选项可供使用。通隧（tunneling）必须会造成网络的负担，因为它必须用到封装机制。无线局域网络设备所面临的另一项挑战是，必须在隧道协议中进行封包切割。有些用来连接基站的局域网络骨干并不支持 jumbo 信息帧，因此行经 Ethenet 的任何隧道协议均须进行切割与重组。除了切割所造成的负担，隧道协议也需要额外的标头信息。切割过程可能造成不小的负担，这取决于所选用的协议。

将用户流量引导至网络骨干可能会降低服务品质。大型网络可能无法在基站与集散设备间提供一致的低延迟传送效能，特别是将通隧机制运用在类似 IP 这种尽力送到（best-effort）的协议上时。对一般的数据而言，服务品质稍微降低尚可接受。如果无线网络是用来服务语音协议，通隧机制就会造成实质上的影响。

21.2.2.4 骨干网络

相较于单一子网络架构，此种拓扑形态较能整合无法支持单一 VLAN 的散置网络。最糟的情况下，使用此种架构必须建构好几个小型的单一子网络骨干。不过，如果将通隧功能移至网络内部，就可以让网络延伸至远方，无须更动骨干的任何部分。

21.2.2.5 用户端

VPN 软件通常与此种架构搭配使用，无线网络工作站的用户端软件必须经过设置。对某些机构而言，这并不会造成太大的负担，特别是大多数用户均已配备 VPN 软件时。不过，有些机构会限制具有远端访问权力的用户数目，以避免整合工程过于复杂，或是远端访问设备造成过大的负载。如果在这类机构任职，安装用户端软件以及部署大范围的无线网络将成为沉重的负担。如前所述，要保护个别工作站免于链路层的攻击，个人防火墙是必备的软件。最好采用内建个人防火墙，同时可以集中控管个人防火墙设置的 VPN 软件。

21.2.3 拓扑形态 3：动态 VLAN

『单一子网络』与『孤岛』等拓扑形态，设计上考虑了市面上第一代基站的限制。早期的基站只是将所有用户连接至同一个网络，并未区分用户群组，也没有给予差别待遇。『动态 VLAN』则是首度使用有线领域 VLAN 的拓扑形态，让用户群组得以使用不同的 VLAN。此种拓扑形态是既有网络的延伸，将安全性系统与过滤条件带进无线领域，而非另外建构一个平行网络。

802.1X 是动态指定 VLAN 的基础。它完美地结合了无线网络与现有的身份认证基础设施。身份认证服务器具有用户数据与用户权限，可以将此权限信息对映到无线网络。举例而言，图 21-7 中的 RADIUS 服务器便是用来为基站指定 VLAN。RADIUS 之『access accept』讯息中包含了一种属性，可用来为通过身份认证的用户指定 VLAN。根据这项信息，基站可以标记来自改用户的所有信息帧，将之送至相应的 VLAN。

在链路层（而非较上层）进行身份认证的优点是，可以将用户置于特定的网络上，并且在一开始就赋予用户访问该网络的权限。当基站从 RADIUS 服务器接收到讯息，就会送出一个 802.1X 之『EAP Success』讯息给工作站。工作站的网卡驱动程序会将『EAP Success』讯息解读为『连上』（link up），并且送出 DHCP 要求，开始初始化网络堆叠。此时，网络已经根据用户的访问权限，自动完成本身的配置设置。

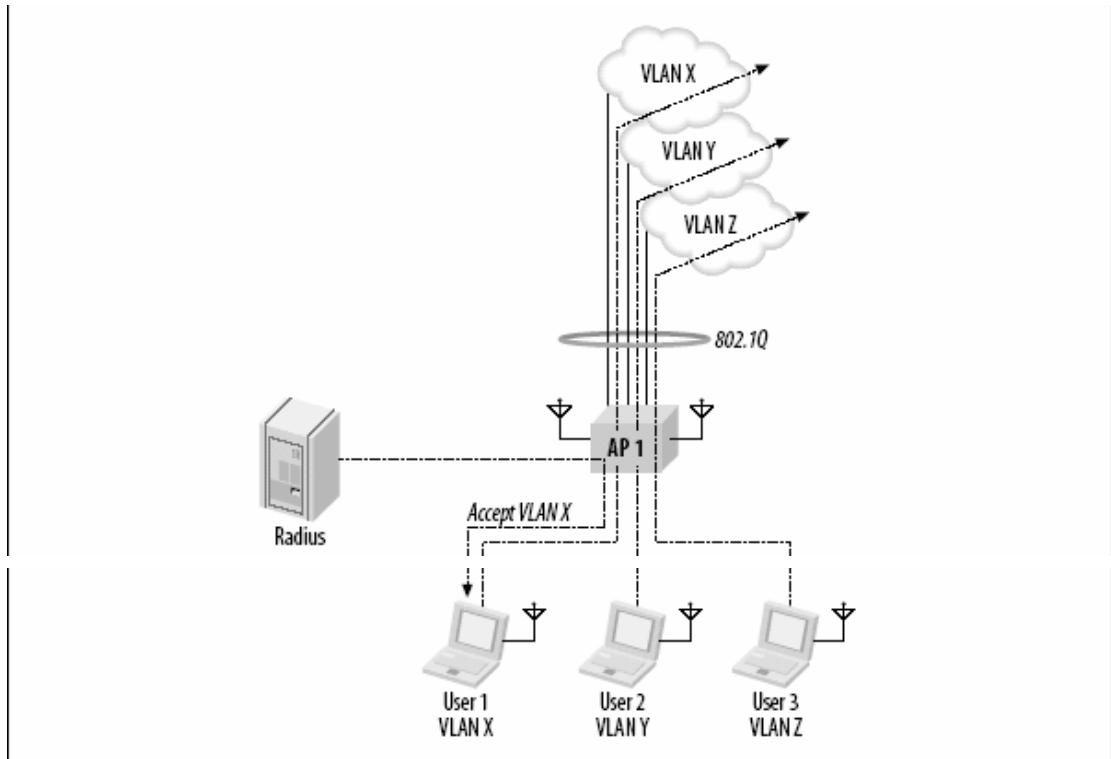


图 21-7：动态 VLAN 拓扑

21.2.3.1 移动性

在最高层次，此拓扑形态的移动性相当于第一种拓扑形态。使用者连接至具备一致性的 VLAN，因此不论身在何处，IP 地址均维持不变。既然 IP 地址不变，任何传输层或应用程序的状态在连接过程中仍然有效。

不过，此种拓扑形态底层所实现的移动性，比单一子网络架构具备更多优点。第一个优点与使用身份认证服务器有关。RADIUS 服务器所提供的属性，可以确保用户连接至同样的 VLAN，因此，用户总是可以连接至网络上相同的逻辑点。

除了有助于移动性，一致的 VLAN 连接可以让其他服务运作得更加顺畅。在链路层提供移动性，可以减轻上层协议的负担以及额外的过程。Ipsec 管道可以维持一致性，因为 IP 地址并未改变。同样地，Mobile IP 也没有必要更新位置，因为 IP 地址维持不变。

21.2.3.2 安全性

由于 VLAN 的指定是通过 802.1X 与 RADIUS，因此此种拓扑形态的安全性，是以链路层动态产生的金为 基础，包括动态 WEP、WPA 与 CCMP。动态产生金带来使用认证服务器的第二个好处。一旦辨识出使用者身份，便可为他们区分群组，给予不同的安全等级待遇。

为了区别不同用户群组的数据，基站会使用多组密钥。身份认证后，每个用户均会被赋予一把预设（广播）密钥，以及一把对映（单点传播）密钥。广播领域（broadcast domain）的界限，是由拥有相同广播密钥的工作站共同定义的，图 21-8 中，左边两个用户属于相同的用户群

组，使用相同的广播密钥。如果其中一个工作站发出 ARP 要求，另一部将会予以回复。分属不同广播领域的用户无法解读与处理此信息帧，因为他们持有不同的广播密钥。虽然各个用户群组必须共用无线频宽，但只要分属不同用户群组，在无线网络上就会有所区别。

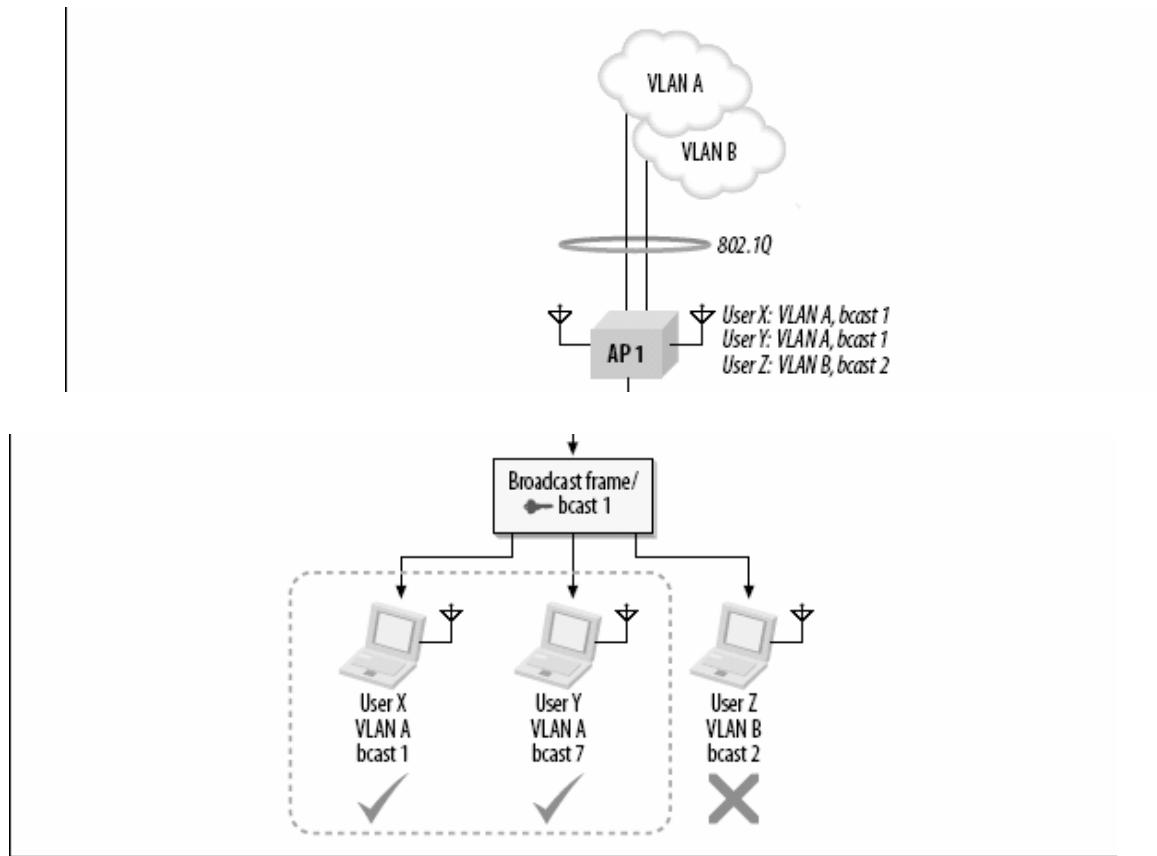


图 21-8 以密钥划分广播领域

此外，以 VLAN 区分用户群组，让网络得以提供差别式服务，如图 21-9 所示。用户识别与差别待遇的做法常用来提供访客服务。内部用户是根据用户数据库进行辨识与验证，然后将之连接至内部网络。访客在用户数据库中并无帐号，因此无法通过网络的身份认证。认证失败后，访客就会被连接至不同的逻辑网络。访客网络或许会显示『启动画面』（splash pages）要求访客点选，同意不得滥用网络。有些机构甚至要求访客必须付费方能访问网络。

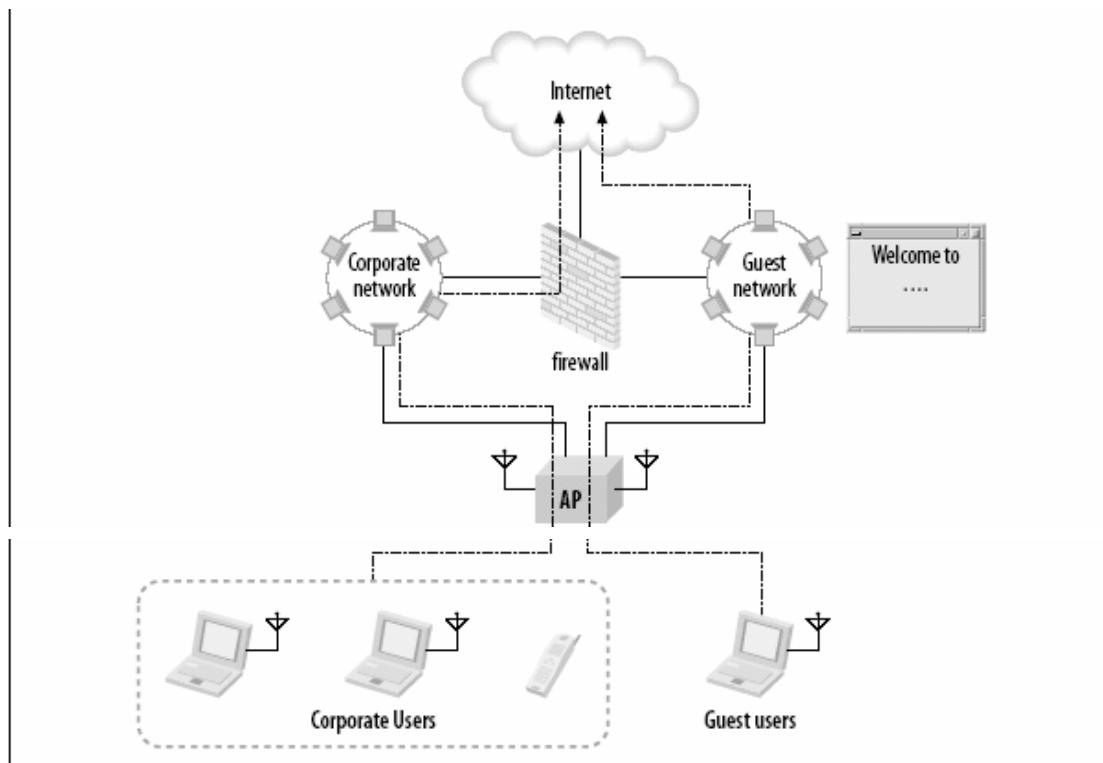


图 21-9: 差别式用户服务

链路层安全性的另一个优点是，可以将组播完美地整合到安全性协议当中。局域网络协议通常会大量使用组播或广播信息帧，而且用到组播信息帧的机会只会有增无减。无线网络之所以吸引人，是因为它们具备弹性且不受空间限制。用来协议自动发现与设置新设备的协议，通常依赖组播信息帧至深。

此种拓扑形态的一项缺点，跟官方对安全性的要求有关。写作本书时，链路层安全性尚未符合 FIPS-140 标准（美国联邦政府网络安全标准），因为 802.11i 的动态金衍生算法还有一点瑕疵。虽然 CCMP 所使用的加密模式已经核准过关，要符合 FIPS140 的要求，802.11i 网络所使用的金衍生算法还需要稍作修正。

21.2.3.3 效能

此种架构不需要架设关卡。在网络边陲交换信息帧，可以省去封包转送设备的需要。无线局域网络属于访问网络，因此就定义上而言，无线局域网络不应该造成网络核心过多的负载。不过，此种架构的缺点是，部署时最好已经有现成的大型高速交换式核心。

21.2.3.4 骨干网络

重新设计网络以便动态使用 VLAN 信息，通常得重新设计网络骨干。哪些部分需要重新设计，取决于无线局域网络与核心网络的连接方式。当无线局域网络连接至核心，以便把用户附接至不同网络，通常是使用 802.1Q 标记链路（tagged link）。无线局域网络产品的差异，在于是否广泛使用标记，以及这些标记在网络上的分布情形。大致上，要将 VLAN 信息传输至基站主要有两种方式。

直接核心连接

此情况下，基站必须直接连至网络核心，通常是通过 802.11Q 标记链路。需要注意的是，基站是以逻辑链路连接至核心网络。使用某些设备时，基站必须直接与核心网络连接，亦即每个与基站连接的交换端口（switchport）都必须支持无线用户所使用的任一 VLAN。将所有基站直接与核心连接，需要在骨干网络大动工程，甚至因此破坏使用此种拓扑的规则。如果连接 AP 的插槽并不支持 VLAN，部署网络之前必须先行布建。

直接连接至网络核心也有潜在的安全风险。大多数基站会对用户进行身份认证，不过基站本身却没有经过这道程序。攻击者只要将基站掉包，就可以直通网络核心。

间接（通隧道式）核心连接

有些产品允许使用隧道协议无须将所有基站直接连接至网络核心，如此可以避免大幅更动骨干网络。用户连接至基站，不过基站将用户的信息帧置于核心网络之前，是将用户的信息帧通过管道传送至远端。基站之间，或者基站与集散设备之间，均可建立传输管道。所使用的隧道协议也许是专属协议，或是简单的封装标准，例如 Generic Routing Encapsulation（通用路由封装，简称 GRE）、IP over IP 或者 Point-to-Point Protocol over Ethernet（简称 PPPoE）。

图 21-10 (a) 中，两部基站分别位于不同的 VLAN。用户身份认证完成后，基站负责将用户连接至适当的 VLAN。如果基站被直接附接至用户必须连接的 VLAN，连接就相当简单。否则，必须在两部基站间建立传输管道。AP2 会先找出用户应该附接的 VLAN 所在，然后通过其与 AP1 之间的管道传送用户的信息帧。逻辑上，用户还是附接至 AP1，不论其实际所在位置为何。取决于实际操作方式，或许有必要避免在距离过远的两端建立传输管道。如果两个网络跨越州际，或甚至跨越海洋，终究会引发使用者的抱怨。

图 21-10 (b)，附接点集中与网络核心，而非分散于网络边陲。基站所接收到的信息帧，会通过管道传送至集线器（concentrator），然后送至适当的网络。VLAN 信息只有在信息帧抵达终点时才用得到。抵达集线器之前，信息帧本身并未包含任何 VLAN 标记。使用远端通隧道系统的好处是，允许用户附接至当地以外的 VLAN，只要集线器能够访问 VLAN 即可。

比较上，通隧道式连接比较不需要大幅修改骨干网络，因为标记可以在当地进行处理，如果式直接连接的话，与基站相连的各个连接埠都必须承载用户所要连接之 VLAN 的完整讯息。对于骨干网络的影响，大致和第一种拓扑形态相去不远。相对而言，间接连接可以跨 spanning tree 领域延伸至较远的地区，而个别交换埠的配置设置也比较简单。

21.2.3.5 用户端

常见的过程系统大多已经内建 802.1X 申请者软件。Windows 2000、Windows XP 与 Mac OS X 10.3 等过程系统均内含 802.1X 申请者软件。如果打算使用其所支持的身份认证协议，就无须担心软件安装的问题。此外，这些内建的申请者软件通常可以通过大规模的系统管理工具进行配置设置，协助配送所需要的凭证或配置设置信息。

21.2.4 拓扑形态 4：虚拟基站

前一种拓扑形态是直接应用 802.1X 与动态 VLAN。不过，只包含一类用户时，这种架构的运作才最顺畅，因此有点不切实际。目前大多数网络在组建时通常是将员工连接至内部网络，同时为访客提供 Internet 的访问。支持不同用户的功能已经相当常见，但必须对安全性架构做额外的调整。不同的逻辑网络必须平行运作，而且通常使用不同的安全性模型。

建构多重逻辑网络的方法之一，就是建构多重实体网络，然后分别管理。但由于耗费网管人员的时间、基站的摆设位置、电力、网络连接与无线电波资源等因素，使得组建多组实体网络根本不切实际。替代方案是使用虚拟基站，只要一套实体建设，就可以建构出多重逻辑网络。实体网络拥有者就像电信业者一样，负责维护基础设施，以及传输其他网络的数据。

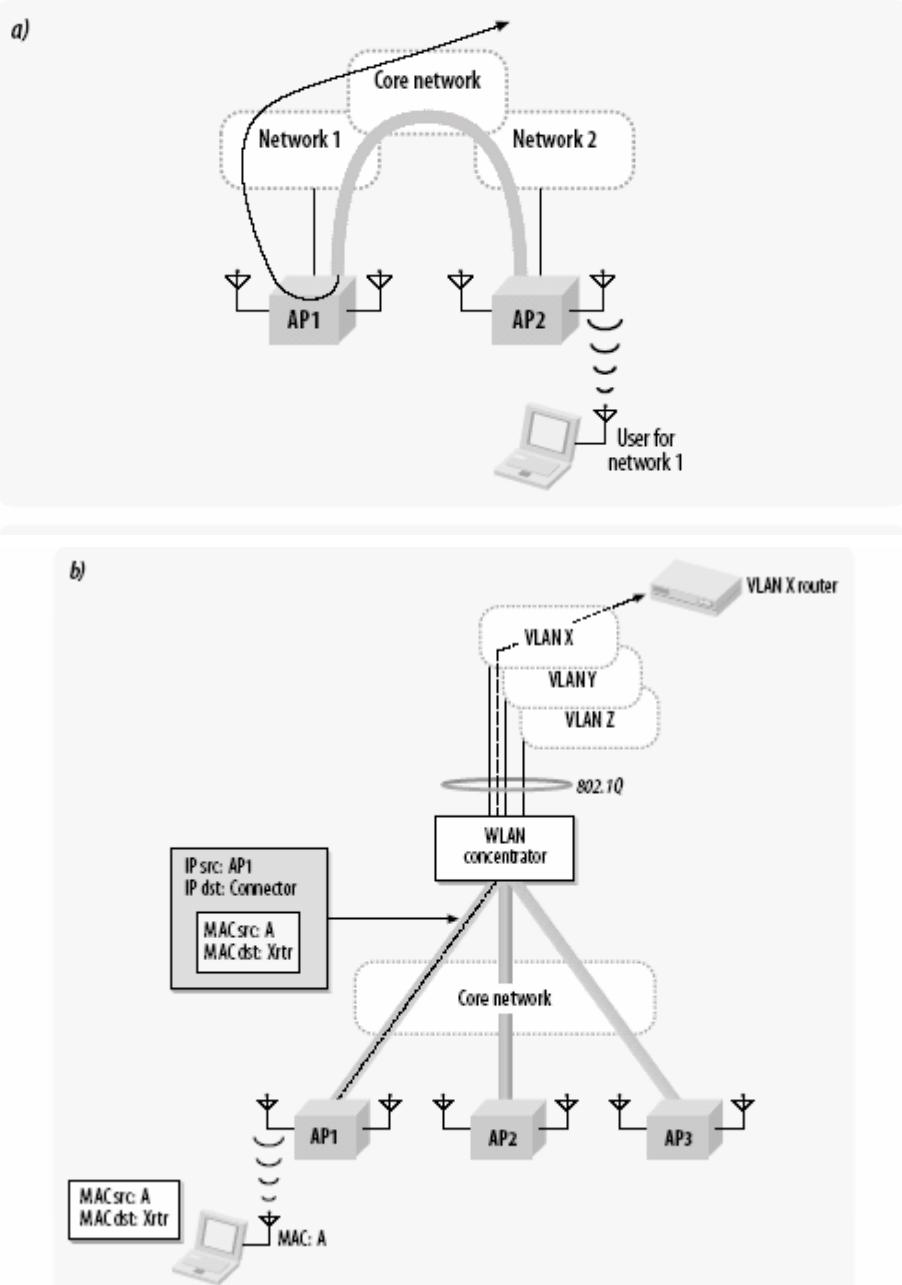


图 21-10：动态 VLAN 的产品与核心连接

几年前，机场兴起一阵热潮，让商务旅客（以及他们的钱包）能够通过 802.11 连接至 Internet。起初，机场是和特定整合厂商合力打造单一无线网络，类似本章所提到的第一种拓扑。它只供商务旅客使用，并不适合所有人。许多无线网络应用根本被忽视。无线网络最适合用来提供需要移动或每隔一段时间就会变换位置的连接，例如零售柜台或是登机口的航空设备。不难理解为何信用卡处理服务或航空公司会认为，设计给旅客用的网络无法提供必要的安全性。

以虚拟基站来设计网络，只需要一组实体基础设施，由实际组建的业主所拥有。实际拥有者负责协调调整栋建筑的频率配置。【注】从资金的角度来看，单一实体网络就是一种独门生意，拥有者可以对访问网络的动作进行收费。分组办公大楼的业主可以让无线网络的使用更加方便，吸引更多的承租人。

对网络用户而言，虚拟基站可能更符合所需。既然实体建设是由单一机构负责，就不致于重复投资也不会产生频谱之争。虚拟基站可以提供一般基站的服务，但因为共用基础建设，相较之下，就便宜得多。最高层的虚拟基站相当与好几部独立的基站。预料未来虚拟基站系统将提供管理界面给用户。网络服务的承租户，未来将可通过底层的管理界面，自行设置所承租的虚拟网络。

以虚拟基站打造的网络，如图 21-11 所示。基本上，它允许网管人员以一组实体设施来组建与控管数座动态 VLAN。图中有三个使用 WLAN 的网络。网络 A 是典型的公司网络。用户要访问此网络，必须在公司的 RADIUS 服务器上具备帐号。网络 B 属于一家热点服务供应商。为了不受设备的限制，许多服务供应商会使用网页身份认证系统，除非用户已经通过身份认证并且同意付费，否则便无法访问网络。最后，网络 C 被设计来提供 IP 语音服务，并且配备了一个 IP PBX 系统。一组基站被部署来支持以上这三个网络。网络 A 使用第一个 SSID。此 SSID 的安全性配置，要求用户必须通过 802.1X 与 RADIUS 服务器进行身份认证，打算连接至该网络的系统，需要安装必要的用户端软件，例如防毒软件。SSID A 可以支持网络 A 上几个不同的 VLAN，这取决于后端 RADIUS 服务器的设置。设置上，网络 A 支持坚固的加密方式。网络 B 使用第二个 SSID，并且通过网页进行身份认证。只要通过身份认证，使用者就可以访问 Internet。网络 B 并未加密，因为服务供应商不希望局限于某种特定平台，或要求用户使用浏览器以外的特殊软件。SSID C 被部署来支持 IP 语音（voice over IP）应用。SSID C 上的流量比其他两个网络具备较高的有限性，因为语音流量对服务品质的要求较高。如何进行身份认证，取决于所使用的设备。有些 VoIP 手机尚未支持 802.1X，网管人员只能依赖 MAC 过滤与静态 WEP 提供安全性。

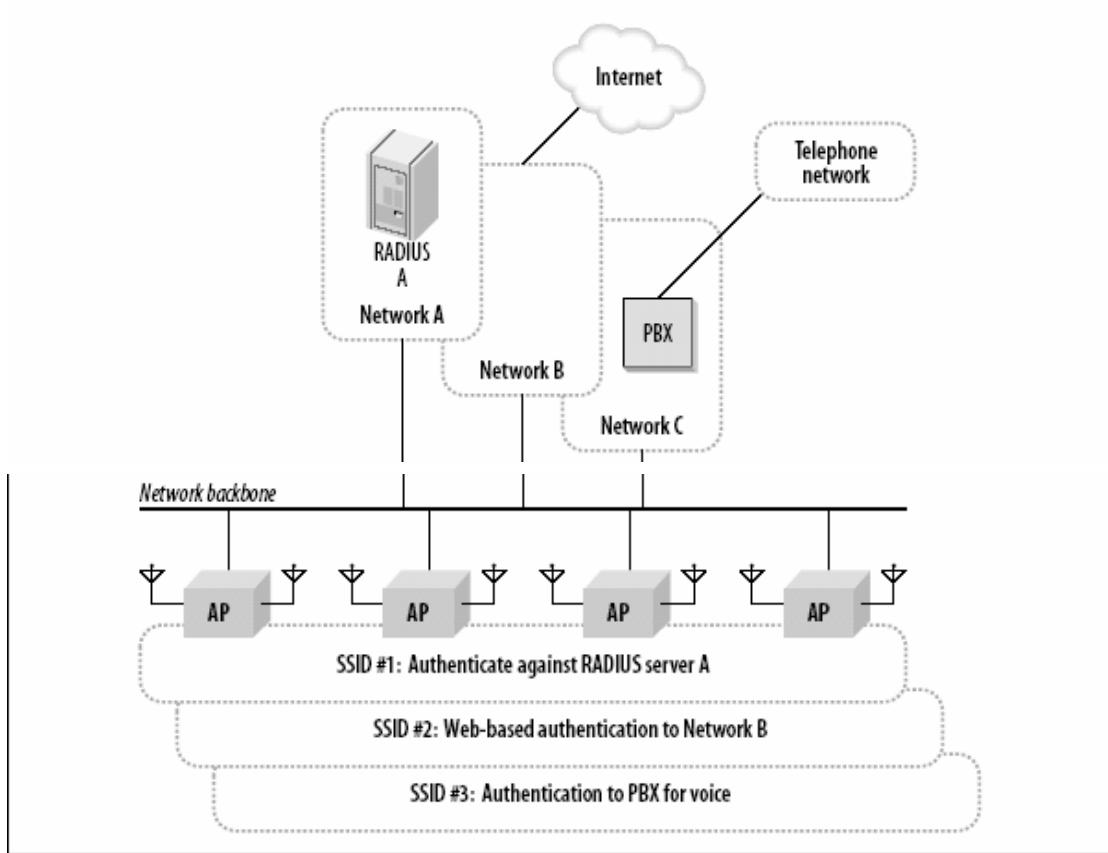


图 21-11：虚拟基站

21.2.4.1 移动性

此种拓扑形态所提供的移动性，基本上和前一种拓扑形态没有两样。VLAN 可以在网络边陲动态产生，并将用户连接至网络，因此用户端工作站是动态附接至网络上正确的基地基站。和之前的情况一样，可以使用额外的协议，让移动性延伸至其他 VLAN 领域。

对虚拟基站而言，限制移动性相当重要。此架构在设计上侧重于如何提供服务，但有时候并不需要无所不在的服务。如果办公大楼打算为承租户提供连接服务，业主或许会限制承租户的连接范围。连接服务可以限制在某个特定楼层或侧翼，而不是整栋大楼随处均可连接。如果机场打算以虚拟基站部署网络，公用的热点服务供应商应该被限制在公用范围，而机场的过程网络就不能随便访问了。不同产品会以不同的做法来限制移动性。和其他网络控制功能一样，最好选用可以集中管理的访问控制。

21.2.4.2 安全性

由于和链路层的关系密切，此种拓扑形态通常搭配 802.1X 与 RADIUS 一起使用。802.1X 不见得必要。每部虚拟基站都应具备本身的安全性配置，让客户得以自行调整本身的安全性政策。不同的客户有不同的需求，以虚拟基站打造的网络，应该容许任何合理的安全性政策。举例而言，大多数热点供应商均采用网页式登入系统。虽然对某些应用而言，网页式登入系统已经够好了，法律上的规定或许会要求，对个人数据的访问采用更严格的做法。虚拟基站网络必须能够同时容许两种访问方式。

21.2.4.3 效能

效能不会受到关卡的限制。由于无线网络直接连接至较大的网络核心，效能上的惟一限制，就是核心的拥塞。

多租户网络所面临的最大问题是，业主所打造的网络是否足以应付所有用户的需求。如果网络是私有且用于自身的目的，就可以估计出网络的需求。如果是提供网络服务给别人，通过咨询用户得来的估计或许会十分模糊。

另外值得注意的是，由于以单一基本台串多部虚拟基站，分析软件或许会显示频道过度的情况。如果网络在设计上是以所有用户所需要的总和频宽为考虑重点，在空中多加几个网络是可以接收的。

21.2.4.4 骨干网络

和其他基站一样，虚拟基站是用来连接无线与有线网络。以虚拟基站为例，无线与有线网络两者均可建构于一套共享的实体设施。除了单一有线网络，或者一组由同一架构所拥有的网络，也会有将几个客户网络连接至骨干的要求。当所有网络均属于同一机构，或许会有类似的安全需求，而且可以轻易地连至无线网络。要将无线网络对映到由不同（或许彼此竞争的）客户所拥有的有线网络，可能需要额外的方式来确保安全性。

21.2.4.5 用户端

和其他拓扑形态一样，需要安装哪些用户端软件，大部分取决于所使用的安全性协议。在简单的一端，网络可以采取最简单的方式，使用网页式身份认证就无须安装任何用户端软件。在最困难的一端，网络可以使用几种安全协议每一种协议各自有其用户端软件的需求。虚拟基站网络的优点之一，在于虚拟基站可以设立好几个网络，每个网络各自有其特殊的安全配置设置。

模糊的界限：Wi-Fi 交换器

过去几年最常被提及的无线网络发展，即是新型『Wi-Fi 交换器』架构的出现。广义而言，Wi-Fi 交换器是将网络功能自基站移转到提供控制与管理功能的整合设备。

对无线网络而言，控制与管理功能十分重要。无线网络通常需要相当多的网管支持，因为它们是由一群小型设备所组成。通过管理功能的支持，Wi-Fi 交换器可以协助网管人员打造更大型的网络。只要通过几部交换设备，网管人员就可以管理所有基站，不必单独管理个别基站。

既然可以省下控管基站的时间与精力，Wi-Fi 交换器有助于在无线网络中加入更多基站。基站数目更多，意味着每部基站的覆盖范围缩小但更为密集，这可以降低竞争频宽的机会。

Wi-Fi 交换器可用于本章所提到的任何一种拓扑形态，虽然各家厂商的产品在各种拓扑形态上的表现可能不尽相同。不同厂商会采取不同的做法来降低管理上的负担，以及提供整个网络的移动性。因此，最好挑选可以适用于自家网络，并且支持所选拓扑形式的产品。

21.3 逻辑架构的选择

选择逻辑架构时，必须衡量许多不同的取舍。其中一些关乎安全性，将于下一章探讨。不过，大部分是跟如何在效能、简单性与功能方面取得平衡有关。

1、不论选择何种架构，起码应该提供移动性。802.11 是在延伸服务组合范围内提供移动性，对工作站而言，此 ESS 必须位于单一 IP 子网络。本章提到的所有架构均将工作站连接至单一子网络，虽然所使用的机制可能完全不同。

a. 对只有几部基站的小规模部署而言，任何一种架构均属可行。如果规模很小，前两种比较容易设置，如果未来不太可能新增基站，此类做法比较具有成本概念。

b. IEEE 的基站间协议，只提供链路层的移动性。若要跨越路由器的界限至新的广播领域，需要在网络层协调无线局域网络访问设备。写作本书时，若要提供子网络移动性，通常需要挑选同一家厂商的解决方案。Mobile IP 虽是开放标准，但并未得到广泛采用。

2、用户端必须感觉到他们被附接至单一 IP 子网络，不论附接点的实际位置为何。不过，并非所有工作站都必须附接至相同的子网络。多重子网络可以在空中彼此重叠。在空中提供多重子网络可以更精确地控制用户的访问权限，以及区分不同的用户群组，但需要用到 802.1X。

3、现有的网络会造成何种限制？过去决策的包袱或许会限制目前可能的选择。

a. 由于 spanning tree 的限制，分布甚广的不规则网络可能无法将 VLAN 延伸至整个网络。在基站必须连接至核心网络时，或许就无法使用单一无线 VLAN 或是动态 VLAN 模型。

b. 动态 VLAN 拓扑形态可能必须借助广泛分布于网络上的 802.1Q 标记。如果尚无法取得 VLAN 信息，网管人员就必须找出一种方式，可以将它传送至支持无线网络的所有地区。需要直接与核心连接的产品，无法相容于路由式核心网络（routed core network）。

c. 关卡（choke point）可能分布在各地。之前已经存在的关卡会对可以附接至各地的无线设备数量造成限制。如果有意在架构中设置关卡，则它的速度必须够快，才不至于对传输率造成限制。

4、网络拓扑形态的选择，部分取决于网络所使用的安全协议。动态 VLAN 指定只能搭配 802.1X 一起使用，因此对打算使用链路层安全机制的网管人员而言，后两种拓扑形态最适合。前两种拓扑形态比较适合使用 Ipsec 与个人防火墙等网络层安全机制。本章并未直接探究不同安全做法之间的取舍，这些将留待下一章处理。

5、静态定位并没有必要。它只会造成不必要的复杂度，却无法带来多少好处。网管人员必须管理地址的配置，并且直接参与无线局域网络的新系统安装事宜。

a. 静态定位只会带来些许安全性方面的好处。传送端并不会验证来源 IP 地址，攻击者可能会集无线网络上所使用的 IP 地址，除非部署坚固的链路层防护。

b. 若要追踪用户，比较好的做法是采用 802.1X 这类以用户为中心的网络。只要在 RADIUS 服务器设置好通行于全网络的用户名，用户与 IP 地址之间就不必存在对应关系，只须对应到用户名即可。

c. 动态定位可以减少用户间意外使用相同地址的机会。通过 DHCP 代理机制，只要一部 DHCP 服务器就可以服务好几个 VLAN；如果已经有现成的 DHCP 服务器，就没有理由再架设另外一部。

表 21-4 列出了本章曾探讨过的各种因素。安全性是相当复杂的议题，不可能被浓缩成简单的表格，因此下一章将以整章的篇幅加以探讨。当各位参考此表与思考购买决策时，切记各种产品适合搭配的技术不尽相同。

	Single subnet	ET phone home	Dynamic VLAN	Virtual AP
Mobility	High if VLAN is large; limited by maximum 802.1D diameter	Depends on size of islands	High	High; but enforcing limitations may be important
Performance	Depends on choke point capacity	Depends on concentrator capacity	High due to distributed encryption	Same as dynamic VLAN
Backbone	High; though may depend on existing network	Varies with range of mobility ^a	Depends on type of connection to network core	Same as dynamic VLAN
Client	Depends on client software ^b	Depends on client software ^b	Built-in to operating system	Same as dynamic VLAN; handles multiple client security models better
IP addressing	High (new subnets and routing)	High (new subnets and routing)	Not required	Same as dynamic VLAN

^a Newer products may reduce the backbone impact by logically attaching access points to a control device in the network.

^b Both the single subnet and central concentrator architectures are typically used with VPN software for additional security. Obviously, if VPN software is used, the amount of client integration work is much larger.

表 21-4：拓扑形态比较表

第22 章 安全性架构

打从无线局域网络浮现台面，就与安全性（或者说缺乏安全性）脱不了关系。无线局域网络部署之所以不简单，是因为要在开放的网络介质中提供安全性，原本就是莫大的挑战。早期的无线网络，简直就像是在停车场开放网络插座供众人使用。

早期限制访问和保护数据的解决方案之所以可笑，部分是因为历史的教训不见得能够立即适用。传统的网络安全强调实体介质的防护，以降低网络遭受攻击的风险，但无线网络之所以有用，却是因为介质并非锁在门墙之后。既然无法为建筑物打造一层 RF 防护罩，最好假定对任何有意访问的人而言，物理层的门户都是洞开的。

既然网络介质无法提供任何实体安全性，就必须通过加密来保护用户的登入工作，以及流经网络的数据。加密可以在仅以无线电波相连的设备间建立信任关系。密码学有助于识别用户的身份，并且确保基站的确不是冒充的。一旦使用者通过身份认证，密码学还可以继续扮演众人所熟悉的角色，将流经网络的数据搅码以防遭人拦截。

网络安全与网络架构之间的关系密不可分。早期的 802.11 网络在安全性方面的基本瑕疵，导致既存的有线网络与无线网络之间被划分了一道实体与逻辑上的界线，因此牺牲了可用性。经过改良后，安全性协议已经能够将无线网络整合到现存的有线网络。但是实体网络仍然有所区隔，因为无线介质具备极为不同的物理属性。对使用者与网管人员而言，它将属于整体的一部分。从某些方面来看，它的演进过程和移动电话网络有点类似。蜂巢式移动电话网络在实体上也有所区隔，因为它们需要运用特殊设备与管理系统，来处理用户电波链路所带来的挑战。不过，它们也是现有电话网络的逻辑延伸。无须训练，用户即可在移动电话网络里使用相同的（语音）应用，而移动电话网络也被整合到了电话管理系统中。如今无线局域网络已有能力提供适当的安全性，因此两者便开始整合在一起。

22.1 安全性的定义与分析

一般而言，数据安全性可用三种属性加以定义，三者兼备方能够确保安全性。此处所提出的只是非正式的定义。本节中，我会试着依循基本的步骤，说明无线局域网络的安全性何以失败，以及如何采用业界所开发的解决方案来解决部分问题。

完整性（Integrity）

大致而言，如果数据遭未经授权的使用者篡改，完整性就算已经破坏。（数据是否遭人不当更改？）

保密性（Secrecy）

这三项属性当中，私密性或许是最容易理解的。每个人都有秘密，也清楚泄密的后果。（数据是否已经被公开？）

可用性（Availability）

能用的数据才算是数据。阻绝服务（denial-of-service）攻击是可用性最常见的威胁。（想要读取数据时是否能够如愿？）

无线局域网络技术在这三个领域均力有未遂。值得注意的是，不论是因为早期加密协议的基本瑕疵导致数据易遭窥视，或者缺乏坚固的使用者身份认证，问题的焦点都集中在私密性方面。然而，无线局域网络的瑕疵不仅如此。在最近的协议问世之前，无线局域网络一向很难防范所谓的流量灌注（injecting traffic）攻击，而缺乏帧验证机制，也使得阻绝攻击变得十分容易。

网络与电脑安全性通常被视为风险管理议题，无线安全性也不例外。有许多方式可以提高无线网络的安全性，而市面上许多产品也都能符合各位的需求。在实际动手之前，最好心中先有个蓝图。对你的网络而言，哪些是最重要的网络安全议题？愿意花费多少代价来降低这些切身议题所造成的风险？本章只是稍微勾勒出必须考虑的议题。较完整的做法可以参考一些重要的政府文件，如 NIST（美国国家标准与技术研究院）所出版的网络安全系列专刊（Special Publication）。Special Publication 800-48 探讨了许多无网局域网络的相关议题，虽然对 802.1X 讲得不深。

22.1.1 无线局域网络的安全问题

802.11 原始标准出炉后，有不少关于安全性的研究与分析陆续进行着。设计当初并未将安全性纳入原始规格，因此对未经授权的用户而言，网络形同门户洞开，也无法保护行经网络的任何数据。设计上，无线局域网络十分具有弹性。弹性通常不是坏事；不过如果一项技术在部署时可以不必考虑适当的安全性。弹性反倒可能变成一种诅咒。

22.1.1.1 请出示身份证明：身份认证

授权使用之前，必须先验明正身。为了区分哪些用户有权访问数据，必须通过密码学来进行身份认证。除非网络能够确认用户身份，否则不该提供机密协议所使用的加密密钥。早期协议的失败原因之一，就是只验证用户所使用的硬件。而不验证用户本身。虽然用户与机器之间的关系密切，但两者之间的关连，不见得如乍看之下那么一致与可预期。

为了改善最初的 802.11 身份认证机制，后续开发出了几种不同的做法。比较常见的做法是组建一套通透的代理机制，负责接收来自网页的要求，然后导向客户化的入口页面，进行身份认证。通过加密网页，网页身份认证可以有效改善身份认证机制，但无法提供更坚固的加密方式，因为无法以之衍生出链路层加密协议所需要的密钥。

22.1.1.2 空气中的秘密：加密

保护行经无线链路数据的私密性，是所有无线网络均须面对的首要挑战。由于没有实体界限，数据就如字面所言“散布于空气中”（in the air），只要持有适当的接收设备，任何人都可随意取得。以 802.11 无线局域网络为例，各位手上的 802.11 网络接口卡即可做为接收器，也可以外接高增益的天线。

要避免数据沦落到“不对的”人手中，必须对数据加密控管。攻击者可以被动聆听帧且加以分析，若要防范数据遭受拦截，势必要借助密码学。密码学就像是广效抗生素（broad-spectrum antibiotic），可以为数据提供机密性，防止数据遭不当人士取得。数据的机密性通常是靠加密协议来达成，只允许拥有密钥之经授权的用户访问数据，确保数据在传输过程中未遭篡改。

22.1.1.3 整个网络的私密性与完整性：私设基站

只要在大多数网络工程师面前提到无线安全性，得到的反应通常是强调如何保护无线链路，提供适当的加密工作来维护链路的安全私密。也牵涉到如何将未经授权的用户排除在外，不论是有线或无线网络。

如果未采取适当的安全机制加以保护，无线网络很有可能变成能够随意进出的门。安全的内部网络与基站之间若连接不当，就可能为外人另辟蹊径，绕过原本未经就位的安全防护。此外，有些网管人员担心未经授权（或私设）的基站会在未经许可的情况下被偷接到网络上。私自架设的基站通常是消费性电子产品，其安全性与可靠性也就可想而知了。

不过，私设设备终究不是特别令人感兴趣的安全问题。在网络的领域中，每股新的思潮都会带来不同的风险。不过这些风险终将被解决，私设设备也不例外。关键策略是找出这些私设设备所在位置，并将可能的损害降到最低。

要找出未经授权的私设设备，有几种可行的方式。最原始与最粗暴的方式，就是在掌上型电脑安装 **Netstumbler**，然后四处搜寻。一旦检测到未授权设备，就可以开始放慢脚步，试着找出实际的位置所在。**Netstumbler** 只是个简易的工具，大多数的 802.11 接口卡也只能显示概略的信号强度。相较于四处搜寻，比较高级的做法是使用无线协议分析仪。有些分析仪提供额外的功能，可以协助追踪未经授权的基站，例如外接用于搜寻的指向型天线，或者能够即时显示目前信号强度的特殊搜寻模式。就算不用指向型天线，能够实时显示信号强度变动的搜寻模式，在定位私设设备上也很有效率。通过 **AirMagnet** 分析仪，我曾经在几分钟内就追踪到一部基站。

四处搜寻私设设备有时会碰上问题，特别是当用户已经认出谁是基站猎人，知道何时该关闭私设设备电源时。除了通过劳力密集的搜寻方式，网络工程师已经逐渐采用网络型解决方案。只要策略性地将无线电探测设备遍布在管辖范围，当这些私设设备一开机，网管人员就会立即发现。所使用的探测工具，可以是分散式分析仪当中的特殊模式，特殊的无线 IDS，或者基站中央控管系统的功能。有些网络型系统甚至能够加以反制，以瘫痪或其他手段来阻绝私设设备，不过这些功能在得到广泛采用之前，可能还需要经过一番改良。

22.1.1.4 网络完整性：流量注入

和有线 Ethernet 一样，伪造帧(frame spoofing) 在 802.11 中并不困难。如果没有使用加密协议，恶意的用户只要修改 802.11 界面的 MAC 地址，就可以达到目的。和 Ethernet 不同的是，802.11 所使用的实体介质会在空中四处传播。802.11 设备并非附接到实体介质，而是置身其中。确保空中的帧来自合法授权的网络相当困难，需要用到一整组加密协议。除了改善加密机制外，WPA 还提供加密协议来验证每个帧，以防范伪造与流量注入攻击。

如同其他一些问题，流量注入的风险取决于许多因素。在某些企业网络，遭窥视的风险可能高于流量注入。对服务供应商而言，伪造帧或许是最主要的风险，因为这对营利没有半点帮助。

22.1.1.5 网络可达性：阻绝服务

802.11 网络可能遭受两种类型的阻绝服务攻击。在电波层次，杂信会严重干扰信号传输。任何位于 802.11 频段的电波干扰源，都有可能使得数据传输中断。攻击者使用已知能够完全断绝传输的杂信，让数据无法传输。由于无法以法拉第屏(Faraday cage) 防护整栋建筑，最好的可行方案就是找出干扰源，并予以关闭。多数情况下，干扰源并非恶意造成，只要能找出干扰源，事情就不难解决。有些手头设备可以显示杂信级别，有助于找出干扰源何在。

就算使用 TKIP 或 CCMP，也只有承载用户原始数据的帧才会验证传送端地址，管理与控制帧并不会经过验证，因此很容易伪造。阻绝服务攻击十分简单，因为者只需要知道基站的 MAC 地址，就可以开始传送 Disassociation/Deauthentication 信息。未来，或许重要的控制信息也必须经过 802.11 协议验证。在此之前，网管人员必须部署可以检测伪造控制帧的工具，否则就得承受风险。

22.1.1.6 网络完整性与可用性：私人设备

无线安全协议是设计来对用户进行身份认证与授权，但使用者通常会拥有好几种机器。有些用户喜欢夹带私人机器到办公室，并连上公司网络。私人设备通常不像设备，装有完整的防护软件与设置。在家里，私人设备通常被直接连到未经过过滤的 Internet。可能会感染各式各样的病毒或蠕虫。一旦感染病毒的机器连上公司网络，它就可能被当成跨越安全防护的跳板。

论及无线局域网络的安全时，往往会提到病毒传媒（viral vector），虽然这属一般性的安全问题。任何带进办公室并连上网络的机器均可能夹带恶意软件，不论连接到有线网络或者无线网络。防范病毒传媒主要有两种方式。其一是在网络周边病毒扫描，将防毒软件或类似工具整合至网络交换机。长远来看，这是有效的策略，短期而言，得视病毒扫描与恶意软件检测等截然不同的需求（高 CPU 负载，较大存储需求）如何整合到目前的交换机硬件，因为交换机通常只包含用来转送到特殊芯片组以及运算能力有限的通用型处理器。

另外一种做法才刚出现。许多采用 Microsoft 技术的网络，非得使用 Microsoft 机器身份认证（machine authentication）。为了确保用户使用的是经过授权且具备安全防护的机器，认证服务器必须将用户身份认证与机器身份认证结合。有些 802.1X 认证者可以结合两种认证方式，虽然这种做法在密码学上并不完整，因为这两种认证方式并未被牢牢地结合在一起。RADIUS 服务器厂商才刚开用类似的做法。如果能够成功结合两种认证，新的身份认证协议（或者协议选项可为此种组合提供密码学上业经证明的安全性。

22.1.1.7 网络完整性：分道传输

网络通常用来服务不同的用户群组。群组间通常没有任何交集，且不应共享数据。VLAN 封包过滤以及防火墙可用来区分用户群组。要在无线链路维持用户区分，不同群组必须使用不同的加密密钥。这一概念在前一章提到虚拟基站已经说明过了。

在网络边界实施分道传输(traffic separation) 效果最好。服务供应商很难使用特定的软件配置。很少有服务供应商能够指定公众网络必须使用特定厂商软件，就算有也是少数。相较之下，强制使用工作系统内建的 802.1X 软件较容易。

分道传输在企业的 802.11 网络中可能没有容身之处，特别是在新公司或小企业。不过对于具备弹性的网络，服务供应商（service provider）一词有内涵。许多学院对 802.11 十分感兴趣，打算在新建大楼或改建时使用 802.11 节省布线成本，并允许其他厂商代售 Internet 访问服务以增加收入。许多城市向同样目标努力，特别是那些已经提供 Internet 访问的单位，如图书馆。一般大众将被授权访问 Internet 的网络上，市政机关的雇员则使用另外的网络。此外，有时必须进一步区分权限，特别是那些掌管机密数据（如公众的健保信息）的市政人员。弹性也有助于各城市达到各自的社会目标，如果现有场所（如图书馆）方便雇员使用的话。

22.2 身份认证与访问控制

设计之初，无线网络就已经考虑到连接的便利性。事实上，便于连接乃是许多无线技术的主要优势。**802.11** 网络会对所有聆听 **Beacon** 帧者，宣告自身的存在。为了防范网络遭受未经授权的访问，可以使用以下四种访问控制：

工作站身份认证

连接至无线局域网络的首要步骤是，进行 **802.11** 工作站身份认证。工作站认证可以是开放系统身份认证，只进行简单的认证程序，或者是共享身份认证，必须使用 **WEP** 密钥。（细节见第 9 章）有些产品提供 **MAC** 过滤功能，可以在身份认证阶段过滤掉未经授权的工作站的 **MAC** 地址。

连接

身份认证完成后，工作站会试图与基站连接。通常，这一程序并未使用安全防护，虽然可以在此步骤使用 **MAC** 地址过滤。

链路层

一旦无线工作站与基站的虚拟网络连接处建立连接，就可以使用基于 **802.1X** 的链路层安全协议。授权用户可以连接至经许可的资源，未授权用户则被踢出网络。无线网络易受窥视，因此必须选用具备坚固密码学基础的身份认证协议。

网络层或传输层

IP 网络在安全性方面有一段不幸的过去，许多较上层的安全性产品可以布建在网络的关键点。防火墙可以用来隔离不受信任的网络以及验证用户身份。至于 **VPN** 终端设备，则能够在不可信赖的网络中提供加密功能。

不同的身份认证协议适用于 **OSI** 协议组的不同层次。起初，链路层安全机制十分弱，网管人员被迫使用较上层的安全协议。过去几年，投注在无线局域网络安全的工程与设计上的努力，主要侧重于坚固的链路层安全机制。目前在网络安全方面，网管人员有几种选择。从最脆弱到最坚固，分别是：

WEP 共享密钥身份认证

若使用共享密钥身份认证，打算访问网络的系统必须回应基站的搜索信息。共享密钥身份认证的构造十分糟糕，因此已被 **802.11i** 拒用（建议不要使用）。

MAC 地址过滤

网络上各基站均拥有一份允许网络访问的 **MAC** 地址清单。**MAC** 地址很容易伪造与复制，但一些旧设备无法提供更好的机制。

WPA 预设共用密钥（WPA-PSK 或 WPA Personal）

WPA 主要新增了一种预设共享密钥模式，允许工作站在只拥有通关密码 **Passphrase** 的情况下进行身份认证。虽然它比上述两种方式坚固，但还有更坚固的做法。

802.1X 协议

802.1X 是设计来辨识与验证用户，之后才准许用户访问网络。因为它是以 **EAP** 为基础，因此 **802.1X** 通常是指，执行于 **EAP** 之上的扩展身份认证方式。有的软件称之为 **WPA Enterprise**。

网络层身份认证

IP 网络不具安全性并非新鲜事。过去许多产品试图以各种方式解决身份认证的问题，一旦网络 (IP) 层建立后，就可以使用各种系统或协议。最适合无线网络方法，就是可用来保护网络流量的 VPN 技术。

22.2.1 工作站身份认证与连接

工作站身份认证或连接阶段所能够提供的安全性十分脆弱。连接初期所能够使用的安全机制一点都不够坚固。

一种早期的「安全性」功能即所谓的封闭式网络 (closed network)。【注】此功能有几种不同的称谓。包括隐藏式网络 (cloaked network)、SSID 广播禁止 (SSID broadcast suppression)、私有网络名称 (private network name) 等等。

802.11 问世之初，工作站必须设置基站所使用的网络名称 (SSID)。当时用户端软件还相当原始，连接之前，会先在空中搜寻具有特定网络名称的 Beacon 帧。封闭式网络有两个组成要件。基站会依标准的规定传送 Beacon 帧，但不包含 SSID 信息元素。拿掉 Beacon 帧的 SSID 可以稍微提高私密性，因为有些用户端软件不会显示出该网络。要与之连接，工作站必须送出包含 SSID 的 Probe Request 帧，因此它的作用类似一把隐藏的密钥。使用隐藏 SSID 功能的基站只接受在 Probe Request 中指出遭隐藏之 SSID 的工作站。不过由于 Probe Request 并未加密；只要观察连接成功的案例，就可以得知 SSID 为何，并以此做为连接之用。需要立即得知 SSID 的攻击者，甚至可以让已授权工作站解除连接，强迫工作站在重新连接时传送必要的 SSID。

MAC 地址过滤是相当常见的做法，几乎所有产品均有支持。基站维护了一份经过授权的 MAC 地址清单，不在名单上的工作站，其连接要求就会被拒绝。过滤 MAC 地址只能算是聊胜于无，仍然还有不少改进的空间。和有线 Ethernet 网卡一样，802.11 网卡也可以变更 MAC 地址，因此以 MAC 地址做为访问控制根本没有任何效果。只要使用封包捕捉软件，攻击者即可监视成功的连接，轻易取得一堆允许连接的 MAC 地址。

使用 MAC 地址过滤功能经常导致一堆令人头痛的问题。维护这些地址清单就是管理上莫大的负担，特别是用户倾向于使用多部设备，或者经常更换所使用的网卡。有些产品并不适合用于大规模的环境，必须分别键入相同的信息。有些可以集中管理地址清单的产品，需要使用 TFTP。但在网络安全上，TFTP 根本毫无立足之地。

第二种身份认证方式为 WEP 共享密钥身份认证。对打算访问网络的设备，基站会送出一个搜索信息。如第 5 章所述，共享密钥身份认证已遭破解，无法防范任何恶意访问网络的攻击者。就算对 WEP 密钥一无所知，也可以假造出合法的回应信息，通过 WEP 搜索。（不过除非还原出 WEP 密钥，否则无法传送帧。）

有些产品容许结合地址过滤与共享密钥身份认证。不过，两者都很容易被破解。除非无线工作站无法支持较坚固的协议，或者无法升级，否则这两种多此一举的方式，根本就不用考虑。这些只能使用原始身份认证机制的设备，通常已经十分老旧。应用于物流工作算是 802.11 技术的一项早期胜利，其所使用的手持式库存与追踪扫描器通常运算能力有限。有些并不支持 WEP，有些甚至还在使用 MS-DOS！

地址过滤与共享密钥身份认证是糟糕的安全机制，除非必要例如设备无法提供更好的机制，否则不要使用。

22.2.2 链路层身份认证

相较于简单的过滤机制，链路层身份认证可说是一大进步，主要的型式有 802.1X 与 WPA。验证用户身份有几点好处。典型的链路层身份认证机制在进行身份认证时，只容许有限的网络访问。只有在确定用户身份后，才会准许完整的网络访问。在无线局域网络领域，能够在网络连接阶段及早取得用户身份，可让网络提供更精确的访问控制，因为可以对用户进行区分，并在用户访问网络之前限制访问权限。对网络协议而言，链路层身份认证是透通的，可以搭配任何网络协议使用。如今网络逐渐走向同质化，而且大多以 IP 为基础，虽然有些旧协议仍然使用 IPX 之类的封包。链路层身份认证协议可用来保护 IP 与 IPX 网络。有时候，链路层身份认证的速度也比较快，因为可以在网络接口移动时立即进行。与其使用为广域网络设计的协议，倒不如使用在链路建立时即可移动的链路层身份认证。

22.2.2.1 WPA Personal（预设共享密钥）

WPA 有两种模式。比较简单的模式，就是传递预设共享密钥（WPA-PSK）给所有无线工作站。无线链路所使用的密钥，是根据预设共享密钥交换的次数衍生而来。和其他使用预设共享密钥的协议一样，WPA 也无法抵抗固执的攻击者所发起的决定式攻击。基本上，WPA PSK 只能当做一种捷径。WPA-PSK 是以通关密语（passphrase）与 SSID 衍生出所需要的预设共享主钥，而不是根据运算密集的 TLS 信息交换程序来产生密钥。【注】有一种称为 coWPAtty 的攻击工具可在 <http://remote-exploit.org> 下载。

大多数情况下，各 SSID 中的所有工作站仅会使用单一预设密钥。在此种网络中所有工作站共享相同的主钥。使用预设共享密钥，攻击者即可监视第 7 章所提到的四握手磋商程序，推导出其他工作站所使用的独特密钥。攻击者也可以伪造信息强迫其池工作站重新进行身份认证，以便捕捉完整的四道握手磋商程序。

WPA-PSK 的安全性，绝大部分取决于通关密语（passphrase）的品质。802.11i 的目录 H 有提到通关密语的品质，并注明通关密语中每个字符通常相当于 2.5 个比特位元的安全性。通关密语太短很容易遭受字典式攻击。

防止使用脆弱通关密语的最佳方式，就是使用二进制预设密钥共享模式，然后键入 256 个位元的预设共享密钥，或者使用较坚固的通关密语。（并非所有产品都允许直接键入预设共享密钥。）通关密语最好使用 20 个以上的字符，并且避免使用常见容易遭字典式攻击破解的词汇。有关通关密语的进一步建议以及通关密语品质的讨论，详见 Passphrase FAQ。

[注]

Passphrase FAQ 可以从 <http://www.stack.nl/~galactus/remailers/passphrase-faq.html> 获得。主要是针对 PGP 的，但其中很多建议可以用于以 Passphrase 为基础的技术，比如 WPA-PSK。

对没有什么重要数据的小型网络而言，可以使用 WPA 的预设共享密钥模式。安全性基本上就是风险管理，有些网络只需要用到 WPA PSK，因为其中并没有什么重要价值。

主要把预设共享密钥方式的 WPA 应用于小型、风险低的网络以及不需太多保护的网络用户；其它情况可以利用下面所述的认证协议。

22.2.2.2 802.1X EAP 身份认证

802.1X 是一种可扩展的架构，其本身并不是一种协议。有一堆协议可供网管人员挑选，这些协议各有其优缺点。要从中挑选出一组候选方案，得先考虑无线网络的实际需求。由于通过空气传输，无线网络原本就易遭窥视，因此必须采用坚固的加密方式来保护用户数据。除了只是传送加密过的用户数据，比较好的做法是提供相互认证。使用者必须加以验证自不待言。不过在缺乏实际线路的情况下，必须使用加密工作，确保用户是连接到合法、经过核准的无线局域网络。随机产生的密钥比静态密钥安全，尤其是如果定期更新的动态密钥的话。符合这些实际需求的协议有三种，不过通常会将第四种协议纳入考虑。

Cisco 的轻量级 EAP (Lightweight EAP，简称 LEAP) 是比较旧的协议。在标准问世之前，它被 Cisco 设计用来解决无线局域网络的安全性瑕疵。值得注意的是，它是最早为个别用户提供动态产生密钥的协议，不过它的设计无法符合其他实际需求。LEAP 使用 MS-CHAP v1 对用户数据进行编码。虽然 MS-CHAP v1 并不是以明文来传送用户数据，不过它基本上已遭破解，无法提供真正的保护。

【注】

可以参看 <http://asleap.sourceforge.net/>，这是一种用于恢复 LEAP 密码的工具；它强制用户进行认证并打乱密码

(许多嵌入式设备仍然使用 MS-CHAP v1，因为它不需要用到太多的 CPU 资源。) 此外，LEAP 也提供相互认证，不过只用到两次 MS-CHAP 交换（每个方向一次）。最后，LEAP 是 Cisco 的专属协议。虽然有其他选项可以代替，用户端必须使用其他额外的软件或者 Cisco 网卡。认证者方面必须使用 Cisco 基站。我曾共事的机构大多试图放弃 LEAP，因为它是 Cisco 的专属协议。用户端系统必须使用 LEAP 软件，它可由 Cisco 驱动程序提供，或者使用其他厂商所开发的用户端软件。经常见到广泛使用 LEAP 的机构另外购买 Cisco 网卡，插在已经内建无线网卡的可携式设备上。由于 LEAP 有其弱点，因此有了 AP-FAST 协议的开发。撰写本书之际，EAP-FAST 尚未得到广泛使用。

这三种被广泛考虑的标准是 EAP-TLS (EAP-Transport Layer Security)。PEAP(Protected LAP) 以及 TTLS (Tunneled Transport Layer Security)。三者均使用 TLS 对用户身份数据提供坚固的加密防护，并且使用 TLS 密钥交换程序，提供链路层密钥所需要的种子。此外，三者均提供相互认证功能。它们均能与身份认证服务器建立 TLS 管道，使用服务器所提供的凭证，做为网络至用户 (network-to-user) 的相互认证基础。

相互认证时，EAP-TLS 均使用凭证。要建立 TLS 管道，网络方面得先提供凭证给用户，让用户验证网络的真实性。验证完服务器的凭证后，用户端系统就会将用户凭证传送给认证服务器，进行类似的验证。EAP-TLS 相当坚固，安全且易于理解，但并非毫无弱点。用户端认证是通过用户凭证，需要存在一套 PKI 来产生。签署与传递凭证。如果凭证系统尚未建立，就不适合使用 EAP-TLS 了。

其余两种协议 (PEAP 与 TTLS) 十分类似。两者均以 TLS 管道传送服务器特征，提供第一阶段的网络至用户的身份认证，并且使用 TLS 管道，为第二阶段用户至网络身份认证所使用的用户身份数据加密。PEAP 与 TTLS 并未完全依赖特征，但无线网络上的认证者都必须拥有凭证。选用 PEAP 或 TTLS，不只是考虑何种协议适合你的需求。TTLS 较具弹性，除了在管道中传送使用者至网络的身份认证数据，几乎可以搭建各种类型的第二阶段身份认证机制。PEAP 的限制较多，因为它要求必须使用 EAP method 来进行第二阶段身份认证。实际上，最常见的 PEAP

suplicant 就是 Windows XP/2000 内建的申请者软件，且只支持一种不需要使用凭证的第二阶段协议：MS-CHAP，version 2。对拥有众多 Windows 工作站的网络而言，PEAP¹是不错的选择，因为它不需要额外的授权或者安装额外的软件。

尽量避免使用 LEAP，因为它是专属协议，也相对较弱。尽可能使用基于丁 LS 的身份认证协议，因为此类协议具备相互认证与密钥传递的功能。

EAP-TLS、PEAP 与丁 TLS 等三种协议均以 TLS 为基础。EAP-TLS 要求以用户端特征进行身份认证，但除非拥有 PKI，否则无法使用。PEAP 与 TTLS 类似，两者都是不错的选择。前者在只使用 Windows 的环境中比较有用，后者在使用旧式身份认证系统的环境中比较有用。

22.2.3 网络层身份认证

许多早期的无线网络是跟有线基础设施隔开的，并且使用现有的身份认证与访问控制机制。举例而言，前一章中，图 21-2 所提到的单一子网络拓朴，有一个理所当然的关卡（choke point）。防火墙通常部署在关卡所在处，提供某种程度的访问控制功能。如果此关卡设备也具备 VPN 功能，除了加密帧，也可以使用 VPN 软件来进行身份认证。

防火墙可以提供较严格的认证机制并也的确能够与 RSA SecurID 之类的单次密码系统整合使用。新型的 IPsec VPN 设备已逐渐整合了类似的功能，虽然必须使用扩展式身份认证（eXtended Authentication，简称 XAUTH）、混合式 IKE（Hybrid Model KE）或者认证控制密钥的搜索 / 回应（Challenge/Reponse for AuthenticatedControl Keys，简称 CRACK）等延伸功能。XAUTH 十分普及，但受制于本章所提到的复合绑定（compound binding）问题。高度安全的网络，或许希望能够以协议延伸功能来避免这些问题，以 IPsec 搭配用户凭证做为身份认证机制。VPN 设备也可以是 SSL VPN 设备，不见得是 IPsec 终端机。除了用户端软件，采用 SSL 的 VPN 设备实际上比较容易使用，因为它们只需要用到网页浏览器。

有些机构选择使用网页式身份认证系统，而不是采用全功能（且昂贵）的防火墙。无线网络本身采用最低限度的身份认证与加密机制，不对访问做特别的限制。有些网络使用 802.11 的开放系统身份认证，而且未使用加密。（一些较有安全意识的网络，已经开始为网页式身份认证系统加上 WPA-PSK 功能，但这是比较新的做法。）代理机制负责接收来自网页的要求，然后导向安全的登入页面。认证完成之前，网页系统会将来自用户端的封包加以丢弃。一旦认证成功，便允许用户端系统的封包进出。必须注意的是，有些网页式身份认证系统的确对登入程序进行加密处理，但并未提供坚固的链路层加密。

当无线局域网络首度成为发烧议题，有些厂商开始销售所谓的无线访问控制器（wireless access controller）设备，其中通常包含封包过滤、身份认证、访问授权与计费服务（authentication, authorization, and accounting services，简称 AAA）以及 DHCP 服务器。有些设备甚至包含 DNS 服务器与 VPN 终端机，以及封包塑型（packet shaping）或频宽限制（rate limiting）。AAA 功能通常提供自与现有企业基础架构（如 RADIUS）相连的介质，这些架构通常已经做好设置，可供远距访问应用。有些产品还包含动态 DNS，如此一来就可以提供个别用户动态的网域名称，以及通过 DHCP 提供 IP 地址。

22.2.4 以 RADIUS 整合用户身份认证

RADIUS 通常被拿来当做身份认证的后台，不论身份认证是在协议栈哪个层次进行。无线设备与 VPN 均采用外部的 RADIUS 服务器。大多数机构都会有一个用户帐号系统，比较常见的

做法是将 RADIUS 服务器摆在帐号系统之前，以便对其他的网络设备进行访问控制。RADIUS 服务器也可以用来整合不同的用户帐号系统，以便形成单一的用户数据库。

虽然 RADIUS 服务器能够定义当地用户（local user），其所提供的用户管理工具通常十分简单。大多数 RADIUS 服务器在部署时，会参照其他帐号数据来源，扮演协议转换的角色。一些常见的外部用户数据库包括：

Windows 网域

大多数机构多少都有一些使用 Windows 网域或 Active Directory 的用户。将 RADIUS 服务器与 Windows 密码整合在一起，对用户而言十分简便，因为 Windows 密码通常就是主要的用户身份证明。一般使用者通常厌恶记住密码。通过 Windows 网域可以让用户使用相同的身份进行不同的工作。从大学院所到大型的多国企业网络，Windows 受欢迎的程度不同，有些机构只用 Windows 网络技术。

一般标记卡（如 RSA SecurID, Secure Computing SafeWord）

一般标记卡通常会使用 RADIUS 前端，有些 RADIUS 服务器也可以将身份证明材料（凭证）直接传给标记卡服务器进行审核。如果整合标记卡服务器，管理人员便可在无线网络中使用较坚固的标记身份认证。

LDAP 目录

目录服务具有相当大的延伸性，希望集中控管用户数据的机构，通常给予评估。密码、访问权限、政策以及联络信息都可以储存在同一个目录之下。当访问 LDAP 目录时，RADIUS 服务器可以根据 LDAP 所提供的数据进行认证。例如，大学的用户不外乎教职员与学生，学生的网络访问权限就有所限制。

Kerberos 域

有些大学也大举投资 Kerberos 身份认证。RADIUS 会从一般用户取得身份数据，然后以之取得 Kerberos 通行票（ticket）。如果认证成功，就允许进行访问。目前，Kerberos 的整合工作都还很缓散。核发给用户的只是假的通行票，并未真正用于身份认证，不过有些大学希望将现有的 Kerberos 架构应用到新的无线网络。预料未来将会出现一些新的协议，使用 Kerberos 通行票数据来进行身份认证。

Unix 密码系统

Unix 密码系统包含 Pluggable Authentication Modules（可抽换式身份认证模组，简称 PAM）以及 Network Information System 网络信息系统，简称 NIS）。大举投资于 Unix 的机构可以利用现成的身份认证系统来产生单一登入点（single-sign-on）使用这些认证机制的 ADIUS 服务器被安装于 Unix 系统，并通过系统呼叫来验证用户身份。

RADIUS 代理服务器

RADIUS 服务器可将认证要求传给其他 RADIUS 服务器。在分散式环境中，例如 大型研究机构，想要建立集中式用户数据库根本不可能。最好的解决方案是接受用户帐号原本就是分散的事实，确保 RADIUS 服务器能够将身份认证要求转交其他 RADIUS 服务器进行处理。

TACACS

TACACS 是另外一种访问控制服务。它广泛使用于网络设备，主要是用来储存网 管人员的帐号，很少用来储存一般用户的帐号数据。

22.2.4.1 RADIUS 身份认证与 Microsoft Windows 数据库

查询 Windows 用户帐号的方式有两种。操作系统 API 调用可用来查询位于网域控制服务器（domain controller）的用户数据。服务器间所使用的网络协议也可以用来查询用户数据在以 Windows NT4 为基础的网络中，网域控制服务器使用了一种服务器间协议，目前这种协议已经被开放源码社群以逆向工程解析了出来。外部的 RADIUS 服务器可以执行伪装成网域控制服务器的软件，通过网络查询 Windows 帐号数据。事实上，大多数 Unix 系统上的 RADIUS 服务器均可借助逆向工程所得出的数据来验证 NT 网域的用户。Windows RADIUS 服务器必须安装在用来查询用户数据的网域控制服务器。

以 Windows 2000 为主的网络大多使用 Active Directory。除了原本的功能外，Active Directory 也导入新的服务器间协议，不过这些都是 Microsoft 的专属协议。Microsoft 的 RADIUS 服务器被称为 Internet Authentication Server (IAS)，可以使用 Active Directory 来查询储存于其他成员服务器（member server）上的用户数据。这些协议尚无人对之进行逆向工程，因此无法用于第三方厂商的 RADIUS 服务器，必须通过网域控制服务器的系统调用 API，方能取得用户信息。访问用户身份证明的要求，一旦通过 API 传给网域控制服务器，网域控制服务器就会使用 Active Directory 协议到远端查询用户数据。

间接的可信查找特性和域控制器需求对微软的 RADIUS 服务器来说是个微妙的优势。它被捆绑在 Windows 服务操作系统中。第三方的 RADIUS 服务器必须安装在域控制器上。因此网管必须在廉价的微软 RADIUS 服务器上考虑第三方 RADIUS 服务器的额外开销。

安装 Active Directoy 时可以选择原始模式。在原始模式中，成员服务器仅使用较新的 Active Directoy 协议。也可以使用采用较旧、较不安全的 NT Domain 协议的兼容模式模式。目前，大多数现在的 Active Directory 采用的是没有兼容选项的原始模式。

因此，网管人员面临一种抉择：到底应该采用 Microsoft RADIUS 服务器，或者在网域控制服务器上安装第三方厂商的 RADIUS 服务器，还是采用相容模式的 ActiveDirectory。最后一种选项牵涉到安全问题，也通常无法作用，因为它同时限制了 Active Directory 的功能。如果需要通过 Active Directory 来验证用户身份，要不就是采用 Microsoft 的 IAS，要不就是在网域控制服务器上安装第三方厂商的 RADIUS 服务器（应该注意的是，并非所有第三方厂商的 RADIUS 服务器均支持 Windows；例如，大多数协力厂商的 RADIUS 程序并无法在 Windows 上执行。）对许多机构而言，这两种选择都是莫大的挑战，因为通常必须大幅修改由网域控制服务器所构成的大型网络的控制程序。

大多数 RADIUS 服务器软件均无法访问 Windows 用户身份证明数据，除非安装在网域控制服务器上。如果需要验证 Windows 用户帐号最好安装一部网域控制服务器。

22.3 以加密确保私密性

使用者身份确定无误并赋予访问权限后，网络必须保护用户所传送的数据不被窥视。无线局域网络能够使用的加密协议如下：

静态 WEP

静态 WEP 使用单一密钥来保护用户端与基站间的数据传输。实际上，所有工作站通常会共用一把密钥，因此大幅降低了使用上的安全性。

802.1X 动态 WEP

2001 年底，传统使用单一密钥的静态 WEP，其瑕疵已经不容忽视。幸运的是，当时 802.1X 规格书刚好从标准委员会出炉，它为我们提供了动态传递密钥的方式。定期更新 WEP 密钥，可以有效防范许多针对静态密钥的攻击。

临时密钥完整性协议 (TKIP)

TKIP 属于 802.11i 的一部分，设计来提供更高的安全性，但无线介质的硬件必须 支持 RC4 加密功能。为了确保帧的完整性，TKIP 搭配 Michael 完整性检验来检测帧在传送过程中是否遭到篡改。TKIP 与 Michael 只是用来包扎 WEP 伤口的绷带。它们的确比较安全，但有多安全就很难说了。

计数器模式搭配 CBC-MAC 协议 (CCMP)

CCMP 是 802.11i 第二种主要组成部份。CCPM 采用新的加密工作方式，将加密与完整性检验工作结合为单一协议，而非分别使用不同的协议。它与过去链路层所使用的 RC4 安全协议完全决裂。如今芯片组已经整合了 AES 硬件加密功能，AES 是 CCMP 所使用的密码锁。

网络层加密协议

除了在链路层保护无线网络，也可以使用历经考验的网络层加密协议，比如 IPsec、SSL 或 SSH。

22.3.1 静态 WEP

静态 WEP 是相当可怕的安全协议。除了了胜于无，此外就没什么好说的了。除非无法使用其他方法加密数据，否则最好不要使用静态 WEP。对大多数设备而言，静态 WEP 可说已遭淘汰。只要操作系统支持并且安装了最新的驱动程序，几乎所有网卡均已支持 802.1X 链路层安全机制。惟一考虑使用静态 WEP 的场合，只有在特定的应用装备无法支持更好的机制时。

各位手上或许留有一些老旧的设备，由于处理能力有限或者升级代价太高，只能够支持静态 WEP。有些用来清点库存的 802.11 手持设备与 IP 电话机即属此类。如果别无选择，最好先检查最明显的安全漏洞。不牢固的 IV 是静态 WEP 工具的活力源。当 Airsnort 经介质披露，许多厂商随即更新固件以避免使用不牢固的 IV。虽然新版固件无法挽救 WEP 的基本瑕疵。至少可以大幅降低风险。部署之前，最好确定所使用的静态

WEP 是否会产生不牢固的 IV。如果答案是肯定的，可要求厂商提供修补程序。如果无法防范此种攻击却又继续供货，只能称之为黑心厂商。

静态 WEP 聊胜于无，比起丝毫不设防，它至少提供了某种程度的保护。它可以防止无心的用户意外连接到隔壁邻居的网络。不过，静态 WEP 并无法防范有心攻击的人士。如果非得使用静态 WEP，最好确定能否承受 WEP 网络被攻陷的后果，并确定攻击者无法以之做为攻击发起线，进一步瘫痪整个网络。

静态 INEP 是逼不得已才会使用的加密协议。除非别无选择，否则不要使用，同时做好适当的防范措施，以免泄露太多弱点。

22.3.2 802.1X 动态 WEP 密钥

虽然 802.1X 是设计来做为身份认证之用，它对 WEP 的改良也同等重要。802.1X 所包含的信息，可用来将密钥从基站传递给工作站。动态产生密钥有助于解决 WEP 的瑕疵，虽然它并不是完整的解决方案。

动态产生密钥有一项重要的前提。密钥必须近乎随机。亦即必须有来源提供密钥素材，或者密钥熵（随机比特位）。密钥素材可以来自身份认证方式，例如以 TLS 为基础的身份认证方式，或者可以直接键入为预设共享秘密。经过一系列工作，所使用的协议就会将密钥素材从一连串的随机比特位转换成链路层加密密钥。

链路层的动态密钥必须从主秘密（master secret）衍生而来。主秘密可以由用户直接提供，也可以来自身份认证程序。

从系统管理人员的观点来看，最重要的是可以动态激荡电波链路产生密钥。网管人员不必凭空杜撰 WEP 密钥，或者负责将密钥传送给用户与网络设备。用户认证程序会产生一堆密码学上认定为安全的随机数据，用来衍生出 WEP 密钥。工作站仍然使用 WEP 加密来保护帧，但用来加密帧的密钥是用户所独有的且定期更新。网管人员可以设置密钥的更新时间。用户的密钥是在身份认证过程中产生且定期更换，而非一直使用同一把密钥直到所有设备同时更换。

配钥信息可用来传递用户密钥（密钥映射或单点传播密钥）以及广播密钥（群组或预设密钥）。任何工作站只要离开网络，或者经过一段时间，就会立即更新预设密钥。工作站连接期间，初始向量（IV）会不断循环使用。不过，IV 的问题来自于重复使用带有相同密钥的 IV。只要将密钥产生计时器的时间调短，就可以避免重复使用相同的 FIV 十密钥组合。以 24 位元的 IV 而言，约有一千六百万种（224）不同的 IV。与 802.11 帧传输速率两相比较，就可以计算出最大密钥长度。分析 802.11 帧速率时，我会把流量负载视为一连串的“交易”，每次交易包含一个 TCP segment 与相应的 TCP ACK。每次交易消耗两个 IV，以一千六百万计算，可以计算出耗尽 IV 空间需要多少时间。表 22-1 列出了以不同负载系数（load factor）计算的结果。在许多方面，此表显示出密钥的存活时间相当短。为了安全起见，密钥的使用时间通常设为半小时，如此可以更有效防范重复使用 IV。

Table 22-1. IV space lifetime

	802.11b	802.11a/g, no protection
Transactions per second	479	2,334
IVs used per second	958	4,668
IV space lifetime, hours		
100% load	4.8 hr	1.0 hr
75% load	6.5 hr	1.3 hr
50% load	9.7 hr	2.0 hr
25% load	19.5 hr	2.4 hr

表 22-1：IV 空间的存活时间

最早出现的 WEP 攻击工具系根据 Fluhrrer-Martin-Shamir 理论。airsnort 与 wepcrack 均先搜集不牢固的 IV，还原密钥需要数百万个帧。近来出现的工具结合了 Fluhrrer-Martin-Shamir 与其他形式的攻击，可以更快还原出密钥，所需搜集的帧，甚至少于百万个。其中 aircrack 【是最值得注意的工具。

必须注意的是不论假设 TCP segment 与 ACK 信息的比例为 1:1 ,比其他具备更佳 TCP segment/ACK 比的模型消耗更多的 IV。不过为了安全值的考虑，以不符实际的压力测试模型来估算安全限制仍有其用处。

WEP 仍然无法抵挡帧完整性检验攻击，这和 WEP 架构有关。事实上，改善完整性检验乃是 802.11i 的主要任务之一。值得庆幸的是，目前尚未出现针对完整性检验的攻击工具。

充其量，动态 WEP 只是过渡时期的解决方案，除非设备不支持 TKIP，否则不应使用。使用动态 WEP 时切记将密钥使用时间调短，以防范 WEP 分析工具的攻击。我建议时间不要长于 15 分钟。

22.3.3 改良型 RC4 加密：TKIP

动态 WEP 是没有更好选择时才用的 (Band-Aid)，或者做为一种考虑更好替代方案时，在合理的安全范围内，部署链路层身份认证架构的方式。802.11i 包含了两种新的链路层安全机制。临时密钥完整性协议 ("Temporal Key Integrity Protocol, 简称 TKIP) 是设计来解决针对 WEP 的攻击，以及维持与现有硬件的回溯相容性。TKIP 比 WEP 安全，但尚未经历完整的考验。

TKIP 的设计目的，是在尽可能提供安全性的同时，能够维持回溯相容性。第一波 802.11 芯片通常是以软件提供安全性，如果有的话。为了解决软件加密所造成效能问题，第二波芯片开始采用硬件加密，包括 RC4 加密。TKIP 系设计来搭配 WEP 帧的处理工作 ‘以及解决 WEP 所具备的一些弱点。

TKIP 保留了 RC4 帧加密，并更新现有的 802.11 系统。和动态 WEP 一样，TKIP 仰赖特定来源提供随机数据以做为密钥的基础。因此必须搭配 WPA-PSK 或其他 802.1X EAP method 一起使用。除了基本类似之处，它也为个别帧产生独特的密钥。以中止针对初始向量的攻击，并在遭受重演攻击时，临时停止传送帧。TKIP 同时改善了完整性检验机制，确保帧的传送者拥有适当的加密密钥，并且使用经过改良的完整性检验。

在大多数硬件中，TKIP 与动态 WEP 可以共存。大多数基站可以为每部工作站暂存特有的链路层密钥。如果一部工作站使用动态密钥，另一部使用 TKIP，就会反应在密钥的储存上。同时使用这两种加密协议的确会降低广播帧的安全性，因为位于相同网络的所有工作站，必须共享相同的广播密钥。

对大多数的部署而言，应该将 TKIP 视为起码的标准，除非系统不支持。然而，不应该将 TKIP 视为长期的解决方案。

22.3.4 C C M P：AES 加密

TKIP 受制于 WEP 留下的包袱。802.11i 的计数器模式搭配 CBC-MAC 协议(Counter Mode with CBC-MAC Protocol, 简称 CCMP) 是全新的设计，一开始就将安全性考虑在内。它的设计目标，是提供能够与现有可信赖协议（如 IPsec）匹敌的安全性，但没有 IPsec 加诸无线局域网络的限制。CCMP 的设计始于 AES 密码锁(cipher)，它是大多数新式安全协议的基础。WEP 的老旧使得 TKIP 无法成为够格的安全协议，但 CCMP 的底层结构已经被美国政府核准，适用于敏感的应用场合。

除了以 AES 来提升效能，CCMP 也针对现有的加密协议进行改良。传统的加密协议可用于加密，以保护行经不可信赖路径的数据，或者用于真实性检验，以确保数据在传输过程未遭篡改。

WEP 只提供加密功能，并且仰赖一种有瑕疵的完整性检验算法。**TKIP** 以两种不同方式使用密钥。和 **WEP** 一样，密钥被用来加密帧。额外的密钥则用来提供完整性检验算法。不过 **CCMP** 允许以单一密钥来完成这两种目的，如此可以减轻计算上的负担以及提升效能。

CCMP 的主要缺点是，用户端软件的实现通常很没有效率。虽然 **CCMP** 没有理由不能与使用 **RC4** 的加密协议共存，但是大部分的驱动程序并不支持这种做法。**CCMP** 与使用 **RC4** 的加密协议并用时，驱动程序必须支持，使用 **COMP** 来传递单点传播帧，以及使用基于 **RC** 缠的加密协议来传送广播帧。我尚未见过任何厂商支持此种工作模式。使用 **CCMP** 的缺点是：由于必须同时支持两种网络，配置设置会变得更加复杂，此外，各位可能必须换掉目前所使用的无线网卡。

长期而言，**CCMF** 是相当吸引人的链路层安全协议，不过由于产品本身的限制，可能必须同时维护好几个无线网络，以及进行设备的完全更新(**forklift upgrade**)。

22.3.5 较上层的安全协议（IPsec、SSL 与 SSH）

当无线协议首度被认定存在基本瑕疵，各方都想要尽快找出解决方案。网络设计人员开始转向业经证明的加密协议，以加密流经空中的数据。其中，**IPsec** 是最主要的受惠者，虽然 **SSL** 与 **SSH** 也经常出现在考虑名单上。以上这些协议均提供识别使用者。加密数据以及确保封包在传输过程未遭篡改的机制。

使用较上层安全协议的缺点是，只能对内容提供保护。网络层安全协议可以为网络层以及网络层以上的协议提供安全服务，但无法保护底层协议。安全管理人员通常担心 **VPN** 工作站遭到反转(**turnaround**)攻击，亦即攻击者使用现成的管道访问受保护的网络。为了解决潜在的漏洞，必须使用标准的主机防护，以及个人防火墙与防毒软件。目前市面上有多种个人防火墙，便宜的必须个别安装，较贵的功能较多，比较牢靠，也可以集中控管。针对 **VPN** 工作站的攻击的确堪虑，因此有些 **VPN** 厂商会在安装套件中随附个人防火墙软件。

实现于链路层之上的安全协议，无法为链路层提供有效的保护。因此，较上层的安全协议必须以额外的主机安全协议加以辅助，例如个人防火墙软件。

实现于较上层，也比较容易支配网络架构。**VPN** 端点通常使用固定的 IP 地址，且大多数 **VPN** 用户端软件并无法应付 IP 地址改变的情况。虽然 **802.11** 支持漫游至不同的网络，但网络可能分别位于不同的 IP 子网络。一旦 IP 地址改变，就必须重新建立 **VPN** 连接。更重要的是，使用者必须接受「只要地址改变，就必须重新连接的情况。」

要尽量延长连接时间，网络设计人员必须在工作站跨越网络时保留连接状态。这可以藉助链路层识别管理工具达成，它可以使用前一章动态 **VLAN** 架构所提到的 **802.1X** 协议。在基站间进行换手工作，或者使用前一章单一子网络架构，针对换手限制来设计网络。对网络管理人员而言，前者在配置设置上比较复杂，但组建上可能比较容易。因为它不需要额外的骨干工程。

许多 **VPN** 技术皆是针对点对点加密所做的设计。组播应用可以通过 IP，但 **IPsec** 并未包含任何方式可以传递群组密钥，因此无法支持多对一的传送。在点对点链路传递密钥算是一个“简单”的问题，因为进行对话的只有两方。（所谓“简单”，是指问题并非无法处理，而且存在解决方案，并不是指很容易就可以达成）。为单点对多点连接配钥是一个“困难”的问题，因为单一传送者与多个接收者之间必须同意使用一组密钥，而且当接收者加入或离开此组播连接时，必须能够更新密钥。组播数据本质上适用于一些场合，最值得注意的是串流介质(**streaming**)

media)。大公司可以通过内部的组播会谈 (multicast session) 召开内部会议，并确保组播数据以无线网络传送时经过加密。组播数据也广泛应用于金融市场，因为它相当适合用来传递市场数据。IPsec 组播仍由标准委员会制定中，目前尚未完成。

IPsec 得到广泛使用是因为它实现于网络层。因此与使用何种应用程序无关。只要应用程序能够适应 IPsec 封装与加密所造成的迟延，就可以正常运作。在最常见的 IPsec 架构中，使用新的程序或新增一部服务器并不需要做任何变动。IPsec 被广泛用于远端访问，这同时意谓着，网络上通常存在一部可以提供加密的 IPsec 终端设备。许多行动设备早已安装与设置好用户端程序，使用者经过训练后会逐渐习以为常。如果有现成的 VPN 集线器 (concentrator) 与闲置的频宽。就可以将现有的 IPsec 远端访问，延伸至内部的无线局域网络。

赋予现有 VPN 集线器新的任务可能会造效能问题，特别是如果 VPN 设备原本是为远端访问之用。相较于局域网络用户，远端访问用户并不需要很大的频宽。定义上，远端访问性能受限于上链速度。既然许多机构仍然使用 T-1 线路或相当于 SD SI 速度的连接，远端访问连接就受限于 2 Mbps。将 VPN 延伸至无线局域网络，需要对 VPN 集线器进行升级，或者使用内建 IPsec 终端机的无线局域网络系统。IPsec 也会导致效能问题。加上 IPsec 标头，最大尺寸的 IP 封包将被切割为两个封包片段其中一个封包将包含标头信息，封包大小仍然相当于最大尺寸，但被 IPsec 标头挤到第二个封包的数据将形成小封包片段。在重组与解密封包之前，必须完成两个片段的接收。

虽然网管人员能够控制 IPsec 解决方案的头端。但无法控制用户端。不论部署规模的大小，安装与设置这些用户端软件都是莫大的挑战。也就是说，如果有用户端软件可用的话。IPsec 用户端软件是在各平台间取最小公分母，因此有些解决方案只支持 Windows。支持 Mac OS 与 Linux 的 IPsec 软件少得可怜，绝大部分是因为 VPN 集线器的缘故。厂商的终端设备需要搭配 X 厂商的用户端软件，才有办法让远端访问更加方便。少数厂商会为自家终端设备提供 Mac OS 平台的用户端软件，但 Linux 用户端软件就很少见了。（Free S/WAN 虽然实现了 IPsec。但并不支持部署所需要的特殊用户端功能。）

用户端软件的负担并不会因为使用 IPsec 而减轻。IPsec 可以在网络层阻挡各式各样的攻击，但无力保护链路层的数据。举例而言，IPsec 并无法阻止 ARP 假造或 ARP 下毒攻击，因为它并不会加密或验证 ARP 帧。IPsec 也无法防范一些网络层攻击。因为 IPsec 要求用户端必须取得 IP 地址，许多以 IPsec 防护的无线局域网络遂允许任何系统连接至网络，并且通过 DHCP 取得 IP 地址。取得立足点后，攻击者就可以对网络基础设施发起 IP 阻绝服务攻击。个人防火墙可以防范链路层攻击，但又得安装。设置与管理额外的用户端软件。近年来个人防火墙已有长足的进步，有些优秀的解决方案甚至允许集中设置与管理。

IPsec 用户身份认证也会导致严重的安全风险 • Site-to-site (网站对网站) VPN 使用双方均了解的对等 (peer) 系统，并且位于固定位置上。在取代专线的情况下，一些位于已知位置的系统可能会核发凭证，采用坚固的身份认证方式。不过，远端访问见全是另外一回事。IPsec 并不是专为用户身份认证而设计的。虽然可以采用数位凭证，但通常因为会造成管理上的梦魇而被拒绝。不少规格书以 IPs 二进行旧式的身份认证，但所有方案均不完整。其所使用的主要协议 XAUTH (eXtended Authentication) 虽然得到广泛使用，但并未完全标准化。XAUTH 要求在 IPsec 磋商之初即表明身份，同时必须以安全性递减的积极 (aggressive) 模式来运作、磋商与最后用来传递用户身份证明的管道之安全性，取决于所使用的共享秘密。一些 XAUTH 实现允许 (甚至

要求) 所有用户使用相同的共享秘密。此外, **XAUTH** 的设计也十分差劲, 同样受制于之前所提到的「复合绑定(**compound binding**)」问题。

(一些通过认证的 **Ipsec** 产品, 可以使用 **TIPS** 模式来停用 **XAUTH**。) 遗憾的是, 许多厂商仍旧持续使用 **XAUTH**。因为它广泛实现于许多 **OEM** 的用户端程序。**XAUTH** 的主要替代方案是混合模式 (**Hybrid Mode**)。混合模式的设计显然较好, 但并未得到广泛使用。

IPsec 的替代方案是只允许使用内建坚固加密系统的应用程序。网页式系统可以通过 **SSL** (**secure socket layer**) 加以保护。主机登入可以通过 **SSH** 加以保护。**SSH** 也可以用来保护多种 **TCP** 网络连接, 虽然连接埠转送 (**port-forwarding**) 的设置对一般用户而言可能过于复杂。有些环境或许已经部署 **Kerberos** 之类的架构来提供应用层的安全性, 在这种情况下, 要延伸至无线工作站并不是什么难事。

22.4 安全性协议的选择

选择安全性协议时, 首先必须决定, 你打算保护网络堆叠的哪一层: 链路层、网络层、传输层、应用层, 还是各层的某种组合? 基于 **802.1X** 的链路层安全防护与 **VPN** 分属不同层次, 两者并非互斥。究竟要选择第 2 层、第 3 层的安全性或者两者全选, 取决于你的目的与需求。两者均提供加密以防范信息遭人窥视。两者均提供用户身份认证。在身份认证完成之前, **802.1X** 会拒绝网络的访问, 以防范可能遭受的攻击, 它所使用的身份认证机制, 也优于 **IPsec** 的远端访问身份认证方式。**802.1X** 搭配改良后的 **Layer 2** 加密, 最能够符合许多机构的安全需求。简单来讲, **IPsec** 管道的安全性高于 **WEP** 连接, 就算 **WEP** 连接使用了 **802.1X** 防护, 并且经常更新密钥。

22.4.1 协议栈的安全防护

本书第一版发行以来。**802.11** 的最大改变就是出现了合理的安全性架构。首先与最重要的是, 安全性协议必须维护网络的安全。在无线局域网络中, 安全性几乎可说是身份认证与加密的函数。

22.4.1.1 「复合绑定」漏洞

大多数传统的身份认证方式并不安全。随着时间的累积, 身份认证协议日渐能够抵挡外来的攻击, 但广泛部署的旧方法仍将使用多年。为了保护这些旧式身份认证协议的安全, 常见的做法是提供某种型式的加密管道, 在不安全的网络中保护以往不安全的认证方式。**TLS** (**Transport Layer Security**) 与 **IPsec** (**IP Security**) 这类坚固通隧技术的进展, 为保护旧式身份认证协议提供了吸引人的方法。使用安全管道 (**secure tunnel**) 来保护较弱的旧式认证方式被称为「复合式身份认证: (**compound authentication**)」, 因为身份认证程序被区分为两个步骤, 首先是建立一个安全的通道, 然后是进行用户身份确认。最值得注意的复合式身份认证, 就是无线网络所使用的 **TLS** 通隧方式 (**TTLS** 与 **PEAP**), 以及 **IPsec** 常用的 **XAUTH** (**eXtended Authentication**)。设计安全性协议相当不简单, 比较简单与安全的做法是, 使用广名部署与历经考验的协议, 例如 **TLS** 或 **IPsec** 来提供必要的加密元件。

不过, 2000 年 10 月, 研究发现, 大多数复合认证方式的共通设计, 不足以防范特性类型的「中间人 J」(**man-in-the-middle**, 简称 **MITM**) 攻击。问题出在管道「内层的认证方式并未与「外层」的防护管道强力结合, 或「绑定」 (**bound to**) 在一起。于管道内交换敏感的「内层」认证数据之前, 这些协议并未检验身份认证是否针对「外层」管道的双方。之所以会产生复合绑

定问题，并不是因为管道内的协议或内部认证方式的弱点，而是因为两者的结合方式。内层的身份认证协议必须证明，内层管道的端点和外层管道的端点是一致的。

理论上，目前复合绑定所产生的漏洞颇大。不过要成功利用这些漏洞，攻击者必须主动参与。**MITM** 攻击要能成功，攻击者必须在目标网络上装设无线设备，与合法的诀证者完成第一阶段的身份认证，然后针对打算窃取其身份的用户端发动攻击。成功的攻击必须实际访问网络与设备，同时主动传送数个封包。

XAUTH 的标准化已经不再持续进行，也不会有后续的修正来解决复合绑定的漏洞。要解决 **IPsec** 的复合绑定问题，可以在所有用户端使用数位凭证。无线局域网络协议尚未到达完成阶段，将会持续修改以解决复合绑定的瑕疵。

22.4.1.2 加密

相较于任何使用 **RC4** 的帧加密方式，**IPsec** 连接或许能够提供更坚固的加密能力。考虑到此标准及其实现已经问世一段时间，**IPsec** 的确相当值得信赖，特别是搭配静态地址与数位想证时。要说它有什么弱点，大概就是网络层协议无法为 **MAC** 层提供安全防护。在受到 **IPsec** 保护的无线网络中，攻击者可以轻易取得 IP 地址，并对其他用户或 **VPN** 元件改动阻绝服务攻击，因为在改动网络协议之前并不需要经过身份认证。

22.4.1.3 安全性认证

有时候，产品必须通过安全性认证（**security certification**），这因所处的环境而异。通常，政府网络必须使用经过评等的产品。在美国，此一程序是根据 **FIPS**（联邦信息 **IPsec** 的 **Quick Mode**（第二阶段）4 是以 **signature**（签证）信息来达到同样的目的，而 **signature** 信息则是 **IKE**（第一阶段）交换程序所得出的结果 **XAUTH** 则破坏了此一模型。

一些政府机构联合起来，以世界级的 **Common Criteria**（共通标准）评等，取代拼凑而成的国家标准。这些安全性评等通常比较为人重视，不过值得注意的是，许多通过评等的产品通常得移除一些易用的功能。目前，链路层无线安全协议尚未通过 **FIPS 140-2** 认证。链路层安全系统当中一些元件必须通过 **KIST** 的审核，整个系统方能得到认证。目前已经验证过的元件列表，参见 <http://csrc.nist.gov/cryptval/>。通过审核之前，必须逐一验证的主要元件有：

密码锁

802.11i 的 **CCMP** 所使用的 **AES** 已经通过审核。**RC4** 尚未核实几乎可以确定未来也无法通过审核，这连带使得 **TKIP** 也无法通过认证。

密码锁工作模式

802.11i 的 **COMP** 所使用的 **CCMP** 模式，于 2004 年 5 月，经 **KIST Special Publication 800-38C** 核实。

Hash 算法

将密钥扩展为密钥阶层的准随机函数，系以 **HMAC-SHA1** 为基础，目前已经核实。

密钥包装

密钥是敏感的素材，必须加密后再传送至网络 **RFC 3394** 定义了 **NIST** 密钥包装函数（**key wrap function**），目前已通过审核。

密钥衍生

2005 年 1 月，NIST 发行了实现指南（<http://csrc.nist.gov/cryptval/440-ZIFPIPSZ402IG.pdf>）。根据这份文件，NIST 打算发行 Special Publication 800-56，正式核可密钥衍生方式。

虽然很少有商用产品符合安全标准，但有个例外相当有趣。一家大型政府契约商 Harris Corporation（正好是 802.11 PRISM 芯片组的原始开发厂商）销售了一套称为 SecNet11 的 802.11 系统，使用国家安全局认证的加密机制。买家必须先经 NSA 审核。价格当然是天价：每张无线局域网络界面卡超过 3,000 美元，每部基站则叫价 1,600 美元。

22.4.1.4 网络支持

除了安全性本身，决定在哪些网络堆叠层级采行安全防护也受到其他因素的影响。最重要的非安全因素考虑与用户端软件有关。搭配工作系统内建的元件显然较具优势。既然 802.1X 申请者已经内建于主要工作系统，因此 802.1X 系统最具优势。IPsec 用户端程序通常因终端设备厂商而异。在上述两种情况中，用户端软件都只要设置一才即可。只要公司所使用的 SSID 不同于其他网络，802AX 用户端通常比较好拿捏该何时开始执行。如果已经广泛部署 Ipsec，一开始将无线局域网络视为远端访问网础或许会容易些，因为这样一来就无须对用户再教育。不过在选择 IPsec 之前，最好确定 VPN 终端设备还有余量，可以应付新用户的局域网络访问速度。

移动性的支持也是重要的考虑。为防止 IPsec 管道被塞爆，必须安排网络提供 IP 的移动性。有人称此种做法为建立一种行动 VPN。IP 层次的移动性可以由网络本身提供，只要让所有基站位于相同的 VLAN 即可，或者通过每部基站连至 VPN 服务器的重叠管道，甚至是通过 802.1X 动态指定 VLAN。既然 802.11i 相容设备能够在基站间转移安全环境（security context），对具有许多高度移动性用户的网络而言，它或许稍具优势。

对网络应用程序的支持程度，也会造成特定的协议偏好。IPsec 并不支持非 IP 协议。仍然使用 IPX 或 AppleTalk 协议的网络可能没有任何选择。IPsec 并不支持 IP 组播，其他链路层安全方案则是将 IP 组播视为一系列的组播帧。对一些迟延不能较高的应用（例如语音传输）而言，IPsec 的速度或许太慢；我尚未听说有支持 IPsec 的话机，或者任何打算推出 IPsec 802.11 电话的计划。

应用不同，需要保护的部分也就有所差异。有时候，只需要针对传输过程最弱的一环加以防护即可，链路层加密即已足够。有时候，则必须使用 site-to-site 加密，全程提供必要的安全防护。数据需要多长的防护距离，取决于离开电波之后所连结网络的安全性。如果两部基站连接至相同骨干，链路层加密或许就已经足够。如果离开电波之后，数据必须跨越不可信赖的网络，就需要某种形式的网络层或更上层的加密保护。在各个层级进行身份认证时，应该考虑哪些因素，如表 22-2 所列。

Table 22-2. Summary of major factors in authentication layer decision

Link layer (802.1X)	Network layer (VPN)
Integrated operating system components	May already be deployed with existing capacity on VPN concentrator
Protection of layer 2 network from attack	More familiar for users; less retraining is required
Better mobility architecture	Protects beyond the radio link
Support for IP multicast and non-IP protocols	Security certifications require VPN; e.g., FIPS
Fast handoff support for voice	

表 22-2: 决定身份认证层级的主要考虑因素

22.4.2 身份认证方式的选择

身份认证技术的选择，通常取决于其与现有数据库之间如何介接。首先必须知道帐号数据目前存放在哪里。究竟是存放在 Windows NT 网域，或者 Active Directory？到底是存放在 LDAP 数据库，或者 Kerberos realm。一旦知道用户数据存放在何处，该选择何种身份认证系统也就呼之欲出了。

22.4.2.1 EAP method 的选择

实际而言，要提供帧加密所需要的坚固密钥，必须使用基于 TLS 的 EAP method。如此一来，就只剩下三种选择：EAP-TLS、PEAP 与 TTLS、EAP-TLS 很难使用，因为每部工作站均需要凭证。如果没有现成的 PKI，实际上也不可能使用这种方式。PEAP 与 TTLS 十分类似，问题在于应该使用哪一种。虽然这两种协议十分相似，但在加密管道中却支持不同的身份认证方式。不妨以连接现有用户数据库的界面，来决定使用何种身份认证方式。如何访问验证所需要的用户数据，决定了应该采用何种 EAP method。其中有三种身份认证方式可以访问大多数数据库，少数情况下必须使用其他可行方式。

Password Authentication Protocol（简称 PAP）传送用户名与密码时并未加密。它只是将用户名与密码传给身份认证服务器，和身份认证服务器所存放的密码进行比对。既然未经加密，因此在未提供私密防护的网络连接中，不该使用 PAP。（用于无线局域网络时，PAP 被包裹在加密通道内，因此是安全的。）PAP 并非一种 EAPmethod，因此并未得到 PEAP 支持。PAP 最常见的用途，就是用于使用「单向加密密码」(one-way encrypt password)的用户数据库，例如 LDAP 名录或 Unix 的 `letclpassword` 档。有些系统只以 SHA-1 或 MD5 格式储存密码的单向杂凑 (on-wayhash) 值，而不是以可还原的格式来储存密码，或者储存密码本身。当用户或程序希望证明其身份时，其所输入的密码会先经过单向杂凑函数的处理，再以所产生的杂凑值与储存在用户数据库中的杂凑值进行比对。PAP 通常搭配标记卡 (token card、一起使用，因为标记卡所使用的文数码 (alphanumeric code) 可以和用户名一并传送。一些支持 TTLS/Token Card 方式的申请者软件即使用 TTLS/PAP，但并不会快取密码，因为标记码很快就会逾时。由

于几乎所有传统的身份认证数据库均支持密码身份认证，因此均可使用 **TTLS/PAP**。如果不确定的话，不妨试试看 **TTLS/PAP**。

Microsoft CHAP version 2（简称 **MS-CHAP-V2**）会进行一次 **challenge/response** 磋商。用客户端与服务器共享一个秘密（**secret**），并且通过相互搜索，以此秘密来计算盘查值。此秘密即为用户密码（**user password**）的 **MD4** 杂凑值。虽然此杂凑值无法还原，但将被当成秘密使用，因此“相当于密码”。**Microsoft** 用户端软件广泛支持 **MS-CHAP-V2**，且通常搭配 **PEAP** 一起使用，做为内层的身份认证方式。如果有现成的身份认证数据库储存在 **Windows** 网域或 **Active Directory**，**MS-CHAP-V2** 就是身份认证方式的不二选择。它可用于 **TTLS**，或者可搭配额外头信息（**EAP-MSCHAP-V2**），当做 **EAP method** 使用。

第三种常见的内层身份认证方式是 **EAP-Generic Token Card**（简称 **EAP-GTC**）**EAP-GTC** 原本设计来记录用户名与标记码。它并未提供任何磋商或私密防护。既它传递给服务器的是，不会重复使用的标记码，未提供任何防护是可以理解的。不过，最近它被当成一种 **EAP method**，用来传送用户名及相应的身份认证数据。有一种 **EAP** 方式允许直接同时传送用户名与密码，但 **EAP-GTC** 仍然可能被当成码传送协议来用‘没有任何方式能够防范 **EAP-GTC** 被当成 **PAP** 之类的身份认证方式使用，除了在实现方面把关。做为一种 **EAP method**，**EAP-GTC** 可以搭配 **TTLSPAP** 一起使用。

此外还有一些内层的身份认证方式可供使用，包括 **Challenge Handshake Authentication Protocol**（搜索磋商身份认证协议，简称 **CHAP**）**Microsoft CHAP version 1**（简称 **MS-CHAP**）与 **EAP-MDS Challenge**（简称 **EAP-MDS**）– **CHAP Microsoft CHAP** 只用于旧式的身份认证数据库。除非现有的身份认证数据库不支持 新的认证方式，否则不应该使用这类认证方式。两者均可搭配 **TTLS** 一起使用，因它们均非 **EAPmethod**。**EAP-MDS** 并未提供安全防护。它虽然被用在有线网络 **802.1X**，但几乎不会用在无线网络，因为无法防范他人窥视。

表 22-多所列的三种内层身份认证方式，或许可以搭配现有的用户数据库一起使用依所选用的内层身份认证方式、可以搭配 **PEAP** 或 **TTLS** 一起使用。此外，也可以根据各位打算使用的 **TTLS** 或 **PEAP** 实现来选择内层认证方式。标准允许 **EAP-GTC** 搭配 **PEAP** 一起使用，但 **Windows** 内建的申请者软件并不支持此种工作。

Table 22-3. Summary of common EAP methods

Inner authentication method	Outer EAP method	Type of account or user database	Comments
PAP	TTLS only	One-way hash systems (most LDAP directories, Unix password format), token cards	Probably the second most common inner authentication method. Most universal; generally works with any database.
MS-CHAP-V2	TTLS or PEAP	Windows user accounts (NT domains, Active Directory) or anything that stores an MD4 hash	Most common form of inner authentication due to the prevalence of Windows
EAP-GTC	TTLS or Cisco PEAP	Same as PAP	Only supported by Cisco supplicant on Windows

表 22-3: 常见的 EAPmethod

选定 EAP method 与内层身份认证协议后，就可以建构所需要的界面。要访问一组 Windows 用户帐号，RADIUS 服务器必须访问用户密码的 MD4 杂凑值。如果使之成为网域的成员，无须进一步设置，Microsoft 的 IAS 服务器就可以从网域系统中取得用户身份证明数据。协力厂商所开发的 RADIUS 服务器必须安装于网域控制服务器，方能够访问用户的帐号信息。任何受信赖的网域，也可以通过网域协议进行访问。

近来 LDAP 名录服务逐渐开始流行，特别是以扩充性为主要考虑的大型网站。LDAP 名录有几种访问方式。有些是通过 RADIUS 前端程序。无线局域网络设备可以直接与 RADIUS 前端对话，或是通过 RADIUS 代理服务器与 LDAP 名录的 RADIUS 服务器对话。有些 RADIUS 服务器也能够扮演 LDAP 用户端的角色。取得名录凭证后，RADIUS 服务器就能够系结至该名录，直接验证用户身份。与名录系结的好处是，可以通过 SSL 来保护名录的访问，进一步保护后端的身份认证连接。功能较少的 RADIUS 服务器也可以与 LDAP 介接，做法是以用户端所提供的 LDAP 验证与名录细节，并且只检视成功的案例。不过，只是进行系结并检视成功的案例，RADIUS 服务器还是无法访问该名录所存放的用户后设数据（user metadata）。如果名录中存放了可供无线局域网络使用的权限信息，RADIUS 服务器最好与之系结，以便将用户授权信息提供给无线设备。

Kerberos 服务器受到许多学术单位的欢迎，有些 RADIUS 服务器可以通过 Kerberos 验证用户身份。这些 RADIUS 服务器会试图从 Kerberos 服务器取得通行票(ticket)；如果成功取得通行票，则允许用户进行访问。不过，通行票与 IP 地址绑在一块，所以对「用户授权」而言并无太大用处。

22.4.2.2 身份认证架构

身份认证系统必须能够与现有的用户数据库介接才有用处。有时候，用户帐号系统并不大，网管人员所面临的主要问题，在于如何建立无线局域网络与用户数据库之间的界面。有些机构十分庞大，即使经过切割。也必须将维护用户帐号的责任分散至各地理或管理区域。不过，分属不同部门的用户工作时，可能需要跨越地理或管理区域的界限。此时，网络设计的最终目标，应该是提供用户移动性与跨界限的生产力。（不介意的话，可以称之为分散式无线局域网络的 Schengen 设计原则。）此种设计常见于大学校园中，由各学院或系所自行组建的网络。

图 22-1 显示了一座虚构的大学校园，其中包含了五个网络：图书馆、负责为一般区域与没有专属网络的系所提供网络的 IT 服务中心。自行组建独立网络的工程学院。医疗中心以及商学院。各部门自行维护本身的用户数据库，采用各自偏好的格式。为了提供无线局域网络的访问，可以通过一个 RADIUS 前端来访问个别的数据库。其中，用户数据库与 RADIUS 前端并未实际标示出来。

Figure 22-1. Mesh authentication architecture

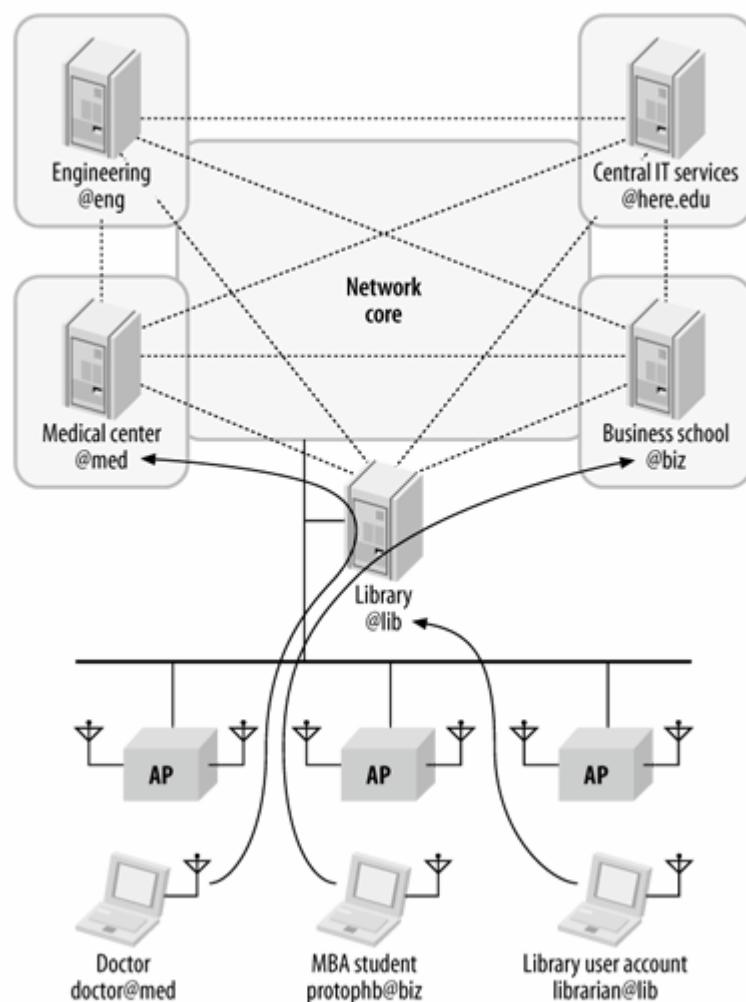


图 22-1：网状身份认证架构

设计身份认证架构时，目的是提供一种身份认证机制，让单一用户帐号的使用得以跨所有园区网络。举例而言，任何进入图书馆的用户，不论是学生或教职员，都应该能够以设籍网络（**home network**）的身份使用图书馆网络。如果各部门的 **RADIUS** 服务器间存在信任关系，且能够彼此传递身份认证要求，那么单一帐号即已足够。帐号系指定给 **RADIUS** 领域，可以将身份认证要求绕送给事先定义好的服务器。图书馆的 **RADIUS** 服务器知道来自 **user@med** 的要求必须转送给医疗中心的 **RADIUS** 服务器。如果该服务器接受此用户，则允许该用户进行访问。

网络间的信任关系乃是此种架构的关键成份。如同在移动电话领域，要能够随处访问网络，「设籍」网络与「参访」网络之间必须存在一种漫游协议。网管人员必须倚赖这种信任关系，因为他们必须开放访问权限给其他单位所验证的用户。在校园环境中，此种漫游协议可能是非正式的。在更大型的网络上，或许需要正式的法律文件来达成协议。一个由欧洲大学所组成的联盟 **EduRoam** 在欧陆组建了一个 **RADIUS** 网状网络。加入 **EduRoam** 之前，必须签署正式的协议文件。

在这类环境中，计费机制也可以派上用场。校园图书馆必须提拨预算购置教学资源，但不包括组建先进的网络服务。通过计费机制，网络服务供应商（例如图书馆本身）可以为来自其他网络的用户提供服务，以此做为网络支出的经费，而不必面临经费无着的困境。

授权

辨识用户与验证身份后。接下来或许需要限制网络的访问权限。限制访问权限有几种不同的方式，比较常见的两种方式是以访问控制表进行封包过滤，以及 **VLAN** 的指定。从某些角度而言，后者是比较方便的做法，可以利用 **VLAN** 间现有的封包过滤机制，为不同用户群组指足适用的塞本规则。

通常，用户帐号当中会包含了若干「后设数据」（**metadata**），用来记式该用户适用何种授权。这些数据通常是针对机构的角色而定。角色必须被转换为具体的行动，例如「将来自 **Group A** 的所有用户 **VLAN A}**，或者「**Group R** 的设备采用 **Filter** 规则。

身份（**Identity**）与角色（**role**）离不开用户帐号，这些数据通常会被转换为 **RADIUS** 服务器与无线局域网络设备本身所依循的限制。角色不同，**RADIUS** 服务器就会传回不同的限制属性。**RADIUS** 属性也可能触委无线局域网络设备更进一步、更为详细的行动。举例而言，**RADIUS** 服务器可能为来自特定设备的数据指定某种过滤规则，但可以确定的是，这些限制的细节将由无线局域网络的硬件来定义。

22.4.3 加密方式的选择

选定身份认证方式后，链路层加密方式的选择就比较简单了，因为必然会挑选大多数硬件所能支持的最坚固协议。这些协议的配置设置方式几乎完全一样，从用户的角度来看，它们的功能没有什么两样。

关于静态 **WEP**，该说的都已经说了 • 除非别无选择，否则不要使用静态 **WEP**。几乎所有通用型设备均已支持较佳的协议，但一些特殊应用设备（如 **802.11** 电话或条码扫描机）除外。如果有安全上的考虑，或许需要停止部署这类设备，如果这些安全问题无法通过其他方式得到适当的解决，或者评估后显示风险极高的话。

使用动态产生密钥的 WEP 显然较好，因为经常变换的密钥可以防范针对 WEP 发动的攻击，如第五章所述。对通用型运算设备而言，起码应该使用动态 WEP 来保护用户数据。有时候，必须更新驱动程序方能使用动态密钥，不过 2000 年中以后驱动程序，大多已支持动态密钥。

不过就算搭配动态密钥，WEP 还是存在种种瑕疵，因此在写作本书当时，大多数维路均采用 TKIP 来提供起码的安全性。TKIP 的硬件需求和 WEP 一样。因此几乎所有的 802.11 设备均支持 TKIP。TKIP 也需要软件的支持，但已经十分普遍。TKIP 与 WAP 已经内建于各式工作系统，如 Windows XP 与 MAC OS 10.3。Linux 尚未广泛支持 WPA，因为驱动程序架构尚无法整合申请者软件，虽然未来可望能够进一步整合。

计划升级为更安全的协议时，大多数机构应该以 TKIP 做为升级的目标。至于动态 WEP，只能视为最起码的要求。

如果链路层加密要求高度的安全性，CCMP 就是不二选择。TKIP 要求，协议检测到密钥遭受攻击时，必须提供反制措施以降低威胁。需要反制措施，无异承认该协议本身强度存在基本的限制。不过，安全性并非全无代价。在所有链路层加密协议中，CCMP 对软硬件的要求最高。它只能用于具备 AES 硬件加密能力的无线界面。近来的网卡几乎均已支持，但较旧的网卡则否。如果各位手上有一堆无法支持 AES 硬件加密的旧式网卡，想要升级为具备 AES 能力的硬件不仅所费不小，也是一项不小的挑战。

CCMP 可以提供最佳的安全性。不过它对软硬件的要求也最高。有些膝上型电脑厂商只采用最便宜的芯片组，因此除非另外购置网卡，否则根本无法支持 CCMP。

22.4.3.1 支持多重 SSID.

802.11 安全协议架构，容许在同一部基站中，同时使用多组加密协议。用户端可以选择使用其中一种协议。单点传播帧的加密通常会采用接收端所支持的最坚固协议，群组帧则是使用所有系统均支持的最坚固协议来加密。如果基站有一组支持 WPA 的已连接工作站，但另外有一部只支持动态 WEP，则群组密钥必须使用动态 WEP。

标准并未限定必须支持哪些协议，不过实现上混用不同类型的加密协议可能会造成问题。其中最常见的限制是，大多数用户端软件并未支持以 CCMP 密钥加密单点传播帧的同时，另以非 CCMP 加密类型（TKIP、动态 WEP 或静态 WEP）来加密群组讯。未来或许会有驱动程序支持此种混合模式。目前，通常是以另外一个 SSID 来支 CCMP。也就是，一个网络支持基于 RC-4 的加密协议，一个网络只支持 CCMP。

遗憾的是，采用两组 SSID 的确可能造成用户的混淆，因为连接至哪一个 SSID，纯粹操之在用户手里。

用户端软件的限制，导致无法对相同的 SSID 同时使用 CCMP 与 RC4 加密。要同时使用两者，802.11 基站必须支持多重 SSID。

22.5 私设基站

网管人员所面临的主要风险之一，就是用户私自架设未经授权的 802.11 网络。所谓的「私设」（rogue）基站，可能造成相当大的威胁。最主要的威胁是，用户私自架设的基站，不像经授权部署的设备具备完整的安全性配置设置；用户或许没有足够的能力与意愿，正确地用攸关安全性的功能。即使这些设备已经采取适当的防护，未经授权的设备也可能干扰现有网络的运作。

22.5.1 检测

对付私设设备的首要步骤，就是确定它们是否存在。要确认未经授权设备的存在，必须使用某种电波设备。**802.11** 设备刚问世那几年，基站还十分昂贵，因此只需要携带一部膝上型或掌上型封包捕捉器（sniffer），就可以扫遍所有基站。当有更多人熟悉 **802.11**，私设设备的检测便需要转变为持续、自动化的程序。考虑到成本与管理因素，如今检测程序已经被整合进大多数的无线局域网络主流系统。取决于厂商的实现方式，检测元件可以是一种扫描功能，定期搜寻未经授权的设备，也可以是特定的扫描设备。未经授权设备的扫描，可以是被动地聆听数据、**Beacon** 或 **Probe Response** 帧，或者主动使用 **802.11 Probe Request** 帧，让未经授权的网络自动现形。

为了达到效果，检测程序必须涵盖所有可用的 **802.11** 频道。起初，企业的部署方案通常采用 **802.11b**，其所使用的电波界面芯片组并无法工作于 **802.11a** 频段，也无法使用 **802.11a** 的调制技术。有些私设基站的人比较聪明，故意采购 **802.11a** 装买，理由是比较不会被网管人员检测到，况且网管人员所使用的分析工具，也只是针对 **802.11b**。

无线局域网络基础设施必须内建检测能力，否则就需要使用独立设备。网管人员通常必须在提供给用户的服务品质、检测信息的品质与成本之间做出取舍。专用的检测设备可以提供最好的检测结果，但成本最高。以原本提供用户服务的设备来检测未经授权的设备虽然比较便宜，但可能会中断或拖累原本的服务。

搜寻未经授权的部署时，主要是针对私设设备所显露的迹象。至少，检测器必须搜寻是否存在于其他 **Beacon** 帧。所有基站与 **ad hoc** 网络均会发送 **Beacon** 帧。比较完整的 **802.11** 系统也会观察工作站的数据，并将电波范围内的工作站列表拿来跟已连接的工作站进行比对。只要出现于前者的工作站并未出现在后者，就是连接至未经授权的基站了。

22.5.2 实际定位

一旦检测到私设基站，在采取任何行动之前，网管人员通常希望能够找出它的实际位置。有时候，只要知道有私设基站存在，让网管人员找到用户并予以停用即可。如果需要主动反制，最好是锁定特定区域的私设设备。目前，有几种主要的定位方式：

- 1.计算最近基站半径
- 2.三角定位
- 3.RF 指纹辨识
- 4.时间差

要找出私设基站所在，最简单的方式是利用最近基站的半径，如图 22-2(a)所示。在网络上搜寻 **MAC** 地址后，就可以根据检测到该设备的基站之位置，粗略判定其位置。开放空间的无线电信号传播系依循已知的物理模型。根据检测到该设备的基站所接收到的信号强度，就可以计算出最大半径，只要知道以最大传输功率进行传输之设备的最大半径可以到多远，再与所接收到的信号强度进行比对即可。图 22-2(a)中，基站所接收到信号的强度，可用来判定其与最近基站间的开放空间距离，但并无法提供任何线索，足以判定该基站位于圆周上哪个位置。

Figure 22-2. Radius to the closest AP

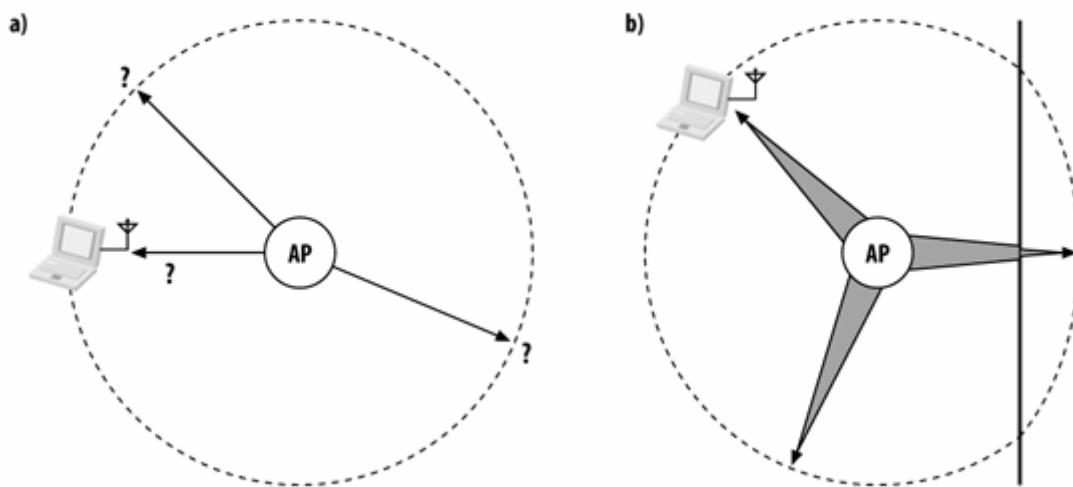


图 22-2：最接近基站半径

基站半径计算有几项缺点。首先，以最大功率传输的信号。其开放空间半径较实际半径长。开放空间模型所容许的半径高达 100 英尺，所得出的 30,000 平方英尺面积过大，因此没有实际用处。比较好的定位方式，是先以一些定位工具为整个电波环境建立一个数理模型，并将特定路径上的建筑物纳入考虑。在大多数办公大楼中。有效覆盖半径通常是开放空间的一半以下。将覆盖半径从开放空间 100 英尺的理论值减少为特定环境多 0 英尺以下的实际值，就可以将目标缩减至较少的 8,000 平方英尺。不过，8,000 平方英尺仍然相当于 70 至 100 个隔间（cubicle），这取决于隔间的大小以及办公室的平面配置。图 22-2(b)的右边有一道墙，它会缩短覆盖半径，因为电波信号必定会穿透墙面。箭头的厚度表示某个定点的信号强度。当电波信号行经墙面，信号强度就会降低，覆盖范围因此变小。如果这类建筑物为数不少，修正覆盖半径的效果就愈好；在充满隔间的典型办公室中，效果就没那么显着，因为信号可以传递至较远的距离。

计算最近基站半径的做法，可以进一步使用三角定位加以改善，如图 22-3 所示。三角定位原本是指根据其与三个已知点的距离来进行定位。有些无线局域网络系统所使用的“三角定位”（triangulation）技术，可以探用三个以上的量测点。重叠的覆盖区域。重叠的半径，有时再加上或然率的模拟，可以用来搜寻设备的可能位置。图 22-3(a)中，三部基站的重叠覆盖区域被用来猜测设备的所在位置。和计算最近基站半径的做法一样，三角定位算法可以搭配对建筑构造的了解，得到比较精确的定位。图 22-3(b)中，若将两面墙所造成的信号阻隔效应也纳入考虑，预测的结果就更为精确。

Figure 22-3. Triangulation

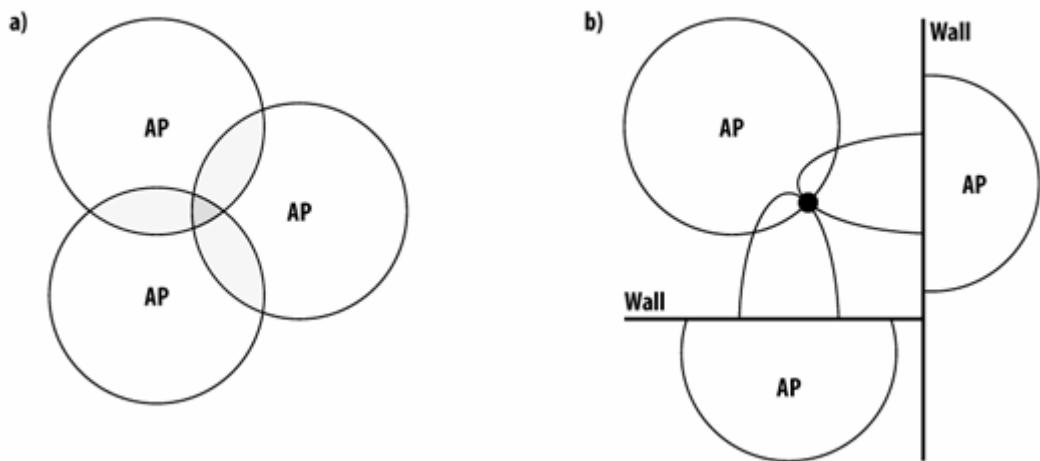


图 22-3: 三角定位

如果采用 RF 指纹量测，定位就可以更加精确。取得无线电波与建筑物的互动数据后，就可以根据这些数据来修正数理模型，了解无线电波的实际行为。要组建一套指纹数据库，必须先将设备摆在已知定点然后加以量测。接收信号强度及其他信号特性等数据，随后会被当成该位置的指纹 (fingerprint) 加以储存。指纹包含所有难以计算的信号传播特性，例如墙面的反射以及多重路径干扰。要定位未知的设备，可以拿它的信号特性与指纹数据库进行比对，以便精确地定位出所在位置。定位预测的品质，取决于已建立的指纹数，这些指纹通常必须通过实地探勘来建立。虽然指纹辨识有助于改善定位信息，但需要搜集大量相关数据与建立够大的指纹数据库，方能达到想要的精确性。

最后一种定位方式，就是根据接收信号的时间差。信号强度受到一些因素的影响，包括建筑物构造。不过，无线电波总是以光速行进。可以在不同量测地点，以三角定位计算接收信号的时间差。虽然这种技术可以精确定位，由于无线电波的行进速度很快，因此需要使用十分精确的对时技术。图 22-4 中，两部基站用来量测来源信号的到达时间。经过一段时间，信号到达第一部基站。定位系统必须十分精确地计算出信号到达两部量测设备的时间差。无线电波每十亿分之一秒行走一英尺，因此定位设备必须能够分辨信号到达两部量测设备的细微时间差。虽然理论上可行，信号时间差的做法通常需要用到相当特殊的装备与计时仪器，它们的精确度是一般基站所无法比拟的。

Figure 22-4. Differential timing analysis

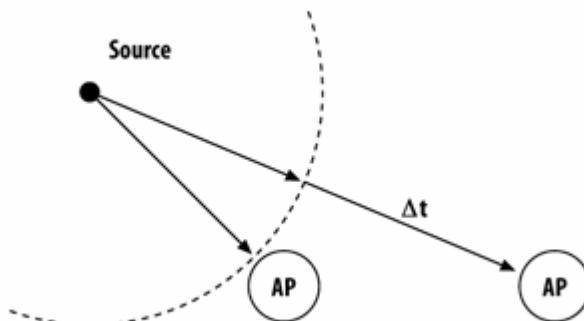


图 22-4：时间差分析

22.5.3 关闭私设基站

有些产品能够自动关闭未经授权的网络，这种功能通常被称为「封锁」（containment）或镇压（suppression）。技术上的细节虽然不同，但同样是使用一些协议上的技巧，来阻止或打断私设基站的连接。一般而言，这些做法若不是阻止其他工作站连接至私设基站，就是设法中断现有的连接。有些技巧是利用无须验证的控制帧，以基础型设备来冒充私设基站。未来 802.11 协议如果对重要的网络控制信息进行验证，这种做法还会有多少反制效果尚待观察。图 22-5 显示了两种对私设网络发动阻绝攻击的主要技术。

Figure 22-5. Rogue suppression techniques

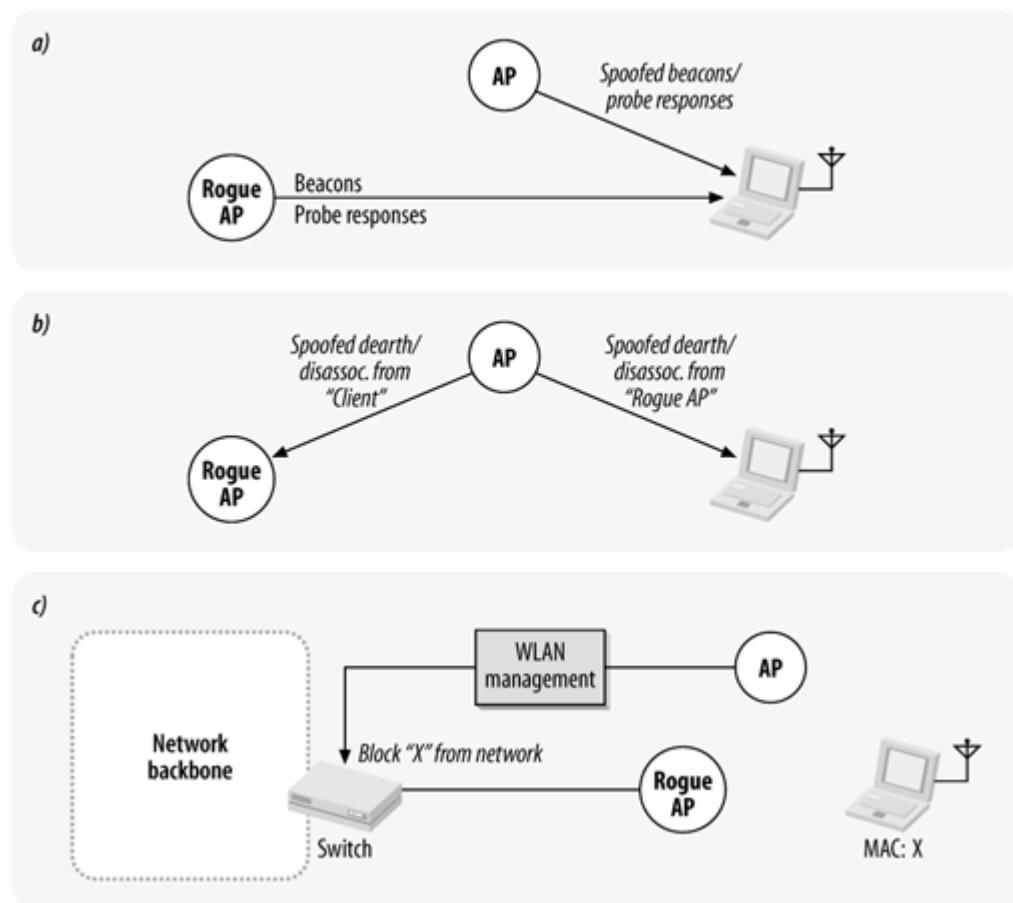


图 22-5: 私设基站封锁技术

要中断连接程序，可以使用一些设备送出伪造的 Beacon 或 Probe Response 帧，如图 22-5(a) 所示。既然 Beacon 或 Probe Response 帧不会经过验证，因此基站可以轻易冒充私设基站。伪造的帧所包含的信息，可能和私设基站所传送的帧彼此冲突，令工作站不知所从。如果发现某个网络既是加密网络（在 Beacon 帧中设置 Protected Frame 位元），又是未加密网络（清除 Protected Frame 位元），有些工作站就无法与之连接。伪造的 Probe Response 帧也可以达到相同的效果。有些无线局域网络系统会试着捕捉工作站的连接要求，把跟私设基站连接的工作站加以俘虏，以避免造成损害。至于已经与私设基站连接的工作站，可以使用 Disassociation 与 Deauthentication 帧来处置，如图 22-5(b) 所示。这些信息并未经过签署，因此容许网络系统将工作站踢出私设基站。要以伪造信息干扰工作站的工作并不简单。由于多重路径，以及基础设施与工作站间的相对位置，均会造成影响，因此不见得能够完全拦截所有这些打算连接至私设基站的工作站传输。有些设备还会以工作站的地址送出伪造的 Deauthentication 给私设基站，迫使私设基站解除这些与其连接之工作站的连接。有些无线局域网络管理系统可以进一步限制私设基站可能造成的损害。如果可以辨识出与私设基站连接的工作站，无线局域网络管理系统理论上会在骨干网络采取行动，不让此工作站连接使用骨干网络的服务，如图 22-5(c) 所示。

封锁私设基站有趣之处，在于 802.11 网络通常是源自用户有移动性的需求。为了确保涵盖范围足以让私设网络停摆，必然得使用相当数目的封锁设备。事实上，封锁所需要的 802.11 基站数量，相当于用来提供服务的基站。为了提供必要的封锁能力，通常需要部署足够的基站，才不会影响正常的网络访问。之所以逐渐以 802.1X *supplicant* 来取代基站，是为了可以在提供服务之前先与网络进行身份认证。用 802.1X 的有线网络可以在私设基站造成问题之前即予以回绝，而不是等到它们出现后才进行封锁。

22.5.3.1 律师的忠告

封锁私设基站可能会被视为意图干扰无线网络的电脑犯罪。（请谘询熟悉当地法规的律师，毕竟这并不是我的专业。）假冒私设基站让它们因此停摆的设备，主要是设计来干扰无线网络的工作。如果该网络属于邻居或对街的咖啡馆所有，这种行为可能已经触法，或者导致民事诉讼。

为了避免替律师制造更多就业机会，在启动反制攻击之前，最好确定私设基站的确连接到自家所防护的网络。举例而言，如果私设基站属于对街咖啡馆所有，如果有人导致他们的网络停摆，他们大概不会善罢干休。容纳许多办公室的大型建筑必定会有许多相邻的无线网络，对这些网络不该採取反制攻击。（如果隔壁就是精于电脑领域的律师事务所，对他们的基站采取反制措施无疑是自找麻烦。）

最近 FCC 管制当局明文禁止，业主声称拥有电磁频谱的任何权力。因此，对承租户或邻居发动私设基站反制攻击是相当不智的。

第23 章 网络规划与工程管理

无线局域网络的部署之所以不简单，部分是因为整个程序并不是那么结构井然，特别是相较于有线局域网络的部署。如今组建 Ethernet 网络已经十分容易。几乎每个人都拥有各自的交换式 Fast Ethernet（或更快的）连接端口。核心交换设备甚至使用更快（或者经过合并）的链路。至于布线方面，不少厂商已经累积了多年的经验，经过这么长一段时间，对于如何布线基本上已经有相当的共识。

相较之下，无线网络就像是蛮荒的西部。网络至终端用户间的服务品质取决于用户与最近的网络设备之间的距离，且随之递减。网络性能（capacity）受到覆盖范围的大小以及建筑物的实际格局所影响。从电波传输的角度而言，每栋建筑物均有其特性，而且到处都有可能出现意外的干扰，例如微波炉、电线或严重的多重路径干扰。

更糟的是，不仅是你自己本身，甚至连用户或邻居的所作所为，都可能对网络介质的品质造成影响。

打算部署无线局域网络时，可以先从明显的问题开始：需要多少基站？应该摆在哪里？要回答这些问题，必须进行实地勘探（site survey）。实地勘探通常在无线局域网络工程初期便开始进行，而且经常是整个网络工程计划相当重要的部分。本章仍是从技术的观点，说明实地勘探与工程本身密不可分的本质。在规划阶段需要做些什么，才能够成功部署？基站的摆设规划属于无线局域网络推行（roll-out）的一部分，因此本章将协助各位拟定自己的部署计划，包括实际的配置计划。

无线局域网络的规划程序分为几个阶段。需求的搜集，不见得需要花费很长的时间来准备冗长的文件；规划程序结束后，对于网络的覆盖范围与容量需求，应该就会了然于胸。为了修正需求，并将之落实为符合需求的设计，可能需要在现场花费不少的时间与精力。

23.1 工程规划与需求

一旦确定要组建无线局域网络，最好及早着手规划。无线局域网络技术仍在持续演进当中，网管人员愈早参与，结果就愈加完美。如果无线局域网络要装设在新建大楼，在建筑物的基本架构图出炉后，就可以尽早让网管人员参与，特别是基站的摆设位置有所限制时。我曾共事的一家机构对空间的美感要求极高，基站最后只能置于钢骨结构旁边，而且被迫隐藏在隔间封板（paneling）之后。如果网管人员早点参与规划，不仅能够找出更适合的摆设位置，也不用浪费那么多金钱。

规划有线网络相对比较简单。虽然视网络规模需要不同程度的经验，但基本上，网管人员都已经相当熟悉整个规划程序。有线网络介质的行为是可预测的，固定式网络的升级也十分容易。无线局域网络技术还没有那么成熟，相形之下规划程序就更为重要了。

无线局域网络工程规划通常被视为实地勘探。然而实地勘探只是其中一环，成功的无线局域网络部署需要好几回合的勘探，每次勘探的目的不尽相同。预计安装于新建大楼的无线局域网络，在施工过程中可能必须来回勘探好几次。如同以往，在“破土”进行网络扩充工作（"breaking cable" on a network expansion）之前就应该着手规划。

实地勘探是组建无线局域网络的核心工作。不过，实地勘探要有结果，事前的准备工作相当重要。在“破土”进行网络扩充工作之前，最好事先搜集技术上的需求与咨询必要的信息，以便理清使用者心目中有哪些期望是重要的。你可以使用下列的检查表来记录使用者的需求；各项要点将在后续各节详加说明：

传输量

需要多少传输量？这个问题部分取决于将用在无线局域网上的设备类型，如果是可以显示较大与较复杂图片的 PC-like 设备，自然希望无线局域网络愈快愈好。大多数情况下，通常会选择采用 54-Mbps 物理层的 802.11a 或 802.11g 网络。

覆盖范围

需要覆盖哪些地区？需要完全覆盖吗？有些区域比较难以覆盖。电梯通道（elevator shaft）通常位于中央大楼的核心，比较难以涵盖。要在电梯里头提供信号不难，但大多数用户或许无此需要。

用户密度

除了用户所在位置，也需要注意用户数的多少。公共场所的用户数通常比较密集，例如会议室、大厅与餐厅。

可移动性

无线局域网络已经不再是玩家专属的新奇玩物。几年前，在过渡阶段，人们还可以接受网络仅提供自动重新设置配置的服务。不过当无线局域网络日渐成熟，设计人员在设计网络的时候，还必须考虑如何在覆盖区域内提供持续的连接。

用户数目

有多少人会使用无线网络，他们心目中所期待的服务品质为何？记得将未来的成长率计算在内！

物理上的考虑

是否需要为无线局域网络骨干重新铺设网线，或者可以利用现成的架构？这些新增加的基站如何供电？基站与天线能否暴露在外，或者必须隐藏起来？

美观上的考虑

无线局域网络需要隐藏到什么程度？基站是否允许被用户看到，或者需要隐藏起来？

逻辑网络架构

大多数情况下，逻辑架构必须在整个连续的覆盖范围内支持相同的 IP 地址区段。在逻辑网络架构下，用户或许会取得不同的 IP 地址。随着近来的技术发展，目前已经不需要再根据 IP 定位架构来调整可移动性区域。

应用上的特性

是否有任何应用对迟延十分敏感？是否有任何应用必须提供及时（time-critical）的数据？

安全需求

部署之前、各位或许想要设计出一种网络，它既可以解决本书所探讨的安全问题，也可以提供一个足以防范未来可能攻击的可靠环境。安全议题与架构，已经在前两章探讨过了。

网络所在环境的考虑

影响无线电波传播与信号品质的因素很多。建材，结构与楼层规划均会影响无线电波在整栋建筑物中的行径。干扰势不可免，但是每栋建筑里的干扰程度亦不尽相同，而且温度与湿度也会造成些许的影响。及早进行实地勘探有助于掌握相关因素，而详细的实地勘探，可以在实际组建之前发现问题所在。

工程管理

和所有工程一样，预先规划时程与预算是不可或缺的。本章并未提供任何非技术层面的指南，因为每个组织的情况通常不太一样。

23.2 网络需求

和其他网络技术一样，部署无线局域网络之前，必须先回答三个问题：“部署在哪？”、“速度有多快？”与“经费有多少？”通常，成本是通过预算程序独立指定的，网络设计人员必须试着在预算的限制下提供最佳的局域网络服务。“部署在哪？”是指无线服务所涵盖的地区组合。一般通常希望能够涵盖所有地方，但有些工程为了节省成本，会将部署规模缩小至会议室与公共空间。“速度有多快？”是指无线网络的性能（capacity）。无线局域网络用户端的速度取决于其与基站之间的距离，以及基站与工作站之间障碍物的多少。要组建一个高传输率网络，必须专注于如何缩短工作站与基站的一般距离。有些实体空间会对无线电波造成相当程度的障碍，需要相当数量的基站方能完整覆盖。

网络设计人员必须在这三项变数中取得平衡，方能够建构正确的网络。在一些环境中，建筑物本身的实体设计很容易阻挡电波的传波，因此必须缩小网络的覆盖范围，性能也会因此受到影响。有些网络预算有限，只求能够符合最低性能要求。在比较少见的情况下，或许可以针对整个覆盖范围提供较高的频宽，不必考虑成本问题。设计人员必须持续针对这三项设计因素进行调整与优化。当无线局域网络的用户逐渐成长，网络本身也必须随之扩充。一开始特定区域的部署，随后

可能必须提供完整的覆盖范围。以覆盖范围为主要考虑，且尽量减少基站数目以节省成本的网络，日后或许会转变为性能较高的网络，以满足用户的额外需求以及日渐增加的用户数。要在这三种需求中取得平衡，纯粹是一种艺术。幸运的是，有一些工具可以协助我们在这些取舍间做出决定。

23.2.1 覆盖范围需求

网络有其覆盖范围。有线网络的覆盖范围，取决于分布各地的网络连接端口。要提供网络服务，必须布线与提供连接端口。无线网络提供覆盖范围的方式不同，因为无线网络的传输介质遍布整个空间，并且能够穿透墙壁。掌握无线电波的空间传播形态，乃是了解如何覆盖整个网络的关键。

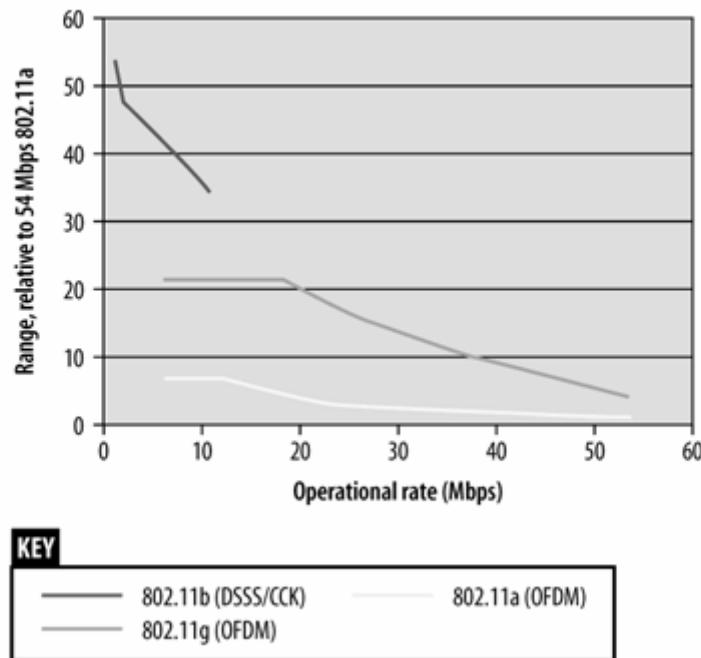
首先必须回答的问题是，要覆盖哪些范围。是涵盖整栋建筑与园区，或是在特定区域提供无线网络？一般的做法是先在特定区域试行，并藉此熟悉技术。有时候，试行的范围也涵盖 IT 部门，大厅或会议室等公共场所也常涵盖其中。

对提出无线局域网络覆盖范围需求的人而言，无所不在(*ubiquitous*)是个流行的字眼，不过对必须满足此项要求的人来说，可能是个恐怖的字眼。这是否意味着必须涵盖建筑物的每一寸空间呢？例如，真的需要为洗手间提供高品质的服务吗？对公共建筑而言，是否连逃生路线也包含在内？

涵盖室内区域需要多少部基站，取决于许多因素。首先，这与建筑物的构造有关。墙面愈多，意味着无线电波将遭受更多物质的阻隔，因此需要更多的基站。不同材质对无线电波链路有不同的影响。以相同材质而言，墙面愈厚，信号损耗愈大。信号功率最容易受到金属影响，因此电梯间（**elevator shafts**）与空调风管（**air duct**）皆会严重妨碍通讯品质。有色或经涂覆的窗户通常会严重干扰无线电信号。有些建筑使用金属电镀天花板，或在地板镶入大量金属。木材与大多数玻璃窗的影响较小，不过防弹玻璃就见不得了。[注] 砖块与混凝土的影响介于金属与一般未经处理的玻璃之间。

第二个主要因素是打算提供何种速度。只是提供无线局域网络访问服务与提供特定的传输率完全是两回事。**802.11a** 的速度介于 6 Mbps 与 54 Mbps 之间。速度愈低，覆盖范围就愈大。相较于只是提供 **802.11** 访问服务的网络，让整个网络支持 Mbps 的传输率需要更多的基站。图 23-1 显示了三种主要 **802.11** 物理层的比较，以及如何在距离/传输率间做出取舍。较高的数据传输率时传输距离相对较短。

图 23-1 是根据开放空间损耗的理论值绘制而成。它显示了 **802.11 a**、**802.11b** 与 **802.11g** 于各种速度下的相对传输距离。计算时，我使用了典型的传输功率(**802.11b/g** 为 20 dBm 或 100 mw，**802.11a** 为 11 dBm)，然后计算每一种速度在何种距离，功率会降至电波灵敏度以下。至于典型的灵敏度，我是以 Cisco a/b/g 无线网卡的规格做为参考。图中所显示的传输距离系相对于最小距离，亦即 **802.11a** 之最高传输率 54Mbps 的最小距离。

Figure 23-1. Relative range comparison of free space loss

为了达到容量目标，相邻基站的覆盖范围必须有相当程度的重叠。如果目的是在特定区域提供高速的传输(比如 36 Mbps)，较低速的传输必然会出现更大的重叠区域。规划时切记保持某种程度的重叠，方能够确保换手工作(handoff)，同时尽量减少基站的数量，以维持最佳容量，这些是设计无线局域网络时必须特别注意的取舍。

覆盖范围的最后考虑因素是网络本身的目的什么。无线网络有特定的覆盖范围，但传输与接收范围可能并不相同。接收范围通常较广，特别是并未将基站的传输功率开至最大时。增加基站密度但调低功率的好处是，在接收范围内会有比较多的重叠部分。只要用户私下部署未经授权的基站，很难不被网络中的基站检测到，而且可以更精确地定位其所在位置。

相较于室内的覆盖范围，户外有另外一套不同的取舍与工程要求，而且通常牵涉到，在恶劣的气候下，使用者是否需要如同往常在外工作。【注】特定的应用也适合将室内/户外覆盖范围一并考虑；例如，机场或许打算为航空公司的传输设备提供户外访问服务。将设备置于户外向来是种挑战，大部分是因为设备本身必须抗风化，必须符合不少环境或安全法规。置于户外的设备必须坚固耐用，通常必须具备防水或抗风化能力。一种解决方案是将基站设备在室内，然后在户外布设天线，不过通常很难找到长度合适的外接天线，就算可以，线材的损耗通常也很严重。有些厂商会在价目表上列出抗风化器材，特别是当他们销售的设备，主要用于大规模的室内/户外安装时。抗风化机壳可能必须符合其他安规标准。国际电工委员会(International Electrotechnical Commission, 简称 IEC) 60529 标准中列有测试程序，可用来评量耐水与砂粒的能力。在美国，外部机壳也必须符合国家电机制造业协会 (National Electric Manufacturer's Association, 简称 NEMA) 250 标准。

23.2.1.1 覆盖范围与实际安装限制

一般使用者的需求中，通常包含所期盼的覆盖范围，不过实际上可能会有所限制。比较常见的限制，包括无法提供电源或网络连接。有些机构要求基站与天线必须予以隐藏，也许是为了维护网络的实体安全，也许只是为了保持建筑物的美观。

基站通常挂得愈高愈好。就像试图夺取战地制高点的童子军，当基站位于所有障碍物之上时，运作容量最好。将基站置于小卧室（cubicle）或其他物体之上，通常可以让信号更稳定地传得更远。有些基站提供壁挂套件，可以固定在墙壁或倒吊式轻钢架天花板（dropped ceiling tile）的吊筋（suspension bar）上。有些厂商建议将基站安装于轻钢架天花板之上，再搭配穿透轻钢架天花板的外接天线。天花板厂商甚至已经开始进入这个市场，生产整合天线的天花板材。

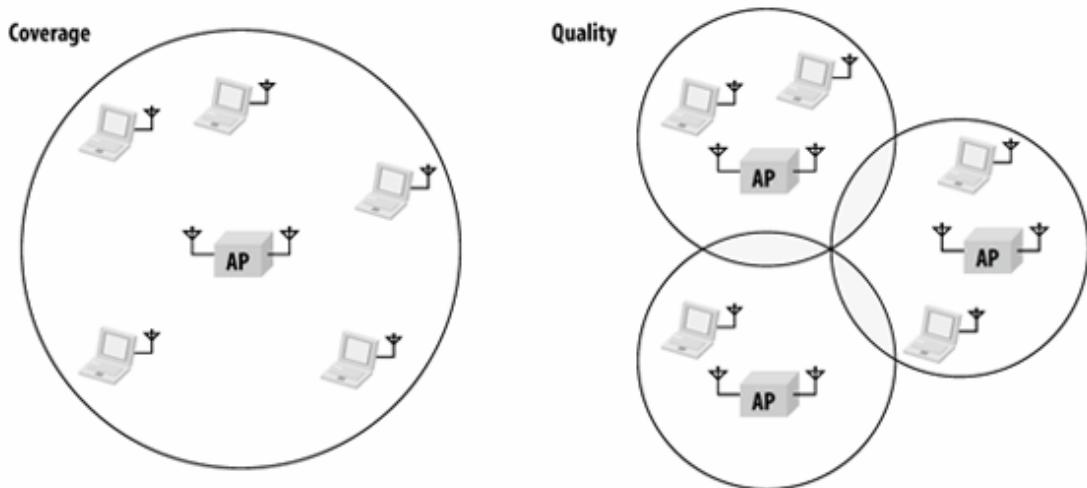
许多商业建筑使用所谓的倒吊式天花板（"dropped" ceilings），在真正的天花板板（actual ceiling）之下，另外悬挂轻钢架天花板（ceiling tile）。把网线与电线置于轻钢架之上，跟空调风管（air ducts）放在一起。有些建筑将整栋建筑的空调风管系统置于轻钢架与天花板之间的空隙。安全标准规定，置于空调风管空间（plenums）的物品，不得危及建筑物的用户。万一失火，建筑物内部人员所面临的最大危险，就是浓厚的黑烟可能会遮蔽视线，阻碍逃生的路线。置于空调风管系统的设备一旦产生烟雾，就会立即弥漫整栋建筑。因此，为了保护建筑物内部人员，置于天花板之上的设备必须符合一些特定的安全标准。如果打算将无线局域网络设备置于天花板之上，务必确定它们是否符合防火等级（plenum-rated）。除了基站，也包含任何附挂于天花板之上的所有辅助设备。灌电器通常不符合防火等级，因为它们通常可以安置于集线槽。布于天花板之上的线材，几乎可确定的是必须符合防火等级。防火安全标准是由 Underwriters Laboratories 所制定，并出版为 UL 的 2043 标准。UL 也负责测试产品是否符合标准，通过检验才予以认证。

23.2.2 容量需求

覆盖范围并非无线局域网络设计的完结篇。在负载范围内，基站的作用类似集线器。对特定覆盖范围而言，无线频宽是固定的。在覆盖范围内，802.11b 基站能够传送 6 Mbps 的用户数据。802.11 网络实际上使用的是分享式介质。除非无人与之竞争介质，距离基站甚远的用户才有办法使用 6 Mbps 的速率。当更多用户使用网络，同样的 6 Mbps 必须由所有用户共享，而协议本身必须公平地（或者不公平地）配置频宽给各工作站。

对服务用户的网络而言，必须在覆盖范围与服务品质间做出取舍。只要搭配高增益外接天线，就可以使用较少的基站，但频宽就必须由较大的范围来分享。基本来讲，扩大覆盖范围的做法并无对错可言，特别是用户密度较低的时候。有些部署会使用单一基站搭配外接天线来覆盖较广的区域，因为对频宽的需求并不高。有些用户不俗的 K-12 学校即属此类，可说是图 23-2 左边的代表。图 23-2 右边，用户较多的网络会倾向使用覆盖范围较小，但数目较多的基站。网络工程师有时会借用可移动电话的术语，称此种网络具有许多“微蜂窝”（microcells）。既然覆盖范围较小，基站就可以服务较少的用户（虽然无法保证）。图 23-2 中，右边的图形将相同的区域划分为三个区域。因此，每部基站只需要服务较少的工作站，每部工作站的传输率也因此提高。

图 23-2：覆盖范围和服务品质的取舍

Figure 23-2. Coverage/quality trade-off

评估需求时，区域总和频宽（或是它的近亲，单位面积的传输量）是相当有用的指标。图 23-2 中，左右两个网络覆盖相同的面积。不过由于具备三部基站，因此右边的网络可以提供三倍的传输量。并非所有网络均需要高区域总和频宽，至少一开始是如此。当无线局域网络逐渐受到欢迎，图 23-2 中的用户从 5 位变成 10、15 甚至 50 位时，就需要进一步增加区域总和频宽。

需要为每个用户保留多少频宽呢？一种做法是对网络应用与容量需求进行详细研究，然后据以设计网络。不过以实际情况来看，大多数网络似乎都是以“测不准原理”(Schrodinger's Cat) 在运作着：只要有封包在传送，网络就会持续运作；一旦深入探讨它的工作方式，它便停止运行。一般而言，大多数无线网络工程均始于“好像有此需要”的模糊概念。而不是“它应该用起来像有线网络”的想法。既然没有任何反对意见，我建议至少为每个用户保留 1 Mbps 的频宽。802.11a 与 802.11g 网络允许为每个用户保留较高的速率，特别是将流量估计地比较高时。

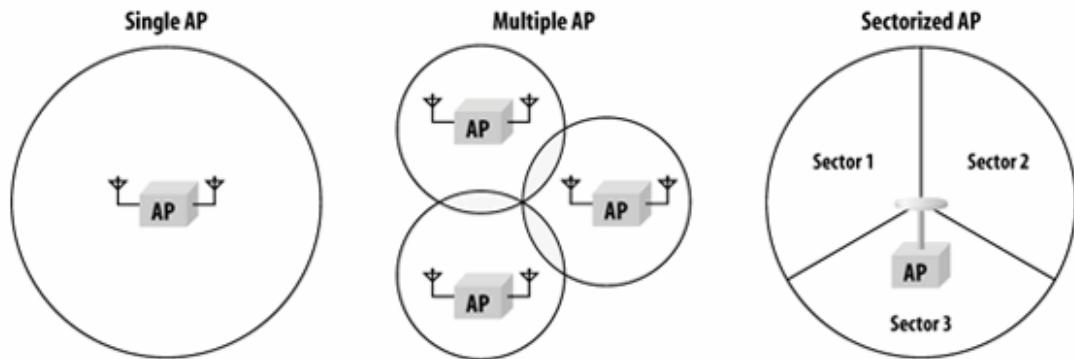
23.2.2.1 探讨覆盖范围/服务品质间的取舍，以及区域总和频宽

正常负载之下，基站相当于集线器，频宽是由覆盖范围内所有用户所共享。使用覆盖范围较广的基站来组建网络通常花费较少，因为所使用的基站数量较少，但服务品质可能较差，因为总和频宽较少。基站负责的覆盖区域愈大，距离较远的工作站也必须使用较低的速率连接。

一种衡量服务品质的方式为，计算服务区内的总和频宽，在某种程度上反映了基站的密度。其他条件不变的情况下，较多的基站意味着较多的无线频宽。图 23-3 显示了三个网络。图左的网络只有一部基站，最高可提供 30 Mbps 的用户数据给工作站使用。中间的网络包含三部基站，使用较低的功率运作。由于将覆盖区域切割为较小的独立电波区域，因此可以提供更多的传输量。粗略而言，将有 90 Mbps 可用来服务工作站。至于图右的网络，虽然只有一部基站，但却使用分区天线(sectorized antenna)，相当于三支指向型天线。在某些实现中，每个分区会被指定不同的频道，如此一来也可以减少工作站传输发生碰撞的机会。在最复杂的情况下，分区天线的每个频道可被当成独立的基站，工作站可用的总和传输量亦为 90Mbps。传输品质也可以用「服务区的每平方尺」(per square foot of service area) 可提供多少 megabits 来衡量，这和服务区的总和可用传输量并不冲突。

图 23-3：服务区总和传输量图示

Figure 23-3. Total aggregate service area throughput illustration



在 Ethernet 领域，交换器可以通过减少介质的竞争来提高网络的传输量。提升无线网络可用频宽的做法，也是采取同样的方式。缩小每部基站的覆盖范围，就可以在单一服务区域部署更多基站。虽然所谓的“Wi-Fi 交换器”宣传不断，但都是基于同样简单的设计原理。当网络中的元件变多，网络管理就变得比较困难，为了将复杂度集中于几个定点，最好不要到处使用合并设备（aggregation device）。

23.2.2 工作站的限制

业界所面临的一个主要挑战，乃是绝大部分的 802.11 操作均受控于工作站及其所使用的软件手中。几乎所有支持可移动性的“重要”协议操作都掌握在工作站手里。用户端软件决定何时漫游，如何扫描新的基站，以及何时连接至网络。网络中，不同机器会出现不同的行为，因为 802.11 并未规范何时漫游或如何挑选基站的算法。把这么多协议交给工作站实现，却又不受任何标准规范，导致工作站的行为通常变得十分神秘。举例而言，可以准备三部膝上型电脑，插上 802.11 接口卡后置于一台车上四处闲晃。这三部电脑将在不同时间漫游至不同的基站，而且通常会显示出不同的行为。未来的标准（特别是即将到来的 802.11k）应该有助于改善漫游决策的品质。

以“决定连接至网络的工作站”为例，大多数情况下，首度启动时，工作站会进行比较有智能的扫描，挑选信号最强的基站加入。对许多网卡而言，它们的智能就到此为止。它们将持续与第一部基站厮守终生，即使附近出现更合适的基站。除非完全丧失信号，否则没有什么可以强迫网卡进行漫游。这种行径通常被称为虫灯效应(bug light)，因为工作站就像是被灯火所吸引的飞蛾，无法抽身。具有虫灯效应的工作站其传输率特别差。就算已经远离原本连接的地点，还是会降低速度只求维持连接。

如此一来不仅拖累远距离工作站的连接速度，也大幅减少了其他工作站的可用频宽。低速传送时，以 OFDM PHY (802.11a 或 802.11g) 封装的最大封包 (1500 bytes) 需要更长的传输时间。在最极端的情况下，以 54 Mbps 传送最大帧需要用到 57 个数据符号，相当于 248 微秒。不过，以 6 Mbps 传送时，则需要用到 512 个数据符号，相当于 2,068 微秒，亦即八倍以上的时间。较慢的传输速率剥夺了其他工作站 1,800 微秒的传输时间。

将这么多攸关整体的协议工作交付工作站处理，限制了网络基础设施在必要时采取最佳手段的可能。举例而言，可移动电话网络能够将手机转交给具有较大频宽的基站处理。无线局域网

络协议尚无此种能力。有些无线局域网络系统厂商已经提供“基站负载平衡”(AP load balancing)功能，宣称可以让网管人员合并两部基站，为所在地区提升整体的网络容量。一种常见的做法是监视每部基站的连接数，或者各基站的流量，然后将工作站自负载较高的基站解除连接，鼓励它们转移至负载较轻的基站。如果得不到工作站的支持，很难达到负载均衡的情况，因为大多数工作站还是倾向连回原先的基站。

23.2.2.3 切合期待的传输量

当更多用户加入无线局域网络，网络频宽必须平均分配给更多用户，因此传输率就会下降。对采用 DCF(分散式协调功能)的网络而言，比较实际的经验法则是，大约可以达到 50% 至 60% 的额定位速率，因为必须将帧间隔，同步信号以及帧框标头等额外的负担纳入考虑。网络协议额外增加了网络层分封与重传的负担。大多数网络协议所面临的共同难题是，要提供稳定的传输就必须使用传输层回应机制。每个 TCP 区段均必须得到回应（虽然不见得是个别回应），而 TCP 回应信号又可能与其他正在传送的区段产生碰撞。[注] 表 23-1 依经验法则列出了每种基站的网络频宽。

表 23-1：根据经验法则的谁估各种 802.11 技术的网络频宽

Table 23-1. Rule of thumb capacity for different 802.11 technologies

Technology	Approximate capacity
802.11 direct sequence	1.3-1.5 Mbps
802.11b	6 Mbps
802.11g, with protection	15 Mbps
802.11g, no protection	30 Mbps, although this will be rare
802.11a	30 Mbps

设计上，跟“服务品质”(QoS)有关的技术通常是尽量榨出更多的网络频宽，但并未得到广泛部署。如果 QOS 的历史有任何值得借镜之处，那就是说之者众，用之者少。

802.11n 及后续标准

超越 54 Mbps 后，802.11 将何去何从？当 802.11a 与 802.11g 标准出炉，产品开始出现在市面上，“下一步往何处去”的问题就会开始浮现。2003 年，IEEE 802.11 工作小组成立了一个高速研究小组，开始探究如何进一步提升无线局域网络的速度 TGn (任务小组 N) 正致力提出一种标准，希望在和除其他协议所造成的负担后，能够达到 100 Mbps 以上的净传输量。任务小组的目标是超越 100 Mbps，看来似乎不难达成原先设置的目标。目前任务小组手中有两份彼此竞争的建议书，在第 15 章已经有所说明。两者约使用“多进 / 多出”(multiple-input/multiple-output，简称 MIMO) 技术来提升速率。粗略而言，其中一种建议书致力于提升最高传输率，另外一种则是维持较低的最高传输率，但侧重在提升无线链路的容量。

23.2.2.4 每部基站的用户数

规划网络时，必须知道每部基站的用户数多少。802.11 限制每部基站最多只能有 2,016 部工作站连接。实际上，每部基站的可连接用户数远低于此。对 802.11b 而言，6 Mbps 的实际频

宽算是合理的假设。要提供每个用户 **1 Mbps** 的连接速度，乍看之下，每部 802.11b 基站似乎只能服务六个用户。不过一网络流量原本就有高有低 (**bursty**)，从流量形式而言，自然可以假设能够服务更多的用户。为每个用户提供 **1 Mbps** 的连接速度是基于“用户有时会处于闲置状态”的前提。我发现 **3:1** 至 **5:1** 大概是较合理的比例。依此比例，一部 802.11b 基站最多大概能够服务 **20** 至 **30** 位用户。

然而，就算升级到 **802.11a** 或 **802.11g**，每部基站所能够服务的用户数也不会因此更多。**802.11** 中，速度取决于距离。工作站距离基站愈远，就会降而使用较稳定但速度较慢的编码方式进行传输。只有距离基站相当近的地方，才可能使用较高的速度，因此每部基站服务 **20** 至 **30** 位用户仍然算是合理。

如果你的应用对网络特性十分敏感（例如 **VoIP**），每部基站所能够服务的工作站数量就会更低。无线网络尚无法对复杂的服务品质进行优先排序，只能依赖介质本身对工作站的访问进行仲裁。语音与数据的特性有别。当介质达到饱和，且基站使出混身解数倾泄出对列中所有数据时，将可达到最高的数据传输率。语音帧必须及时传递，且对列必须尽量维持在低档，才有办法接收高优先的帧并立即传送。不论直接使用 **802.11** 链路或通过 **IP** 传送，语音流量对于迟延或剧烈的变动 (**jitter**) 均十分敏感。为了避免不必要的迟延，在更好的 **QoS** 技术来临之前，必须进一步限制每部基地只能服务 **8** 至 **10** 个电话听筒。

23.2.3 可移动性的需求

无线局域网络已经不再是玩家专属的新奇玩物。几年前，当使用者移动到不同位置，网络仅重新进行自动配置设置还可以接受。当无线局域网络日渐成熟，使用者开始期待不论身在何处，网络均能够提供无间断的连接。

连续的覆盖范围与无间隙的漫游。应该是园区环境的常态。使用者可能以无法预料的方式移动于园区之内，但仍然希望持续使用网络且连接不致中断。一般而言，只要未动用交通工具，使用者就会认为无线局域网络仍然可用。为整个园区设计覆盖范围时，必须考虑到用户可能跨越路由器的界限，因此设计时必须考虑如何维持他们所使用的地址，通常是通过某种型式的隧道协议。不同的无线局域网络架构有不同的隧道方式。详细的讨论，参见第 21 章。

23.2.4 网络整合的需求

网络规划有两个要素。首先，实体整合 (**physical integration**) 纯粹是一步一脚印的工作。除了建筑蓝图，如果可能，最好取得实际的网络架构图。省去了昂贵费时的布线消耗，安装无线局域网络硬件变得简单不少。知道现有集线槽的位置与所有线路的内容是重要的第一步。逻辑整合 (**logical integration**) 是第二个步骤，包含如何将无线局域网络整合至现有的网络。

23.2.4.1 实体整合

实体整合包括如何将各个元素摆到正确的位置。基站必须根据事先的规划摆设，并正确地布线。如果考虑到美观因素，新增设备时或许需要重新布线。否则，从现有的插槽接线到基站所在位置即可。取决于所选择的产品与架构，网线可能是接到基站控制器、特殊的 **wireless VLAN** 或是集线槽当中的网络。

除了配线，还得供电给基站。在基站所在位置直接供电并无不可，但不建议这么做。许多企业级基站的设计，主要是通过 **Ethernet** 网线供电，甚至连电源供应器都没有提供。（有些基站则是另外提供 **48** 伏特的电源供应器，亦即其电源电路被设计成运作在 **PoE** 的电压。）有些交

换器可能具备 Ethernet 供电 (PoE) 的能力，但使用前必须检查与确定是否相容。符合 802.3af 标准是电源相容的最佳保证，不过各位手上或许有些设备属于厂商的专属规格。如果必须在集线槽提供电源，可以购买其他厂商所生产的灌电器 (power injector)

23.2.4.2 逻辑整合

进行无线局域网络的逻辑整合之前，必须先挑选一种架构（参见第 21 章）。不同架构有不同的整合需求。不过，一般而言，无线局域网络至少必须连接到某个网络。若要连接一个以上的网络，或许必须使用以 AAA 为基础的动态网络指定 (dynamic network assignment)。这些网络绝大部分属于 IP 网络。不过有时候，无线局域网络也需要支持旧式的网络协议。

网络规划的第二个要件是思考逻辑网络的变动。可移动式工作站该如何定位？如果所有无线工作站将使用单一 IP 子网络，则必须为之配置 IP 地址空间，并确定它能够被正确传送至无线子网络。配置新的地址空间时，切记给所有基站与其他辅助设备留点额外空间。切勿禁不起诱惑地采用地址转换 (address translation)。虽然有些应用程序可以搭配 NAT 一起使用，但未来的应用程序如果不认得 NAT，就会造成潜在的问题。在 NAT 普及之前已经写就的应用程序也可能无法使用。

扩充网络时，必须新增基站设备。基站或许需要 IP 地址。如果基站的地址是通过 DHCP 取得，最好在 DHCP 服务器中为每部基站指定固定的地址，不要让 DHCP 服务器随机指派。如果基站通过 IP 隧道 (tunnel) 连回中央控制器，各位或许必须设置一些过滤规则让双方得以进行传输，并且分别在基站与中央控管设备上设置必要的传输管道。

23.3 物理层的选择与设计

802.11 物理层的选择通常由用户需求而非实体设计所驱动。大多数情况下，它也会受到打造最快网络的需求所驱动。物理层的选择关系到工程层面。物理层本身并无优劣之分。选择物理层时，其实是在一些不同的因素间做取舍。总而言之，2.4GHz ISM 频段比较不受障碍物的影响，因此 802.11 b/g 信号的传输距离较远。不过，传输率会受到回溯相容性的限制。而且很难只用三个频道来规划网络。此外，使用 2.4GHz ISM 频段的设备并不少，很可能受到某些设备，例如 Bluetooth、2.4 GHz 无线电话、X10 影像照相机，或其他类似设备的干扰。即使干扰不存在，只能使用三个频道也会限制传输率，如果频道与其他网络重叠的话。802.11a 比较适合高密度、高传输率的网络，除了不受回溯相容性的限制，能够使用的电波频谱也比较宽。

表 23-2 所示为 2.4 GHz 与 5 GHz 802.11 网络的比较表

Table 23-2. Quick reference comparison between 2.4 GHz and 5 GHz 802.11 networks

	802.11b/g (2.4 GHz)	802.11a (5 GHz)
Performance (throughput) per AP	Low for 802.11b; 802.11g may vary from medium to high	Highest throughput per channel
Potential performance per unit area	Low with only 3 or 4 channels, channel overlap and interference is practically guaranteed	High greater number of channels means less self-interference between network elements
Range	Lower frequency has longer range	Worse free-space loss of higher frequencies is higher
Interference	Many other uses of frequency band Very limited channel selection leads to lots of co-channel interference	Frequency used by many fewer devices More channels make layout easier, especially in three dimensions
Backwards compatibility with older hardware	Compatible with 802.11 direct sequence and 802.11b hardware	None

要减轻大规模无线局域网络部署的负担，方式之一是尽量自动化。有些产品可以自动规划频道。其中一种做法是根据实际的测量结果来进行频道规划。网管人员可根据使用者密度、安装的容易度以及环境的限制来摆设基站。网络启用后，基站就会通过有线网络彼此沟通，以便选择最佳的频道配置。有些产品会持续监控无线电波，依环境的变化来动态调整频道的设置。除了实际的测量，另外一种替代方案是为建筑物建立虚拟模型。为建筑物建立虚拟模型时，可以利用数理模型将干扰降至最低，并根据计算结果来配置频道。和无线局域网络其他设计层面一样，有些产品会同时采用这两种技术。

23.3.1 2.4 G H z (3. 2.11 b/g) 频道规划

802.11u 与 802.11g 共用相同的频段。两者适用相同的管制要求，也使用相同的频道表（表 23-3）。虽然最多可以有 14 个频道，但每个频道只有 5 MHz 宽。直接序列传输展开时，所跨越的频段会宽于所指定的频道（参见图 12-5）。要得到最佳的效果，第一与第二个旁瓣最好不要受到干扰。理想情况下，频道之间最好相隔 33MHz。大多数管制区的无线频谱并不足以配置三个完全不相重叠的频道。大多数用户宁愿容许第二个旁瓣稍微重叠，这样起码有相距至少 25 MHz 的三个频道可用，不致于只能使用两个完全不相干扰的频道。如此一来，就可以得到 1、6、11 的频道组合。虽然每个频道会稍微受到干扰，不过牺牲一点传输率换得第三个频道还是十分值得。

有时候，四频道的配置（1、4、8 与 11）也有其用途。【注】不过代价是信号重叠的部分更多，最高传输率也会因此降低。虽然牺牲最高传输速度（peak speed）以换取较高的整体速度（total area speed）在某些情况下是值得的，不过我个人认为并不划算。

表 23-3 不同管制区域所使用的无线频道

Table 23-3. Radio channel usage in different regulatory domains

Channel number	Channel frequency (GHz)	US/Canada^a	ETSI^b
1	2.412	✓	✓
2	2.417	✓	✓
3	2.422	✓	✓
4	2.427	✓	✓
5	2.432	✓	✓
6	2.437	✓	✓
7	2.442	✓	✓
8	2.447	✓	✓
9	2.452	✓	✓
10 ^c	2.457	✓	✓
11	2.462	✓	✓
12	2.467		✓
13	2.472		✓

注 a 802.11 标准允许美国与加拿大使用不同的无线频谱，不过美国 FCC 与加拿大产业部采用相同的规范。

注 b 并非全欧均采用 ETSI (European Telecommunications Standards Institute) 所建议的规范。例如西班牙（本表并没列出）就只能使用频道 10 与 11。

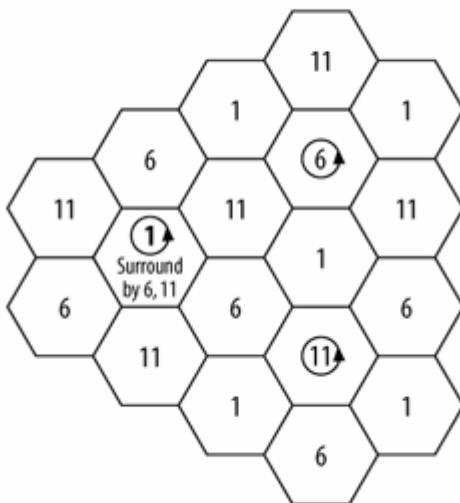
注 c 所有管制当局均允许使用频道 10，因此大多数基站会以之做为预设频道。

实地勘探的部分目的，是为了在规划覆盖范围时，能够尽量避免频道重叠。天线的价值在此浮现，因为它们可以调整覆盖范围，使之符合建筑物或房间的形状。不论选用何种天线，均可采用一种通用的样式。可移动电话产业使用六角样式（hex pattern）做为频道规划的基础。图 23-显示了规划大型覆盖区域时不可避免的问题。从不相重叠的三个频道挑选其一做为中心频道，以粗体字表示。本例中，我随意挑选 1 做为中心频道。为避免重叠，中心频道四周必须使用其余两种不相重叠的频道。为四周选定频道后，就可以接着规划其他中心频道。图 23-4 中，可以看到另外两个以圆圈标示的中心焦点。

当然，图 23-4 所呈现的是理想环境中的频道配置。在建筑物中，电波的传播不仅受到障碍物的影响，频道重叠的情况也通常无可避免。举例而言，中心频道 1 外环的频道 6 与频道 11 就可能互相干扰。

图 23-4：频率规划

Figure 23-4. Frequency planning



23.3.1.1 2.4 GHz 频道规划的限制

只有三个频道无法进行频道规划并不令人惊讶。数学上有所谓的四色地图定理(Four-Color Map Theorem)。早在 19 世纪中就已经发现，绘制任何二维地图至少需要四种颜色。【注】遗憾的是，802.11 b/g 网络只有三个不相重叠的频道。地图的相邻区域若使用同样的颜色便难以分辨。相邻基站的覆盖区域若使用同样的频道亦然，且因为共用频道的干扰，必然会影响双方的传输率。

要将频道的重叠的程度降至最低，通常必须仔细调整基站的摆设位置或借助外接天线，不过得付出不少时间与精力。在三维空间里，那就更不容易了。电波信号可能穿透地板或天花板，因此规划频道时必须考虑到三维空间。

在 Cray 超级电脑的协助下。经过 1,200 小时运算，终于在 1976 年证明了四色定理 (Four-Color Theorem)。它是最早通过电脑辅助得到证明的定理。

即使在宽广、开放的平面空间，各位认为绝无可能的地方，还是会出现意外的干扰。2002 年，Associated Press 在一篇干扰问题的报导中提到，Florida 附近居然成立自己的 ad-hoc 频率配置委员会，以确保左邻右舍不致使用相邻频道！

23.3.2 5 GHZ (802、11a) 频道规划

以 802.11a 规划网络有两项主要优点。首先，802.11a 起码有 12 个频道，因此频道规划不成问题。表 23-4 显示了各频道的频率。必须注意的是，有些早期的 802.11a 网卡并不支持最高频段，因此 149 以上的频道并不适用于所有网卡。如果遇上这种情况，要不就是换掉旧网卡，否则就只能使用其他八个频道。不论是 8 或 12 个频道，对二维空间的规划而言均绰绰有余，至于三维空间，只要小心规划，大多数情况都不成问题。

表 23-4.a 802.11a 频道（附注美国管制规定）

Table 23-4. a channels (with United States regulatory notes)

Channel number	Frequency (GHz)	Notes
36	5.180	Lowest maximum power
40	5.200	Lowest maximum power
44	5.220	Lowest maximum power
48	5.240	Lowest maximum power
52	5.260	Slightly higher maximum power
56	5.280	Slightly higher maximum power
60	5.300	Slightly higher maximum power
64	5.320	Slightly higher maximum power
149	5.745	Not supported by all cards
153	5.765	Not supported by all cards
157	5.785	Not supported by all cards
161	5.805	Not supported by all cards

23.3.3 混合式频道规划 (802.11 a+b/g 网络)

大多数网络通常一并使用 802.11 b/g 以便相容于旧硬件，而以 802.11a 做为未来扩充之用。有些厂商所推出的双频基站只比单频机种贵上一些。有时候，三模/双频网络的组建成本，只比单纯的 802.11g 网络多出几百或几千美元。除非预算很紧，否则多付一点成本就可以让频宽加倍，其实是十分划算的。

在可预见的未来，大多数 802.11 设备还是会使用 2.4 GHz 频段。大多数芯片组厂商还是专注在生产 802.11g 设备。市面上一些三模芯片组同时支持 802.11a 与 802.11b/g，不过尚未广泛内建于膝上型电脑。当初我所组建的 Supercomputing 无线网络，同时间最多会涌进 1300 位使用者，其中只有 100 位使用 802.11a。当芯片组与无线网卡的价格持续滑落，且 802.11a 逐渐为大众所接受，预料室内将大幅改用 802.11a。至于户外环境，传输距离还是主要的考虑因素。频率愈低，传输距离愈远。因此在户外仍然将由 802.11b/g 维持目前的领导地位。

23.4 基站摆设位置规划

目前，大多数用户认为有线网络就是可行 (just work)。以产品的成熟度与可预测性而言，无线网络还是有所不及。无线网络所使用的协议还是有点难以预测，有些较新的协议甚至得卷起袖子亲自动手。规划网络时，有一堆工作必须优先进行。由于无线网络让使用者得以不受空间限制访问资源，因此网络本身必须清楚掌握用户所在位置。

一旦了解用户需求与决定采用何种 802.11 物理层，接下来的问题就是应该将基站置于何处。取决于需求与预算，决定基站的摆设位置可能只需要几个小时，也可能需要来回进行好几次，花费大量的时间与金钱。此一程序之所以称为实地勘探，是因为有一些工作必须在网络的装设地点进行，不过新一代的工具已经可以通过电脑模拟，取代不少基站摆设工作。

有几个选项可用来判断，应该将基站置于何处。对同意列名于使用客户名单的早期采用者，厂商可能愿意提供实地勘探服务，虽然在本书付印之前，成为早期使用者的时机早已消逝。加值经销商或许也有能力进行详细的实地勘探。经销商可将实地勘探当做顾问服务来销售，或以之做为成交的筹码。有些专门从事技术教育训练的公司，也会提供类似的课程。

23.4.1 建筑物

建筑物的构造乃是限制基站摆设位置的主要因素之一墙壁、门窗都会影响电波信号。取得楼面设计蓝图并及早实地勘探，对网络规划有极大的帮助。有时候，各位也许有机会针对施 Z 中的建筑进行规划。这时候必须把握每一次实地勘察的机会，因为在墙壁砌起之前，可以更清楚掌握建筑物的内部结构。为施工中的建筑物进行规划的主要缺点是，除非等到建筑物完工，否则无法进行各项实验。

一旦取得楼面设计，就可以评估收讯范围必须涵盖哪些地方。如果建筑蓝图十分完整并且包含布线信息，应该会同时记录就近的电源插座。各位也可以初步观察有哪些结构可能造成问题，例如空调风管 (Ventilation duct) 或者以钢筋混凝土砌成的墙面，不论是否使用电子仪器让规划程序自动化，都应在现场再次确认。看看是否有蓝图未曾记载的变更之处。确认现场所使用的建材。除非是老旧建筑或古迹，否则墙壁应常采用轻隔间材质 (sheetrock hung from studs)，只要敲敲墙面就可以得到验证。看是否有防火墙（实际的防火墙，不是网络防火墙），因为防火墙对 RF 信号会造成相当大的影响。结构或承重墙可能是钢筋混凝土材质，这将对电波形成极大的障碍。如果必须将基站隐藏在特定地区，就该彻底研究如何隐藏，以及对网络工作有哪些潜在的影响。此外，挑高的天花板或者其他难以安置的地点也必须加以检视。在巡视过程中，可能会有来自四面八方的异样眼光；不要在意，继续前进。完整巡视一遍，可能会得到不少异样的眼光。就将它视为此行的绩效指标吧。

根据第一次实地勘探，记录下所有相关的环境因素。最重要的是，各位可以根据结构的变更修正蓝图。毕竟绘制之后的变动通常不会记录于蓝图，尤其是老旧建筑。同时，最好记录下潜在的干扰源。**2.4 GHz ISM** 频段无须使用执照，因此使用该频段的各种设备，可能并未统一管制。新型的无线电话 (cordless phone) 同样使用 2.4GHz 频段，Bluetooth 与一些其他无线设备亦然。如果预料干扰源不少，可以使用频谱分析仪在无线局域网络频段测量辐射量。事实上，除非是特别顽强的干扰源，否则不必每次都祭出频谱分析仪。一种名为 **Berkeley Varitronics Yellowjacket** 的手持设备，内建了 2.4 GHz ISM 频段的频谱分析仪，可用来追踪非 802.11 信号的干扰。如果贵单位有在进行 RF 测试，必须为实验室加上屏蔽，以免干扰无线局域网络。依经验法则，基站的摆设至少要远离较强的干扰源 25 英尺。

23.4.1.1 基站摆设位置的限制

实际上，尽可能将基站置于高处意味着最好将它们摆在天花板的高度。许多办公建筑使用倒吊式(dropped) 或悬吊式(suspended)天花板。基站可以安装在天花板吊筋(ceiling mounting bars)，或者置于天花板之上。必要时，可将基站置于所有办公室隔屏 (cubicle) 之上。不妨跟厂商确认基站的辐射样式(radiation pattern)。如果基站原本的设计是从天花板向下传送电波，将它们置于办公室隔屏之上就无法达到预期的效果。

比较常见的做法，是根据实际限制来调整基站位置。主要的限制因素之一，在于基站通常通过 Ethernet 缆线连接至网络。【注】离基站最近的集线槽不能超过 100 公尺。由于规格较具

弹性，有时候网线可以比规格稍长，但总不能永远心存侥幸。取决于跳线面板（patch panel）、支架(riser)与天花板的布线，实际上需要使用较长的网线来连接基站。

多数产品可以使用第二种电波构成网状后端骨干（"mesh" backhaul）。预料这项功能会随着时间的推移变得普及。

电源通常是基站摆设的另外一项限制因素。早期的基站需要用到电源插座，不过机关行号很少会在天花板上安装电源插座。安装电源插座通常所费不低。随着 802.3af 的发展，有些组织开始通过网线为基站供电。Ethernet 供电（Powerover Ethernet，简称 POE）优点不少；不过，要让 100 公尺的网线维持 48 伏特的电压，本身就有工程上的难度，也无法在缆线长度方面投机取巧。

为无线网络布设新的网线是值得考虑的，特别是如果现有的网络插座无法轻易支持新的基站时。现有的网线通常在踢脚板（baseboard）附近，不适合用来连接高挂式网络设备。架设新的网线有许多优点。它可以直接拉至基站所在的天花板，如此就不会露出丑丑的网线。旧式的布线或许在 Category S 线材成为标准前就已经存在。布建新的网线也可以增加某种程度的弹性。考虑到有时需要移动基站，有些新式的布线会在天花板的网线终端加装网络插座，允许使用跳线（patch cable）让基站移动至附近。

取决于天花板上的元件配置，有时很难沿着空调风管布线，或将基站置于风管附近。通常，只要将基站稍微挪至下一块天花板的位置即可，并不会严重影响基站的覆盖范围。此外，让基站远离灯座及其电源线也很重要。

最后的考虑因素与实体的安全性有关。有些机构认为必须为基站加上防盗措施。有时候，将基站安装于天花板就算防盗措施，毕竟已经将基站隐藏起来。有些基站附有防盗锁孔，可将之固定在无法轻易移动的物体上面。

23.4.1.2 施工中的建筑物

随着无线局域网络的普及，有许多无线网络在建筑物施工期间就已经开始着手设计。为施工中的建筑物设计无线局域网络不仅有许多乐趣，也是不小的挑战。

首先碰到的问题是，会受到其他工程进度的影响。幸运的是，可以借助模拟工具来估计所需要的基站数目。施工图通常十分完整，而且通常在实际动工前，网络小组就可以取得相关图面。一开始，可以先评估不同材质可能造成哪些影响，并且建立初步的模型。

当建筑物逐渐成型，就可以到各个区域巡视一遍。取决于施工时间，实地勘探可以分几个阶段进行或者一次解决。在施工期间进行勘查，通常需要得到承包商的首肯。安全帽外加放弃申诉抗辩权利（liability waiver）。在建筑物各个区域确认一下模拟阶段所做的假设是否正确。例如，赋予各个墙面的电波损耗系数是否正确，当初所建构的模型是否需要修正？完工后，就可以将基站置于定位实际进行测试，进一步检验当初所做的预测是否正确。

为施工中的建筑物设计无线局域网络，最大的挑战之一就是环境处于持续变动的状况。比较少见的情况下，可能会因为缺料甚至是美观上的考虑，于最后关头更换建材。记得尽量让设计保持弹性，并且预留一些安全空间以防错误发生。

23.4.2 初步规划

决定基站的数目与初步摆设位置是规划的第一个里程碑。几年前基站还十分昂贵，当时决定初步摆设位置的最佳方式是估计需要几部基站，然后将它们集中置于开放空间。如今基站已经相当便宜，尽量减少基站数目已经不再是主要的考虑因素。

根据两项经验法则，可以粗略估计出所需要的基站数量。第一项经验法则是根据区域来计算。在典型的开放办公室环境，以最大功率传输的基站可以覆盖 3,000 至 5,000 平方尺（275 至 400 平方公尺）的区域。只要知道打算涵盖多大范围，将之除以每部基站的覆盖范围(footprint)即可。少有障碍物的开放空间可以取较大的数目；封闭隔间的办公室，或者内部结构复杂的建筑物，就要取较小的数目。除了根据区域大小，也可以根据用户密度来估算所需要的基站数量。依经验法则，可以将组织中的用户数除以 20 至 50。如果无线网络十分受到欢迎且广为使用，就可以除以较小的数目。如果无线网络对用户而言仍属新鲜且属于实验性质，就可以除以较大的数目。这两个数目取其大者，就可以粗略估计出应该安装多少部基站。

只是粗略知道需要多少基站，不见得知道应该将它们摆至何处。要将这些粗略的估计转换为初步计划还需要不少工作。如果经验足够，就不难判断应该将基站置于何处。结构墙或防火墙通常会完全阻隔信号。多层建筑的主要承重结构通常位于中央核心，而且通常使用钢筋混凝土材质。以每尺 10 dB 至 20 dB 的衰减计算，通常可以将之视为一种 RF 屏蔽。当信号穿越两三间一般大小的办公室，大多数基站仍然能够维持在最小速度之上，这取决于中间障碍物的多少。一般而言，尽可能将基站摆在障碍物较少的开放空间。要让基站能够随时提供必要的服务，最好将基站置于办公室隔间与走廊之上。

到目前为止，制定初步计划通常是依赖人工方式，需要高度的技巧与广泛的经验。过去几年开始出现了一些模拟工具，可将初步规划程序加以自动化。这些工具将依照建筑物的工程图建立电波传波的数理模型。当网络设计师变更模型中的基站摆设位置，此工具就会立刻重新计算出基站的覆盖范围。这类电子工具很有价值，可以合理推估基站的摆设位置，减少实际验证的次数。对于尚在施工的建筑，这些工具更是特别有价值。有些工具能够直接读取建筑设计图，亦即电脑辅助设计（Computer-Aided Design，简称 CAD）文档。有些工具只接受简单的图形档，例如 GIP 或 JPEG。记得要取得建筑平面图。建筑平面图通常是由设备部门负责保管，也可以通过房东或业主取得。如果是新的建案，不妨直接向建筑师索取。

虽然模拟工具十分有用，切记不要只是纸上谈兵。电波传波十分复杂，特别是在室内的微波频段。电波对不同材质有不同的反应，只要隔个几寸，覆盖范围就可能截然不同。要使用这些模拟工具，必须具备正确的建筑营造知识，但是网管人员不见得专精于此。模拟工具并无法完全取代实际的试验。

不论使用何种技术，还是得从实体规划推衍出初步计划。此时尚不需要电波频道的细部规划。如果使用模拟工具，不妨让它提供一份建议案，等到实际安装后再做修正。不过，初步规划就是初步规划。不要期待可以就此定案。这个阶段的目的，并不是搞定所有任务，只是取得一个切入点。表 23-5 依经验法则推估了典型的全向型天线在不同空间的最佳覆盖半径。如果打算提供较高的传输率，覆盖半径就不能太长。最好的做法是借助本节所讨论的模拟工具。

表 23-5：依经验法则推估不同类型空闲可能的覆盖半径

Type of space	Maximum coverage radius (2.4 GHz)	Maximum coverage radius (5 GHz)
Closed office	Up to 50-60 feet	35-40 feet
Open office (cubicles)	Up to 90 feet	60 feet
Hallways and other large rooms	Up to 150 feet	75 feet
Outdoors (without antenna engineering)	Up to 300 feet	Don't even bother!
Outdoors (with custom antennas)	Many miles	Don't even bother!

23.4.2.1.1 报告

初步计划可以做为进一步可移动的基础。它可以用来自评估特定区域部署无线局域网络的成本。此外，也可以聘请布线承包商根据初步计划实际布线。计划本身可能包含：

1. 初期工作所搜集到的需求汇报。
2. 根据实地勘探测量所评估的覆盖范围。覆盖范围可以细分为收讯良好、收讯普通与收讯不良三种。根据数理模型所提出的报告，可以勾勒出不同传输率的大致轮廓。
3. 描述各个基站的摆设位置以及相关配置。有些自动规划软件工具能够根据平面图提供细部的位置与设置信息，例如：
 - a. 基站的工作频道。
 - b. 最大覆盖范围，或许是以不同速度的覆盖轮廓来表示。
 - c. IP 配置，如有必要的话轻量级基站可能没有 IP 地址。
 - d. 天线类型与摆设，包括指向型天线所指的方向。
 - e. 产品特有的信息。有些机构会根据 MAC 地址来追踪设备，因此在报告中包含相关信息就十分有用。

23.4.3 电波资源管理与频道规划

图 23-4 容易造成一种错觉，让人误以为频道规划十分简单。打造室内网络时，信号的传播其实复杂得多。频道重叠的情况通常发生于室内，因为必须使用较高的功率方能穿透障碍物，因此到处充斥的信号功率均高于必要。初步计划应该包含基本的频道表（channel map）。可以确定的是，频道规划必然需要进一步调整。进行调校时，可以使用手持式工具，以人工方式找出重叠的频道，或者让基站自动搜寻最空闲的频道。既然 2.4GHz 频段只有三个频道可用，任何变动都可能在网络中造成骨牌效应（ripple），需要花费一些时间以得出最终的解决方案。

23.4.4 规划的修正与测试

取决于所要求的精确程度以及预算的限制，计划的修正程序可大可小。在小型或预算很紧的工程中，只要有初步规划，使用网络后视后续发展如何即可。比较慎重的部署可能会依初步计划安装部分或全部的基站，然后进行一连串的测试，验证是否符合需求。如果初步计划十分精确，

或许不需要任何修改。测试的主要目的。在于找出之前未曾发现的干扰或死角，据以重新设计。大多数情况下，干扰问题可以通过基站重新摆设来解决。基站摆设位置通常不需要太大的调整。如果还是无法解决，可能就要更换不同的天线或基站了。有时候，可能需要经过好几回合的设计与测试阶段，虽然这种做法比较少见。

检视计划时，尽可能复制使用者经验。无线局域网络与基站间的障碍物会使电波强度减弱，因此在实地勘探时，尽量复制原本的使用情境。测试时与完工后，应该使用一样的天线。如果办公人员也会用到无线网络，记得确认一下，关起门后是否能够合乎收讯上的要求。更重要的是，记得关上金属百叶窗，因为金属物质最容易影响无线电波。

信号测量应该符合网络用户的期待，除了一项例外。大部分实地勘探工具是以某个定点，根据几个特定时点的数据来评判信号品质。因此在实际进行测量时，记得将膝上型电脑置于定点。务必多测量一些数据，因为使用者会带着膝上型电脑四处移动，而且多重路径衰落效应可能会导致信号品质有相当的落差，即使只是相隔几步之遥。

比较严谨的机构可能会测试不同的用户端设备。无线局域网络会因实际上的差异而有截然不同的表现，就算使用完全相同的软件，工作站也会显现出截然不同的行为。如果需要知道系统的实际表现，就值得对软件使用相同的配置设置，在同一时间进行相同的测试，以便多搜集几个系统的信息。

最后的测试报告应该包含基站的最后摆设位置，以及确实的涵盖范围。覆盖范围可以用地区来表示，虽然附上各区域能够稳定提供的传输率可能更为有用。有时候，效能特性报告也十分有用，特别是应用程序的组合具备某种特性时。

如果建筑物尚在施工，验证程序就必须等到完工后进行。如果整栋建筑同时施工，最好及早进行基本的测量工作，以便判断是否需要大幅修改电波模型，将费时与正确性的验证测试留到最后。

23.4.4.1 验证与测试工具

过去，要得知基站的覆盖范围与完成基站的规划相当费时，因为需要将基站摆至不同的位置，反覆测量基站的信号品质。随着自动规划工具的发展，不论是根据模拟或自动调整机制，在验证阶段通常已经不必用到这些工具了。通常只有在岭现测试系统遭遇问题时，才需要深入分析电波链路的容量。

最常见的信号品质测量项目就是封包（比较正确的说法是帧）错误率(**packeterror rate**，简称 PER) 与接收信号强度指标（**received signal strength**，简称 RSSI）。帧错误率愈低愈好。过去，8 % 以下的 PER 就有办法提供可接受的容量。基站较为密集的网络，应该能够轻易达到 5% 或更低的帧错误率。比较复杂的基础型设备，通常可以直接测量个别工作站的帧错误率，以及 RSSI 与信噪比。能否达到较高的传输率，RSSI 与讯噪比是关键因素。必须通过特定讯噪比门槛，才有办法以特定的传输率传送可辨识的帧。

少数工具可以测量「多重路径时间迟延」（**multipath time dispersion**），亦即测量信号经由不同路径的时间因素。迟延范围（**delay spread**）愈大，信号的相关（**correlation**）还原工作就愈困难。如果迟延范围较大，设备就必须接受较高的错误率，或者降速使用较保守的编码方式。不论如何，传输率都会因此下降。迟延范围愈大，传输率就愈低。测量多重路径传播比较没那么重要，不过这种用来搜集多重路径问题相关数据的工具还是颇有价值。

当 802.11b 还是无线网络的主流，市面上有许多针对携带式运算平台（如 Compaq 的 IPAQ）开发的手持式工具。不过随着 802.11a 与 802.11g 的普及，手持式设备就逐渐失宠而为 Tablet PC 所取代。大多数手持式设备使用较慢的外接介质，无法跟上新式标准的传输率。举例而言，IPAQ 使用 16 位元的 PC Card 介质，时钟只有 8MHz。虽然这种速度对 11 Mbps 的 802.11b 介质而言已经足够，不过较高速的 802.11a 与 802.11g 就得使用 CardBus 介质。Tablet PC 在验证阶段还具有另外一种优点。它可以执行许多初步规划可能会用到的工具，包括可以执行验证软件来搜集当地的测量信息，以及将这些验证测量数据和之前所计算出来的预测值进行比对。

特别难缠的干扰，有时候必须动用频谱分析仪，方能找出非 802.11 网络的干扰源。能够扫描大范围的频段以找出信号传输来源的设备，并不便宜。如果不花个几千美元，可以请个咨询顾问。或者使用限定于 ISM 频段的频谱分析仪来追踪干扰源。不论如何，频谱分析仪都是最后的手段，只有最难缠的问题才需要用到。

23.4.4.2 RF 指纹的搜集

有些无线局域网络系统需要搜集上一章所提到的 RF 指纹（fingerprint）。惟有在基站已经置于最后定位，方能进行指纹的搜集。之后，就可以将测试设备摆在特定位置上，让系统搜集指纹。

23.4.5 准备最后的报告

在规划与测试过程中，应该准备初步文件，记录基站的摆设位置。测试完成之后，必须以文件加以记录。如果初步计划是以电子档存放，除了根据测试结果加以修正，也必须将变动纳入最后报告。

除了基站的摆设，有些客户还希望知道，将驱动程序安装至所有受影响的膝上型电脑，需要花费多少时间。影响多大，必须视客户所使用之管理工具的复杂程度。有时候，只要在报告的附录中附上一份驱动程序安装说明的副本即可。有些客户则会要求驱动程序的安装细节，以确定驱动程序的安装会自动对 Windows Registry 进行任何必要的变更。

23.5 使用天线调整覆盖范围

有时候，基站的覆盖范围必须涵盖某些不按常理的特定区域。大多数基站均会使用全向型天线，此种天线在各个方向的辐射范围均等。不过，有时候需要将基本的电波覆盖样式，从圆形调整为其他形状。通常，这牵涉到调整基站的覆盖范围以符合特定区域，或者提升信号以填满某个区域。随着基站价格大幅滑落，已经没有必要以天线调整覆盖范围，虽然这种做法仍有其重要性。

过去，无线电波设备厂商需要提供天线，并确保系统符合免照频频的管制规定。2004 年 7 月，FCC 放宽了管制规定，允许无线电波设备厂商指定最大增益，让使用者自行选购具有相同增益特性的天线【注】。在此之前，无线电与天线必须一并送测，私自更换天线基本上是违法的。新的管制规定出炉后，制造商可以单独验证符合管制规定的系统。而一般用户可以选用任何符管制规定的天线。举例而言，如果无线电系统制造商送测时使用 10 dBi 的天线，使用者就可以自行选购增益较低的同类型天线（例如 8 dBi），并且合法使用。

23.5.1 天线类型

无线网卡均内建天线，不过这些天线只能算是差强人意。如果打算在整个办公室、甚至更广的范围内（如公司园区）收信，必然得为基站加装外接天线。考虑特殊的天线时，只须注意若干必要的规范：

天线类型

天线类型决定了本身的辐射形式，天线可以是全向型（omnidirectional）。双向型（bidirectional）或是指向型（unidirectional）。全向型天线适合覆盖较大范围时使用，双向型天线特别适用于走廊，指向型天线则是最适合在建筑物或不同网络之间架设点对点链路。

增益

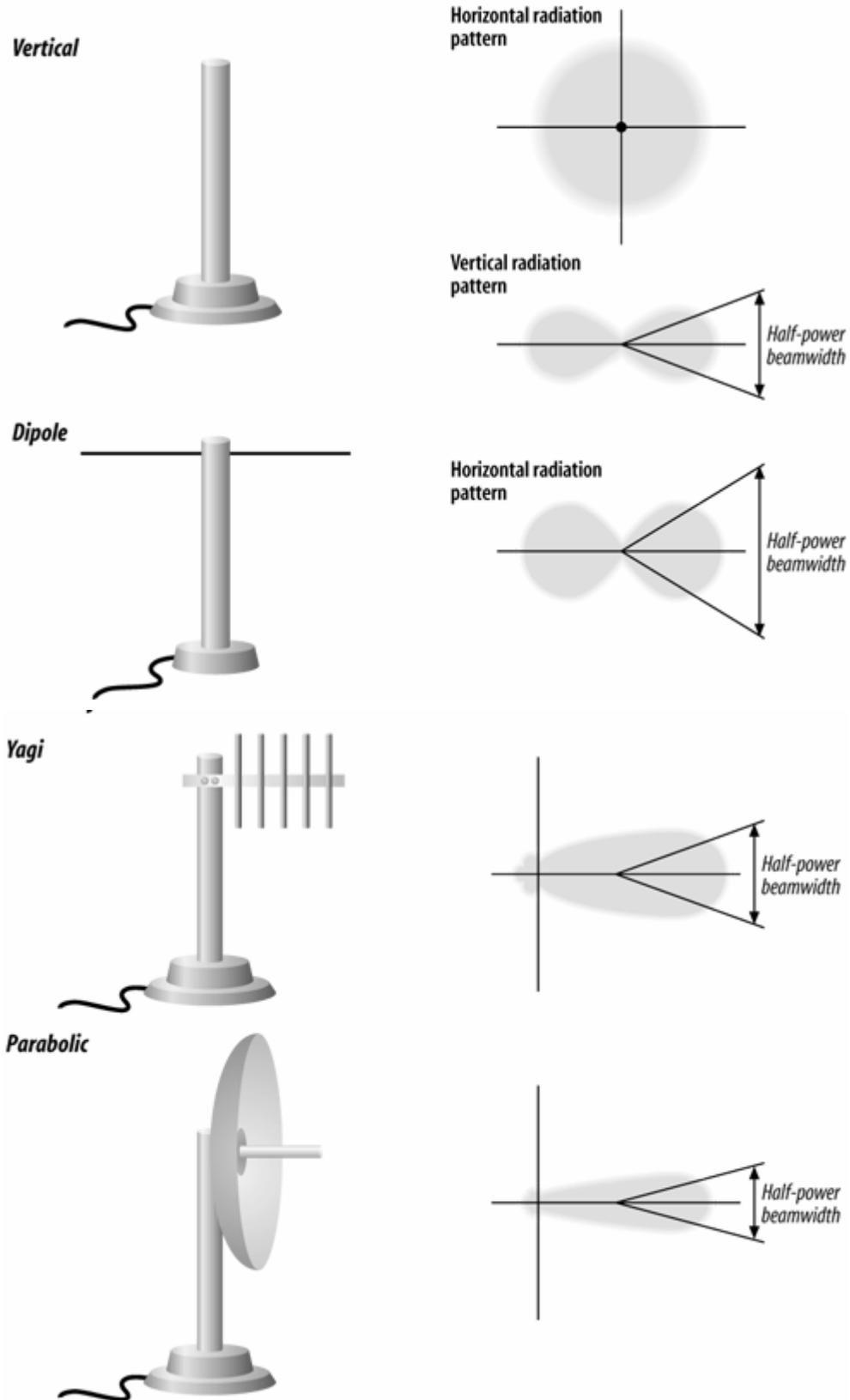
所谓天线增益，是指天线沿所指定的方向提升信号的程度。天线增益的测量单位为 dBi，代表相对于等向性辐射体（isotropic radiator）的分贝数。等向性辐射体纯粹是理论上的假设，代表任何方向的辐射均相等的物体。不妨打个赌：我从未见过无线网卡内建天线的增益规格，不过我猜可能为负数（亦即比等向性辐射体差）。简易型外接天线的增益大约为 5 至 7 dBi。指向型天线增益有可能高达 24 dBi。【注】如果你想要更多的树桩，在 Arecibo 的射电望远镜可以有超过 80dBi 的增益。

半功率波束宽

半功率波束宽（half-power beam width）意指天线辐射形式的宽度，以天线辐射衰减至峰值的一半加以测量。半功率波束宽是了解天线有效覆盖范围的关键。以高增益天线而言，半功率波束宽可能只有几度一旦离开半功率波束宽的范围，信号通常会迅速衰减，这完全取决于天线的设计。不要以为半功率波束宽与全向型天线无关。典型的全向型（垂直）天线只有在水平面具有全向性。只要位于天线上方或下方，信号就会减弱。

就天线而言，我们探讨的重点几乎完全放在传送特性，主要是因为一般人比较容易理解。值得庆幸的是，天线的接收特性与传送特性相同。不论接收或传送信号，天线愿加诸的作用是一致的。这个结果或许在各位意料之中，不过如何证明其为如此，已经超出本书的范围。现在，让我们看看现有的天线类型（图 23-5 显示了各种类型的天线）：

Figure 23-5. Antenna types



垂直天线

这是相当普通的全向型天线。大多数厂商均会销售各种类型的垂直天线，主要差别在于增益不同。垂直天线所宣称的增益由 10 dBi 至 3 dBi 不等。全向型天线如何产生增益呢？要记得，垂直天线只有在水平面才具备全向性。在三维空间里，其辐射形式类似甜甜圈。较高的增益意谓着该甜甜圈经过挤压，也意味着天线较大且较为昂贵，不过 802.11 服务所使用的天线并不大。

如果打算涵盖特定的户外区域，例如公司园区几栋建筑物之间的中庭，就不适合使用悬挂在屋顶的垂直天线，特别是建筑物本身相当高的情况下。由于本身半功率波束宽的缘故，垂直天线比较适合水平辐射，向下辐射的能力就不是那么好了。如果遇上这种情况，最好将天线置于一或二楼窗户外面。

偶极天线

偶极（dipole）天线具有 8 字型的辐射形式，亦即适合用于走廊或较狭长的地区。实际上，它和垂直天线看起来没有什么两样。事实上，有些垂直天线不过是直立组装的偶极天线。

八木天线

八木（Yagi）天线是常见的高增益指向型天线。它的形状有点类似传统电视天线。支架上悬挂着一排平行的金属片。然而，802.11 服务中，大概不会见到裸露的八木天线，因为商业用途的八木天线，通常会封装在天线罩（radome）里。天线罩本身只是一层塑胶外壳，用以保护买于户外的天线主体。802.11 服务所使用的八木天线增益约在 12 至 18 dBi 之间。校准八木天线并不会比碟型天线来得困难，不过还是需要一些小技巧。

碟型（抛物线型）天线

这是一种增益相当高的天线。由于碟型（parabolic）天线具备相当高的增益（商用 802.11 天线最高可达 24dBi），相对的波束宽也就更为狭窄了。碟型天线大概只能用来架设建筑物之间的链路。由于波束窄，因此对一般使用者而言并没有太大用处。有些厂商宣称其所销售的碟型天线传输距离可达 20 英里。预设上，链路两端系使用相同的天线。不要低估校准碟型天线的困难度。某种商用产品据称只有 6.5 度的波束宽。安装碟型天线时，最好将之牢牢固定。否则只要被暴风雨打偏，连接就可能为之中断。

有些厂商会额外区分网状（反射面有点类似弯曲的烤肉架）与平滑状碟型天线对此使用者无须担心，只要天线设计得好，就不必担心网状（mesh）与平滑状(grid) 反射面的容量差异。不过在强风地带，网状碟型天线就比较占优势。碟型与八木天线主要用于建筑物之间的链结。最大的问题是正确校准天线。如果双方距离不出目视范围，不妨训练一下自己的瞄准能力。其实在这种情况下根本不需要用到如此复杂的天线。如果栋距之间超出视力范围，除了买个较好的指南针，另外最好向美国地质勘查局（U.S. Geological Survey）买份地形图，然后估计如何彼此对准。记得要调整磁北（magnetic north）。如果愿意花一笔费用，或许可以在其中一方安装高增益的垂直天线，如此可以简化整个安装程序，因为只需要校准单边天线。如果信号相当微弱，校准完第一支天线后便可以用碟型天线取代垂直天线。

高增益天线可能会有管制上的问题，特别是在欧洲地区，因为当地的功率限制较美国严格。在美国，以 Orinoco 品牌销售的高增益碟型天线不能使用 ISM 频段边际的频道（即第 1、2、10 与 11 频道），因为信号会泄漏到频段之外。

23.5.1.1 天线接线

花了这么多工夫探讨天线，现在让我们回过头来思考，如何将天线连接至基站或无线网卡。大部分厂商均销售两种缆线：较便宜的细线（通常直径为 0.1 英寸）以及较昂贵与较粗的低损耗线（通常直径为 0.4 英寸）。细线通常不能超过几英尺长，因为细线相当容易造成信号损耗，太长就会吞噬掉所有信号。我曾接触过一个网站，它将基站隐藏在天花板之上，并使用穿越天花板的外接天线。不过，整个组装最后只是白费力气。外接天线的增益为 2 dB，但天线与基站之间的线材却有 2 dB 的损耗。细线主要是用来连接膝上型电脑的无线网卡与桌上型的可携式天线，如此而已。以数字来说明，假设有家厂商标明两公尺的缆线损耗为 2.5 dB。这意味着，在两公尺长的缆线中，信号强度消失将近一半。另外一家厂商所提供的线材标明在 2.4 GHz 频段，每一百英尺损耗为 75 dB。这意味着信号是以 2 的 25 次方（大约三千三百万）倍数损耗，这显然不是大家所乐见的。我知道有家厂商建议使用中度增益的 RG58 线材。

在携带式的场合，RG58 的确比细线好上一点，不过也好不了多少（每一百英尺 35dB）。如果采用 RG58 线材，请尽量将缆线截短。更好的方式是舍弃 RG58，看看能否换成 LMR-200（一种高品质・损耗只有一半的线材）。

如果使用低损耗线材，结果将会如何？情况显然较好，但可能不如各位的预期。有家 802.11 厂商使用 Times Microwave LMR-400 线材。LMR-400 是相当高级的线材，不过在 2.4 GHz 频段，每 100 英尺仍有 6.8 dB 的损耗。也就是说，在 100 英尺长的线材中，超过四分之三的信号会消失不见。由此例可知，天线要尽可能靠近基站，将传输线的长度尽量缩短。如果打算采用屋项型天线。为中庭用餐的使用者提供网络服务，记得不要将基站置于地下室的集线槽，然后再拉线至屋顶。如果可能，最好将基站置于屋顶，再以抗风化材料加以封装。如果不行的话，至少将基站置于阁楼或屋顶的管线间隙。尽量缩短传输线是最好的做法，没有其他方案可以取代。同时，切记传输线绕经墙壁或导管时有可能变短。我一直搞不懂为什么，不过只要仔细测量，就会发现缆线总是短少个两英尺。重点是：基站至天线的直线距离或许只有 20 英尺，如果最后得用上 50 英尺的缆线才有办法连接彼此，也不用太过惊讶。缆线本身或许会行经转角与导管，何况在到达目的地之前，还存在其他可能影响线长的因素。最后，天线接头也有关系。所有无线厂商均销售不同长度的缆线，并会附上所需要的接头与转接器。我强烈建议采用最便捷的方式，直接购买现成焊好接头的线材。接头损坏是无线系统失灵最常见的原因，尤其是安装 RF 接头经验不足时。

23.5.1.2 天线分集

改善多重路径衰落（multipath fading）常用的一种方法，就是使用多组天线（天线分集）。与其加大天线，无线系统可以使用多组天线，然后选用接收信号较佳的天线。采用天线分集（antenna diversity），并不需要用到复杂的数学理论或信号处理技术。有些无线局域网络厂商在无线网卡中内建多组天线。有些产品甚至允许无线网卡外接多组天线。802.11 标准建议使用天线分集，但并未强制要求。如果环境中的干扰十分严重，挑选厂商时不妨将天线分集纳入考虑。

23.5.1.3 放大器：放大功率

放大器主要用来提升信号的功率。在电波网络的发射端，放大器可以协助将信号传送至更远。涵盖更大的范围。有些发射放大器也整合了接收前置放大器，有助于改善信号灵敏度。

在室内部署 802.11 网络，通常无须使用放大器来提升传输功率。提升基站的传输功率可以覆盖更大的范围，能够加入网络的工作站也就愈多。为了维持信号品质，设计网络时最好使用较多的低功率小型基站。如果无线局域网络的部署重点在于覆盖范围而不计信号品质，就可以使用高功率的垂直天线。

一般而言，高传输功率只是说来好听，实际上并不见得较好，除了一些例外的情况。在提高基站密度之前，社区网络可能希望提供较大的覆盖范围，何况基站的价格远高于放大零件。以 802.11 打造的点对点链路也是放大器一项不错的应用。如果距离过长，天线增益根本就无法将信号拉至杂信基准之上 Ruby Ranch InternetCooperative (<http://www.rric.net>) 【注】 RRIC 本身就是个迷人的网站。我极力推荐。当地的电信公司拒绝在附近提供 DSL 服务，而一群志工却使之付诸实现。

所使用的上行链路算是记录比较完整的一个户外点对点案例。以 802.11 打造广域网络 (WAN) 的远端 ISP 也会广泛使用放大器。SSB Electronics (www.ssbusa.com/wireless.html) 与 HyperLink Technologies (http://www.hyperlinktech.com/web/amplifiers_2400.html) 是两家 802.11 放大器厂商。不过，如果打算使用 802.11 放大器，切记：

- 1、不要超出法定功率限制，不论是绝对功率或者 ERP 皆然。
- 2、802.11 无须使用执照。如果干扰到其他服务，那是你自己的问题。如果一项有照服务干扰到你，那也是你自己的问题。如果网络的服务范围太广又使用高功率，干扰问题通常无可避免。
- 3、必请使用合乎 802.11 标准的设备。有些放大器虽然涵盖所使用的频率范围，但是使用上并不合法。

FCC 的确强制要求落实相关规范，而且罚款相当惊人。如果你违反相关管制规定，FCC 大概会很不高兴，特别是超过功率限制或使用未经许可的设备。

第24 章 802.11 网络分析

没有痛苦，就无自觉。

—据说出自 C.G.Jung

1990 年代，电脑专业人员有如医师一般，必须为人们诊断疑难杂症。如同医生会遇到陌生人所提出的医疗问题，电脑专业人员也必须面对一堆由陌生人所提出的古怪技术问题。每当有陌生人知道我从事网络相关行业时，通常会问到：“为什么 Internet 经常断线？”“每当思索这个问题，我愈是相信真正的问题应该是：为什么 Internet 不会经常断线？”

虽然不敢奢望能够以本章有限的篇幅来回答上述问题，不过看得出来，网络问题虽然已经影响到了我们的现实生活。网络会断线，无线网络也不例外。无线局域网络能够提高生产力，完全瘫痪的风险也相对较高，何况可以确定的是，有限的频宽必然不够使用。建立无线局域网络后，网络工程师必须准备就绪，随时调查可能发生的问题。

不论针对何种网络，可信赖的网络分析工具在工程师的百宝箱中向来不可或缺。在骨干有线网络方面，不乏一些可以在疑难排除时提高生产力的网络分析工具。同样的，无线网络的疑难排除也可以受益于合适的网络分析工具。有时候，就是得凭借这些工具，才有办法知道空中发生了什么事。本章主要讲解网络工程师所凭借得网络分析工具。市面上有许多商用分析软件，Linux 平台也有一些免费得工具可用。不过在深入研究这些工具之前，我们最好先来探讨为什么网络管理人员需要无线网络分析工具。

24.1 网络分析工具

虽然有共同得传承，802.11 毕竟不是 Ethernet。它具备一些额外的协议功能，每个功能都可能是问题的来源。网管人员有时必须深入协议底层的细节，了解空中到底发生了哪些事，才能解决 802.11 网络的问题。在有线网络领域，网络分析软件向来被视为网管人员百宝箱里相当重要的工具，因为他们能够提供底层的细节。在无线网络领域，分析软件不仅同样适用，或许更重要。在 802.11 网络中，可能出现差错的细节更多，因此要能迅速找出疑难排除的着力点，一套优秀的分析工具是不可或缺的。

问题的避免最好开始于规划阶段。有些分析软件可以提供 RF 信号强度的细部统计报告，在决定基站摆设位置时非常有帮助。分析软件可以协助网管人员确保 BSS 之间有充分的重叠，以便及时切换，避免产生接收信号死角。当无线网络逐渐成长，必然需要能够为更多人提供服务。为了不影响效能，管理人员可能会考虑每个基站的覆盖范围，以便在既定范围内提供更多综合频宽。在缩小覆盖范围的过程中，网管人员或许必须将部署计划重新演练一遍，终究还是离不开手边的分析工具。

既然无线网络的频宽有限，迟早还是必须面对效能问题。效能问题有可能是因为有太多使用者共享太少部基站，或是与无线层所导致的问题有关。802.11 的设计者了解，无线传输介质可能导致哪些问题。实际上，遇到持续干扰时，通常会以较简单（以及较低速）的编码方式重新传送信号，并且对信号进行分片处理。

干扰是影响 802.11 网络效能的主要因素之一。除了直接导致已传送信号失效而必须重传，干扰同时会带来两种间接影响。低劣的传输品质可能导致工作站切换到较低位率，以便保持可靠

的无线链路品质。低速传输通常可以提高传输的成功率，不过也因此牺牲了传输量。此外，802.11 工作站可能会为了克服干扰而分片待传送的信息，因此降低了实际传送使用者数据的比例。相对与其它局域网络协议，802.11 的包头并不算小。当传输数据量不变，分片信息必然会增加所传输的包头数量。

一般网络只会用到几种应用程序。到底使用者所抱怨的效能问题，是指一般性的网络问题，或是某种特殊应用上的问题？只要检查所传送的封包大小，网络分析软件即可帮助找出问题原因。小封包较多，代表遇到干扰而使用帧分片功能。有些分析软件还可以提供无线网络帧传输率的分配报告。802.11b 网络能够以 11Mbps 的速率传输。不过如果干扰存在，帧即有可能以较低速率（5.5Mbps、2Mbps 或是 1 Mbps）传送。如果工作站具备高速的运作能力却以较低的速率传输，很有可能是因为大量干扰所致。效能取决于无线电波的性能（capacity）。降为较低速率的工作站或许不会占用太多传输量，却会占用电波介质相当多的时间。有些分析软体可以针对电波的使用率（radio utilization）提出报告，在追踪特定效能问题时特别有用。

要解决干扰的问题，可以将基站或天线换个角度，或是在覆盖不足的区域加装一部基站。分析软件可以让网管人员在心里有个概念。知道应该进行何种改变有助于解决问题，不必等到使用者向你描述有何异样。有些分析工具可以提供所收到帧的 RF 信号品质报告，以协助网管人员找出较佳的硬体摆设位置。避免将使用者当成白老鼠反覆试验，可让你看起来更专业一点，也可以让使用者舒服些。缩短疑难排除时间向来就是网络分析工具的强势所在。此外，网络分析工具尚可协助网管人员检验 802.11 MAC 特定功能的运作是否正常。

虽然可以在数据流经无线骨干网络时再加以解析，不过问题通常出现在无线链路上。帧是否得到回应？如果没有，则必须加以重传。DS 位元的设定是否正确？如果答案是否定的，那么位址栏位的诠释必然会出现错误。如果基站的有线端出现格式不对的封包，可能的损毁点将不只一个。分析工具可以在帧行经空中之际加以检视，协助找出损毁封包的来源。格式不符的帧可能来自工作站，也可能是被基站损毁的。寻求厂商支持之前，先确定问题所在，对问题排除有莫大的帮助。

24.1.1 8.2.11 网络分析软件

802.11 网络分析工具目前十分常见，每个无线局域网络管理人员的工具箱都应该配备。大部分的 802.11 网络分析软件都只须搭配一张 802.11 网卡即可使用。之所以不需要特殊硬体，是因为一般市售的 802.11 网卡，均已提供捕捉封包所需要的 RE 硬体。惟一需要注意的是，这些软件通常只能搭配市面上几种网卡使用。

任何无线网络部署的预算，都应该将网络分析软件纳入考量。要直接购置或自行打造悉听尊便，不过我预料大部分机构主要还是以采购商用产品为主，将开发与除错的工作交由网络分析软件厂商负责，毕竟商业级分析软件的采购、安装以及使用，都比自行打造来得快。

24.2 Ethereal

Ethereal 是标准的开放原始码网络分析软件。和其他专属分析软件一样，它支持一系列通讯协议，可以从不同网络界面捕捉即时数据。和其他专属分析软件不同的是，Ethereal 完全来自一句口号「Sniffing the glue that holds the Internet together。Ethereal 可以在大部分的 Unix 及 Windows 平台上执行。这两种平台的原始码均自由取得，不过修改工作在 Unix 平台上比较容易，因为 Unix 平台有许多可以免费取得的程序开发环境。如同许多开放原始码专案，Ethereal 的发行受到 GNU Public License 的规范。许多常见的网络协议解码功能均内含其中。就本节而言，最重要的协议是 IEEE 802.11 以及 LLC，每个 802.11 帧都会用到这两者。当然，TCP/IP 阴定组也包含在内。

随著 802.11 逐渐普及与 Linux 逐渐提供更好的支持，可供搭配的硬体也愈来愈多。起初只有 Prism 芯片组网卡支持网络分析。不过，目前大多数界面卡均已提供这项功能。本节所使用的 Ethereal 为 2005 年一月底所发行的 0.10.9 版。

Windows 平台上的封包捕捉

Ethereal 采 pcap 这个封包补捉程序库之上。Windows 可以使用移植到此平台的版本，不各为 WinPcap。虽然 Windows 几乎支持所有 Ethernet 界面无线网卡的程序界面还是有所不同。有些网卡使用 promiscuous 模式时无法补捉任何帧。即使关闭 promiscuous 模式，有些网卡依然只能补捉往来于该工作站的讯框。相较于 Linux，在 Windows 补捉与线封包与所使用的网卡密切相关，因此我比较倾向使用 Linux 平台。

24.2.1 编译与安装

要建立 Ethereal 程序已经不像以前那么困难。一些无线分析所需要的修正档，均已整合到主要的原始码中，因此可以「开箱即用」(out of the box)。在编译 Ethereal 之前，必须先安装 libpcap 与 GTK+程序库。libpcap 用来捕捉封包，GTK 则是用来显示结果。此外，核心 (kernel) 功必须支持才有办法捕捉封包，因此在设定核心配置时，必须加入 Packet Socket (CONFIG_PACKET) 选项。Ethereal 本身使用标准的开放原始码编译程序。

Ethereal 与 Windows

在 Windows 环境中，可执行套件的重要性相对较高，因为缺乏高品质而免费的开发环境。虽然在 Windows 环境上并未提供相同等级的 802.11 支持，Ethereal 还是值得拥有，特别是在每天都需要用到 Windows 系统的日常工作裡。Windows 版的 Ethereal 可执行档，可自 <http://www.ethereal.com> 下载。在 Windows 裡，Ethereal 需要用到 WinPcap 程序库来提供类似 libpcap 的支持。WinPcap 可自 <http://netgroup-serv.polito.it/winpcap/> 下载。WinPcap 只支持 32-bit Windows 作业系统 (95、98、ME、NT 以及 2000)，以 BSD 方式授权使用。值得注意的是，Microsoft Research 对 WinPcap 提供了部分的赞助。

24.2.2 将无线界面设定为监听模式

要捕捉封包，必须先将无线界面切换为监听模式 (monitoring mode)，这相当于 Ethernet 界面的封包捕捉模式 (promiscuous mode)。被动监听模式的方法，因无线驱动程序而异。

24.2.2.1 Cisco Aironet 无线网卡

Cisco Aironet 无线网卡有两种监听模式。第一种称为 rfmon 模式，驱动程序会传回目前工作站所在网络的所有帧。第二种简称为 Y 模式，驱动程序会捕捉目前频道的任何帧。要选取监听模式，可以通过 proc 文档系统更改驱动程序的执行配置：

```
bloodhound: #echo "Mode: rfmon" >/proc/driver/aironet / ethX/Config
bloodhound: # echo "Mode: y" >/proc/driver/aironet/ethX/Config
```

要回到正常的工作站设定，可将模式切换回 ess

```
bloodhound:#echo "Mode: ess" >/proc/driver/aironet/ethX/Config
```

捕捉封包时，必须将所使用的网络界面名称提供给 Ethereal。2.4.19 版以前的系统核已可以使用界面的 Ethernet 名称 (ethX)，2.4.20 版之后则使用 wifiX。

24.2.2 Prism 无线网卡

采用 Prism 芯片组的网卡有两种驱动程序可供使用：Absolute Value Systems 的 linux-wlan-ng (<http://www.linux-wlan.org>) 以及 HostAP 驱动程序 (<http://hostap.epitest.fi>)。linux-wlan-ng 驱动程序在 0.1.15 版之后，将监听纳入基本功能。它的启用是通过 wlanctl-ng 命令，而非无线延伸功能 (wireless extensions) 命令：

```
bloodhound: -# wlanctl-ng w1an0 lnxrecy_wlansniffer enable=true channel=6
```

要关闭监听模式，可以使用如下的命令：

```
bloodhound: -# wlanctl-ng w1an0 enable=false
```

采用 Prism 芯片组的网卡也可以搭配 HostAP 驱动程序进行监听。它使用自订的 (private) 系统呼叫 (类似无线延伸功能) 来启动监听模式。只要传送监听模式命令 (2 或 3) 给网卡，就可以启动监听模式。模式 2 可以监听所有标头，模式 3 只用来监听 802.11 标头。要关闭监听模式，可以将模式指定为。：

```
bloodhound: -# iwpriv eth1 monitor mode
```

```
bloodhound: -# iwpriv eth1 monitor 0
```

24.2.3 Orinoco 无线网卡

0.15 版以后的 orinoco cs 驱动程序不须修补便已支持监听模式。较早版本的修补程式可自 <http://airsnort.shmoo.com/orinocoinfo.html> 下载。要检视驱动程序是否经过修补，可以用 iwpriv 命令来查询：

```
bloodhound: -# iwpriv eth1
```

如果驱动程序支持监听功能，也可以通过 iwpriv 来予以启用。支持监听功能的驱动程序具备两种模式。模式 1 会在前面附加 Prism 格式的监听标头，用来报告信号强度及其他物理层参数，模式 2 则只附加 802.11 标头。监听时可以任选一种模式以及频道。例如要监听第 6 频道且要求附带完整的 Prism 标头监听信息，可以使用如下的命令：

```
bloodhound: -# iwpriv eth1 monitor 1 6
```

要停止监听，可以将模式指定为 0

```
bloodhound: -# iwpriv eth1 monitor 0
```

24.2.4 采用 Atheros 芯片组的网卡

采用 Atheros 芯片组的网卡使用第十九章所提到的 MADwifi 驱动程序。最新版的 MADwifi，可以用 iwconfig 命令将网卡切换为监听模式。如有必要，也可以用 iwconfig 指定所要监听的频道，例如以下列命令来设置 ath0 接口：

```
bloodhound:~# iwconfig ath0 mode monitor
```

```
bloodhound:~# iwconfig ath0 channel 6
```

不过我发现某些版本必须事先指定一个 IP 地址，接口才会出现在封包捕捉列表。所指定的 IP 地址与实际使用与否无关。

```
Bloodhound:~# ifconfig ath0 1.2.3.4
```

```
Bloodhound:~# ifconfig ath0 up
```

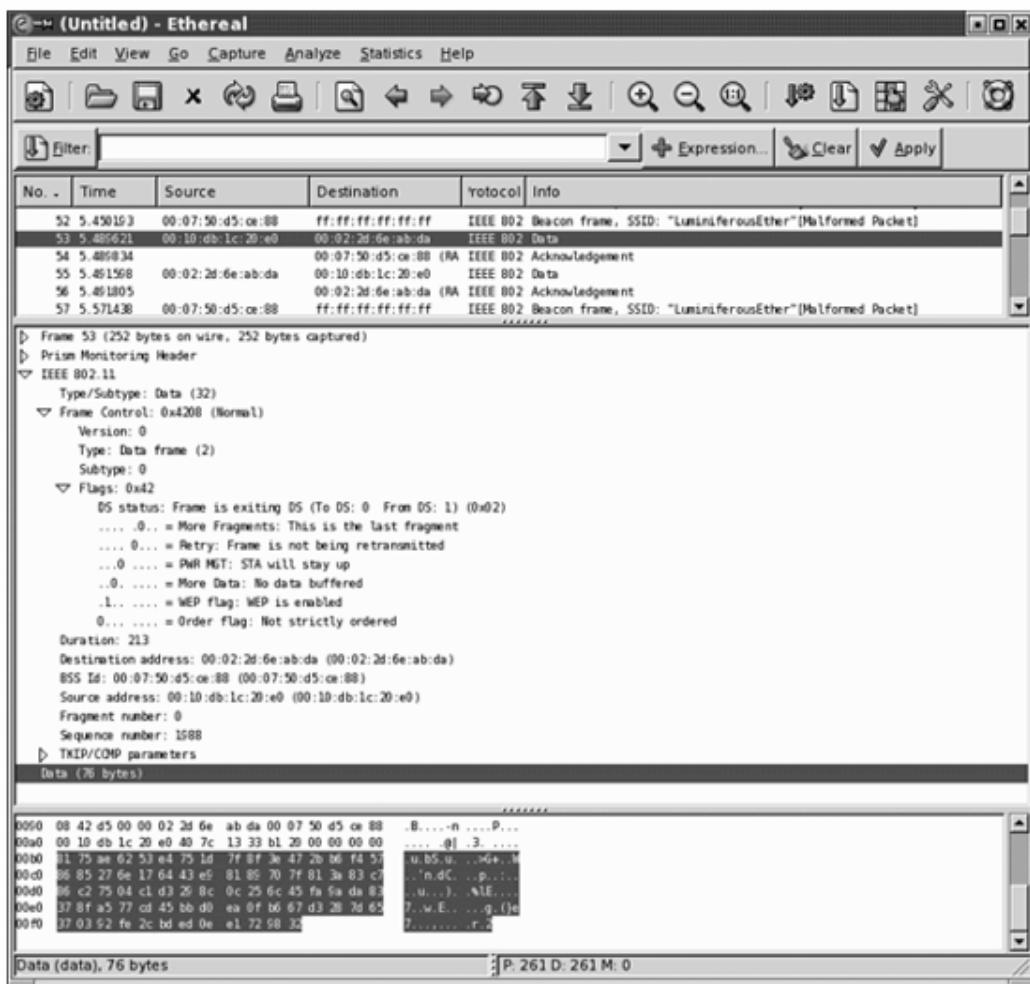
24.2.3 执行 Ethereal

执行 Ethereal 后会跳出主视窗，如图 24-1 所示。任何使用者均可执行 Ethereal，但是必须具备管理者权限方能够捕捉封包。（不过任何使用者均可载入捕捉档进行分析。）主视窗分为三个部分：最上面的窗格称为封包列表窗格（**packet list pane**），提供个别封包的高价观点。它会列出每个封包的捕捉时间（**Time**）来源与目的地址（**Source** 与 **Destination**）、协议（**Protocol**）以及封包的基本解码（**Info**）。**Protocol** 栏所填的是用来分析该帧的最终解码协议。在 802.11 网络上，最终的解码协议可能是 IEEE 802.11 管理帧，或是 TCP 协议分析（如果该 802.11 帧包含了一个经过 LLC 封装的 IP 封包，以及一个装载 HTTP 的 TCP 区段）。随着链路层加密的使用频率增加，802.11 通常成为最终的解码协议，因为 Ethereal 的原始封包捕捉（**raw capture**）无法对这些帧进行解密，也无法「看透」受保护的上层协议。

中间的窗格称为树状视图窗格（**tree view pane**）。封包中所有主包头均会列出，展开后可以得到更多细节。所有封包均有基本的「**Frame**」树状视图，其中包含到达时间与捕捉长度等细节。802.11 网络可以加入 **Prism Monitoring** 包头，其中包含无线链路数据。**Prism** 包头原本是针对 Prism 设备所开战，后来为大多数驱动程序所采用。虽然图 24-1 来自采用 Atheros 芯片组的网卡。不过 MADwifi 驱动程序还是在前面附加了 Prism 监听包头。有些驱动程序则提供是否启用 Prism 包头的选项。

最底层的窗格称为数据视图窗格（**data view pane**）。用来显示所选封包的原始二进制数据。同时会标示「树状视图窗格」所选之栏位。如果能够的话，就会进一步解析该帧。对于未加密数据，Ethereal 可以解读链路层（Logical Link Control，简称 LLC）包头 LLC 可以包含 ARP 封包 "IP 封包"TCP 区段（segment）等数据 Ethereal 包含了许多常用的协议解析器（**dissector**）。通常可以完整解析 802.11 帧。不过经过加密的帧就无法解读了，如图中反白部分所示。

Figure 24-1. Main Ethereal window



在树状视图窗格选取任何栏位，数据视图窗格中相应的位就会反白显示。图 24-1 选取了帧的 Data 栏位，底下的数据视图窗格即以反白显示。我个人比较喜欢使用等宽字型（monospace font），如此一来底下数据视图窗格所呈现的数据就可以对齐栏位。

位于 Ethereal 视窗最上方的信息列包含四个重要元素。最左边的按扭（Filter::）用来指定过滤条件，只列出感兴趣的封包。其后的文字输入框（text box）允许使用者直接键入过滤条件，不必从头开始设置。Ethereal 会将之前所使用的过滤条件留存在历史列表（history list）条件的切换变得较为简单。最后是一个文字栏位，用以显示各种不同的信息，这取决于当时 Ethereal 正在进行何种过程。它可能显示 Ethereal 目前正在捕捉封包，也可能显示所载入的捕捉文档名称，或树状视图中目前标示出的栏位。

24.2.3.1 捕捉数据

数据的捕捉十分直接。找到 Capture 选单，接着选取 Start 选项，随即会出现 Capture Preferences 视窗。Ethereal 可以使用它所检测到的任何接口，甚至是无线局域网络接口。

第一件事是选取想要监听的界面。以无线网络接口而言，所使用的名称可能是 `eth`, `ath` 甚至 `wlan`。不过在开始捕捉封包之前，必须先将接口切换到监听模式。在 `Ethereal` 中可以使用`-i` 命令列选项来指定接口。如果想统一使用单一接口处理分析事宜，可以使用命令将 `ethereal` 对映至 `ethereal -i ath0`。

通常，我会启用“`Update list of packets in real time`”以及“`Automatic scrolling in live capture`”两个选项。如果不选取前者，只有当捕捉停止时方能追踪整个过程..。如果不选取后者，整个追踪纪录就无法下拉到最后面。对于即时分析而言，速度相当重要。将域名解析（`name resolution`）停用，可以减低封包捕捉的负担，也让工作站免于丢失封包。

24.2.4 减少数据量

原始的捕捉文档可能十分庞大，要在一堆无用的封包中披沙拣金可是一件极高度的挑战。善用网络分析软件的关键在于，将封包数目筛选至关键的少数封包。为此，`Ethereal` 提供了三种方式：捕捉过滤（`capture filters`）。显示过滤（`display filters`）抓及标注封包（`marking packets`）。

24.2.4.1 捕捉过滤

捕捉过滤（`capture filters`）是降低 `Ethereal` 所处理数据量的最有效率方式，因为它们会大量涌入监听封包的接口。如果封包捕捉接口丢弃某个封包，该封包就不会送至 `Ethereal` 做进一步处理。遗憾的是，捕捉过滤对 802.11 而言并没有多大用处。如果在前面附加 Prism 监听包头，就无法使用捕捉过滤。

`Ethereal` 使用了 `libpcap`，因此其所使用的捕捉过滤语法和 `tcpdump` 一样。其中提供了一些基本的语句，可以任意组合为较长的表示式。这些基本语句允许以 Ethernet 或 P 地址、TCP 或 UDP 端口号，以及 IP 或 Ethernet 协议作为过滤条件 • 也有一些是以来源或目的地址作为过滤条件。遗憾的是，大多数适用的协议编号在 802.11 网络中通常经过加密，因此没有多大用处 •

802.11 帧在 LLC 包头中携带有 Ethernet 协议编号，因此在加密网络上无法轻易予以过滤。

24.2.4.2 显示过滤

显示过滤（`Display filters`）用在 `Ethereal` 能够辨识的任何栏位，光是这一点就比捕捉过滤强大许多。显示过滤可以使用 `Ethereal` 内建的所有解码器，因此可以过滤 `Ethereal` 能够辨识之协议的所有栏位。无线局域网络管理人员可以根据 802.11 或 LLC 包头栏位来过滤帧。802.11 封包过滤的实际范例将于本章稍后提及。

24.2.5 使用 Ethereal 进行 8.2.11 分析

应用到 802.11 网络时，有些 `Ethereal` 功能可以随时使用。本节将会列出一些在无线网络使用 `Ethereal` 的小技巧，排列先后并无特定意义。

24.2.5.1 显示过滤

`Ethereal` 可以过滤 802.11 包头中任何栏位。帧栏位将依结构阶层排列。所有 802.11 栏位的变量名称均会前置 `wlan` 字样。并以两种次类别分别记载 `Frame Control(wlan.fc)` 及 `WEP Information (wlan.wep)` 栏位的相关信息。图 24-2 显示了 802.11 包头栏位的变量名



称。图中，每个栏位均会标上数据类型。Boolean 栏位会标上 B; MAC address 会标上 MA; 无符号整数会标上 U，另外加上位数。表 24-1 所列出的是相同信息，只不过删去了无助于 **Ethereal** 显示过滤的栏位。

Figure 24-2. Header component variables

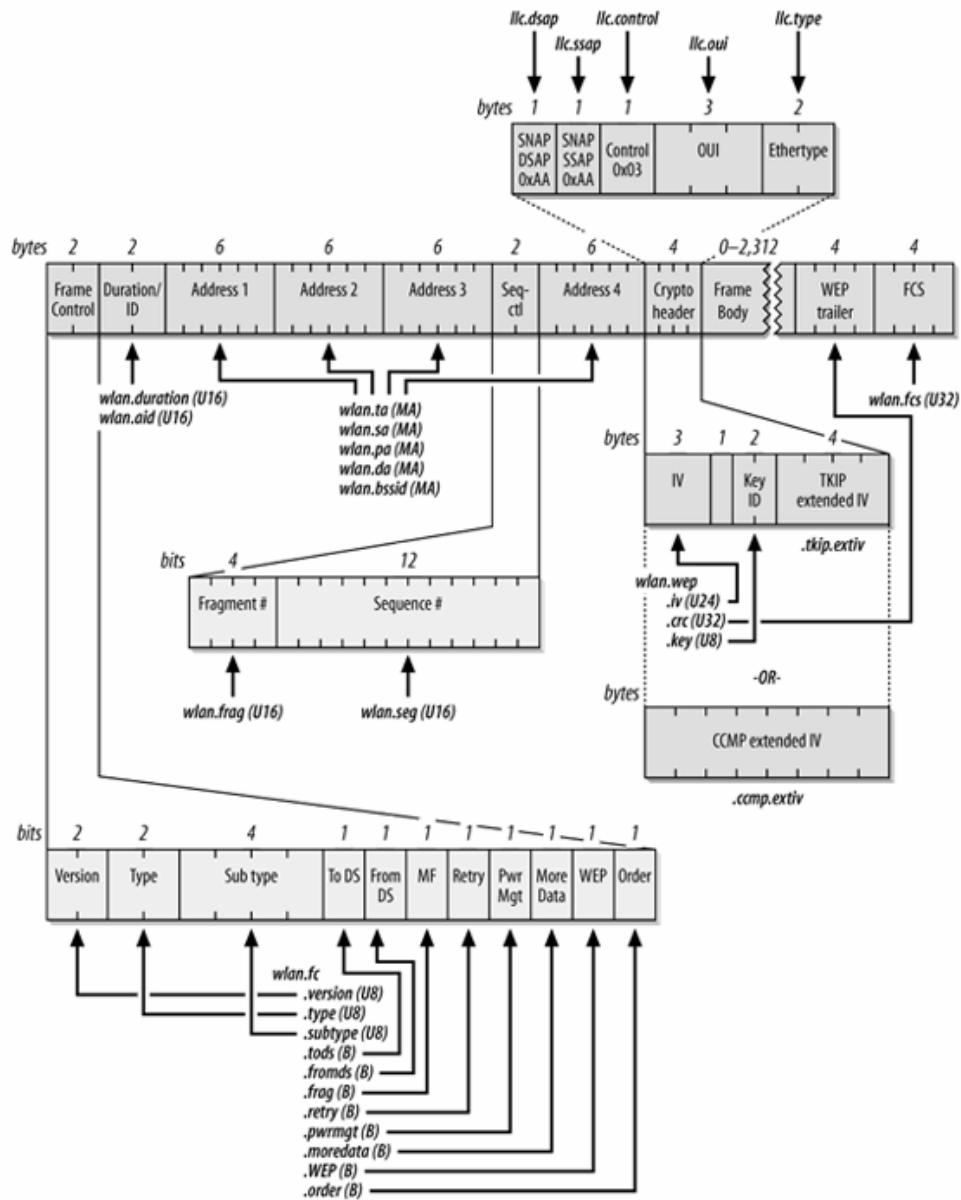


Table 24-1. Ethereal fields for 802.11 header components

Table 24-1. Ethereal fields for 802.11 header components

802.11 header field	Ethereal field
Header fields	
Either source or destination address	wlan.addr
Transmitter address	wlan.ta
Source address	wlan.sa
Receiver address	wlan.ra
Destination address	wlan.da
BSSID	wlan.bssid
Frame control subfields	
Frame type	wlan.fc.type
Frame subtype	wlan.fc.subtype
ToDS flag	wlan.fc.tods
FromDS flag	wlan.fc.fromds
Retry flag	wlan.fc.retry
Protected frame (WEP) flag	wlan.fc.wep
Protection fields	
WEP Initialization vector	wlan.wep.iv
TKIP IV	wlan.tkip.extiv
CCMP IV	wlan.ccmp.extiv
Key identifier	wlan.wep.key

这些栏位可以通过运算符 (operator) 加以组合。Ethereal 支持了一组标准的比较算符: `==` 代表相等, `!=` 代表不相等, `>` 代表大于, `>=` 代表大于或等于。`<` 代表小于, 而 `<=` 代表小于或等于。举例而言, 显示过滤若为 `wlan.fc.type == 1`, 代表控制帧.逻辑算符 `and` 与 `or` 均有支持。如同许多程序语言, 惊叹号 (!) 代表逻辑上的否定。Boolean 类型的栏位可用来检视存在与否, 因此欲启用 WEP 的控制帧可用如下的“显示过滤”来表示:

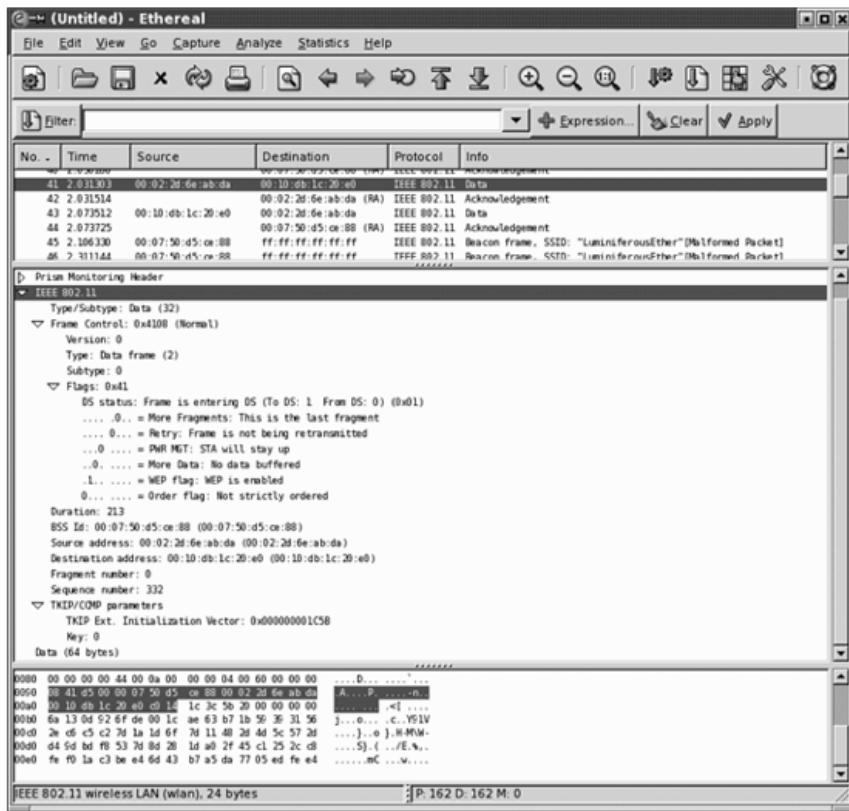
`wlan.fc.type == 1 and wlan.fc.wep`

图 24-多以树状视图 (tree view) 显示了完整的 802.11 包头。在树状视图窗格中选取 802.11 包头。底下的 ASCII 视图就会将组成 802.11 包头的位反白显示。将 802.11 包头的树状结构展开, 即可解读所有栏位。

24.2.5.2 了解 LLC 包头以筛选协议

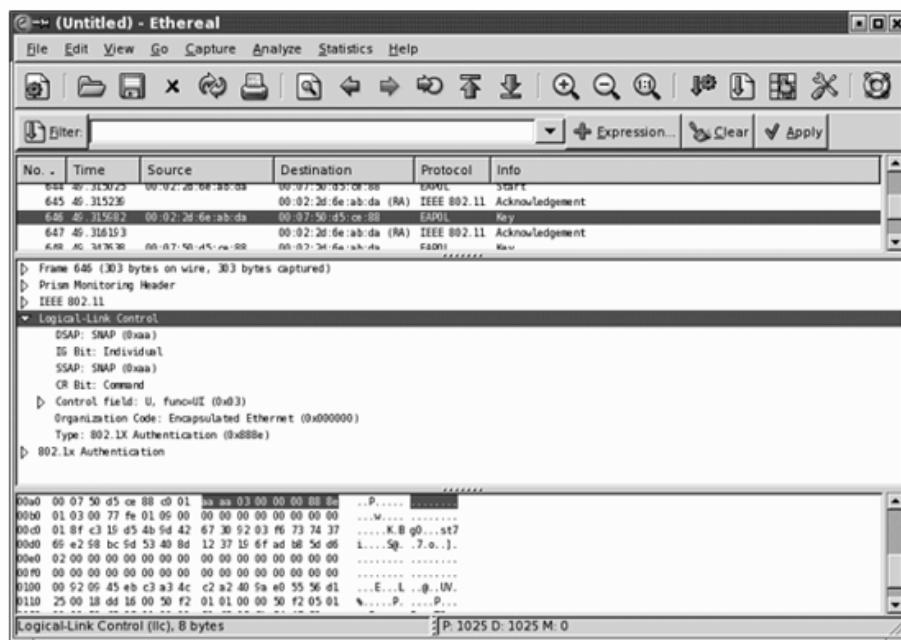
为了在无线链路之上, 以多任务传送较高层协议的数据, 802.11 采用了 LLC SNAP 封装。(SNAP 封装在第三章结尾处已有提及。) 802.11 并无协议栏位, 因此接收端无法直接从包头分辨不同类型的网络协议。为了能够支持多种协议, 因此加入了长度 8 个位组的 SNAP 包头。SNAP 包头经过解码, 显示于 Ethereal 的树状视图窗格, 如图 24-4 所示的 EAPOL 密钥帧。

Figure 24-3. An 802.11 header in tree view



点选树状视图中的 LLC 包头，相应的 8-byte 包头即会出现在封包倾印(packet dump)处。从数据视图窗格 (data view pane) 该包头由五个栏位构成：

Figure 24-4. LLC SNAP header



DSAP (目的服务访问点) - llc.dsap

对 SNAP 封装而言，这个值通常设置为 0xAA。

SSAP（来源服务访问点）-llc.ssap

对 SNAP 封装而言，这个值通常设置为 0xAA。

Control（控制）-llc.control

此栏位源自 HDLC 和所有以 HDLC 传递的数据一样，它被用来将 LLC 包头之后的数据标示为未编号信息 (unnumbered information) 所谓未编号信息是

指，使用非连接式数据传输(connectionless data transport)，而且该数据无须重新排序或予以回应。

OUI（组织代码）-llc.ui

此栏位用来决定如何解释其后的位组。IP 以 RFC 1042 标准封装于 LLC；RFC1042 规定使用 OUI 0x00-00-00。(有些厂商或许会使用特定的 OUI 做为专属系统传输之用。)

Protocol Type（协议类型）-llc.type

此栏位由相应的 Ethernet 帧复制而来。Type 栏位对应到 Ethernet 的类型代码。在 IP 网络中，其值可能是代表 IP 的 0x0800 或代表 ARP 的 0x0806。图中显示为 0x88-8e，因为此帧乃是 EAP OL (802.1X) 帧。

802.11 规格将 LLC 封装列为必要，因为这样一来，802.11 帧就无法直接承载信息。不过有时 LLC 包头经过加密，除非事先解码，否则无法得知实际的内容。

24.3 802.11 网络分析项目清单

为了说明网络分析软件如何协助网络工程师监看无线局域网络流量，本节列出了排除一般身份认证问题时的项目清单 (checklist)。此处所举的例子虽然使用 **Ethereal**，不过也适用于之前所提到的商用软件。

24.3.1 显示过滤初探

显示过滤对 802.11 而言特别有用，因为它们能够用于解码帧的细节。在进行一般疑难排除程序之前，了解显示过滤的若干组成要件将有所帮助。

24.3.1.1 排除 Beacon 帧

追踪 802.11 原始数据时，Beacon 帧可能造成妨碍。大多数产品最多每秒可送出 Beacon 帧十次，占捕捉到的帧绝大多数。要移除 Beacon 帧，可以撰写相当于 Beacon 帧的显示过滤条件，然后予以排除。

- 以 wlan.fc.type==0 指出所要筛选的是管理帧。
- 以 wlan.fc.subtype==8 指出所要筛选的是 Beacon 帧。
- 将两者合并后，为其加上惊叹号（逻辑的否定运算）：!(wlan.fc.type==0 and wlan.fc.subtype==8)。

24.3.1.2 筛选来自特定工作站的数据

通常，封包捕捉系针对某部受测工作站与工作站之间将会有不同类型的帧往来，因此进行筛选的方式，取决于所要筛选的项目。

第一种方式是在显示过滤中使用 `wlanaddr` 变量，以之代表来源或目的地址。

- 若要保留来自某部工作站的数据，可以使用

“`Fwlan.addr= =00:02:2d:6e:ab:da`”形式的显示过滤，只要在其中填入适当的 MAC 地址。这种方式相当于使用

“`Fwlan.sa= =00: 02:2d:6e:ab:da or wlan.da= =00:02:2d:6e:ab:da:`”只是后者比较冗长。

来源与目的地址只出现于 802.11 数据帧。要排除某些问题，可能必须深入检视 802.11 管理过程，例如帧的正面回应。帧的正面回应是针对接收端地址，而非目的地址。要检视往来于特定工作站且包含回应信息的帧，可以在显示过滤中指定接收端地址。

- 只要以”`wlan.ra= =00:02:2d:6e:ab:da`”形式的显示过滤，将受测工作站的 MAC 地址指定为接收端地址，就可以显示所有传送给该工作站的回应信息。要检视该工作站所发出的回应信息，必须加入第二个接收端地址，格式为

“`wlan.ra= = 00:02:2d:6e:ab:da or wlan.ra= =00:0b:0e:84: 32: 91`”，其中第二个地址代表提供服务的基站。

24.3.1.3 筛选特定的协议

如果可以取得数据帧的内容，则可以把 LLC 包头设置为显示过滤的对象。要查看特定的协议内容，可以使用 `llc.type` 变量。输入协议编号时，必须使用不带破折号的十六进制数值。

- 使用”`llc.type= =0x888e`”形式的显示过滤，可以查看特定的 Ethernet 协议。

此外尚可利用 LLC 包头来搜寻以 802.1H 封装的帧，其 OUI 为 00-00-F8。 `llc.oui` 系六个位的十六进制数值。在加密网络上，LLC 包头只出现于 802AX 帧，因此如果此过滤条件没有显示较上层的协议，也无须感到惊讶。

- 以 RFC 1042 进行分封的帧，可用 `llc.oui= =0x000000` 予以显示
- 以 8023H 进行分封的帧，可用 `llc.oui= =0X0000F8` 予以显示。

24.3.2 一般疑难排除过程

对如何以“显示过滤”筛选出感兴趣的帧有了初步了解后，就可以进一步探讨疑难排除过程。本节主要在探讨如何筛选出感兴趣的帧并予以描述，不打算使用一堆画面捉图 (`screenshot`) 详细举例说明。

24.3.2.1 身份认证疑难排除

- 显示过滤：筛选出往来于某部工作站的 EAPOL 帧，同时查看其回应信息
`llc.type= =0x888e and wlan.addr= =supplicant-MAC and
(wlan.ra= =supplicant-MAC or wlan.ra= =AP-MAC)`

每个 EAPOL 帧均有一个识别码，以序号的形式出现。每个 EAP 封包均用来回应之前所接收到的信息。查看 802.1X 会话程序 (`session`)，确定每个 EAPOL 帧均有相应的 802.11 回应

信息，而且 EAP 识别码会逐一累进。有些申请者无法应付重传的情况，并会导致当机。（因此，基站必须对这些当掉的 802.1X 会话程序解除身份认证，要求其重新开始。）

只要查看 EAP 封包的内容，就可以发现身份认证于何处失败。如果是在 TLS 管道建立后才发生错误，有可能是因为申请者无法验证服务器的凭证。如果数据已经通过 TLS 管道，便有可能是其它因素所造成。此时可以查看 RADIUS 服务器的纪录档找寻线索。

24.3.2.2 密钥传递的疑难排除

- 显示过滤：筛选出往来于某部工作站的 EAPOL 密钥帧。

```
Llc.type= =0x888e and eapol.type= =3 and wlan.addr= =supplicant-MAC
```

正确传递密钥必须经过六个步骤。部分磋商程序如图 24-5 所示。首先必须完成四道磋商。作为一开始的完整性检验，必须确定每个帧均得到正面回应。最快的方法是检视 Ethereal 中的帧编号。如果帧编号每次进 2，有可能跳过的即为 802.11 回应帧。

密钥传递失败最常见的原因之一，就是申请者 (supplicant) 与认证者 (authenticator) 的安全性参数不符。Ethereal 内建解析器 (dissector) 可以解读密钥帧中所包含的信息元素。图 24-S 的树状视图窗格底不显示被解读出的信息元素之开头。其中，群组密钥被解读为动态 WEP 之后只有一组单点传播密码锁组合 (unicast cipher suite)。WPA 规定只能有一组单点传播密码锁组合，不过大多数产品并未遵循此规定。有些申请者并未依循一般做法，因此无法顺利通过身份认证。如果 Association Request 与密钥磋商程序所使用的信息元素不符，认证者将会判定此次交换程序失败。

24.3.2.3 效能的疑难排除

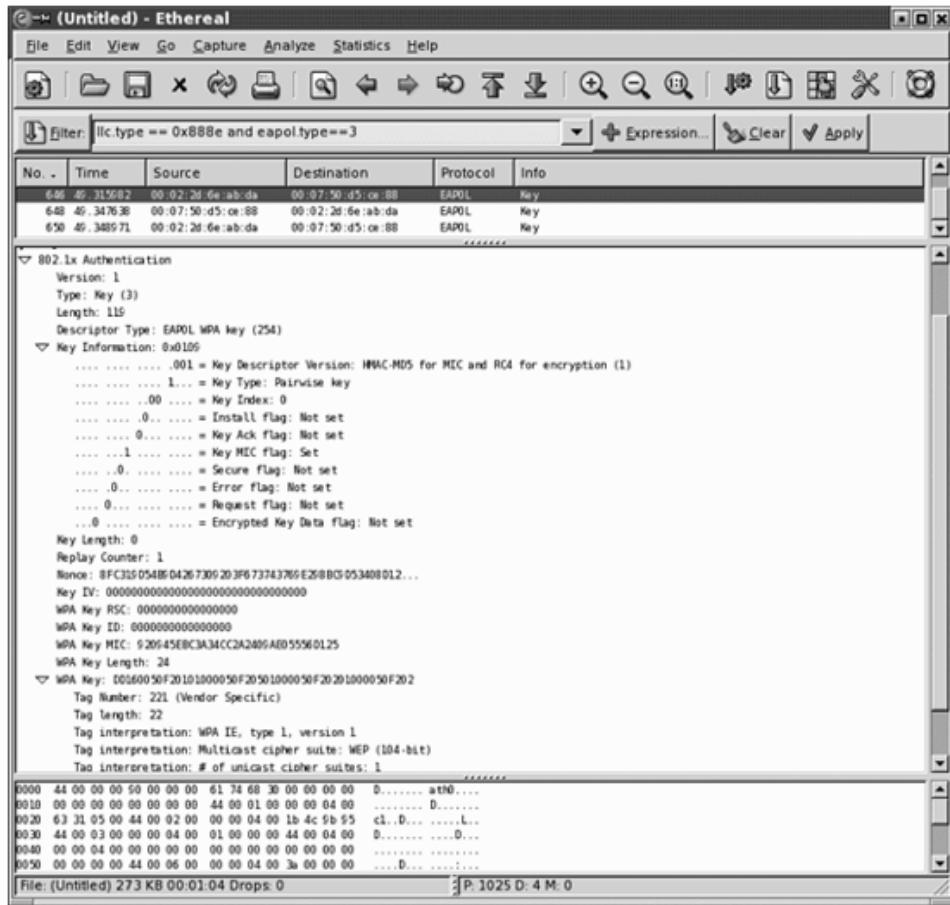
排除效能问题通常比辨识效能问题来得简单。一般而言，效能议题可以分为下列几种：

- 显示过滤 1：筛选出往来于某部工作站的帧，同时检视回应信息。

```
wlan.addr= =client-MAC and(wlan.ra= =supplicant-MAC or wlan.ra= =AP-MAC)
```

此过滤条件可以显示往来于特定工作站的所有数据以及回应信息。检视记录下来的所有数据，并查看是否有重复传送的帧。如果没有接收到回应信息，则必须重传完整的帧。如果重传数次之后仍然没有得到回应，网卡就会降低传输速率以改善连接的可靠度。较低速率所需要的“信噪比”较低。解决这类效能问题的方式之一，是在该区增加基站密度以提升信号品质・改善基站或工作站所使用的天线也会有所帮助。

Figure 24-5. Key handshake



- 必显示过滤 2：筛选出低于某种速率的数据。

`prism.rate.data <(speed tag)`

搭配上一个过滤条件，可以只显示高于或低于特定速率的帧。Prism 监听包头中是以一个整数代表帧速度。由于它是以 500 kbps 为单位，因此以 megabits 表示时必须将它乘以 2。例如，要显示所有低于 2 Mbps 的帧，必须指定为

`prism.rate.data<4。`

数据视图窗格下面的状态列，用来显示封包数目以及已显示的封包数目。图 24-1 中，被捕捉到的帧数为 261（注记为 P），而这 261 个帧均已显示 C 注记为 D）。以计算机搭配显示过滤 2，将可以让你对何种速率传送多少帧有大致的概念。有些商用软件系以“精灵”（wizard）且向时显示分析结果。

- 显示过滤 3：筛选出来自重叠网络的数据。

`wlan.bssid != AP-MAC`

使用者或许会抱怨因网络重叠所造成的效能问题。802.11 b/g 网络的效能特别容易受到重叠网络的影响，因为实际上只有三个 C 非重叠）频道可用。要评估网络重叠的程度，可以在捕捉封包后使用“显示过滤 3”保留来自其它网络的帧。如果帧为数不少，试着找出那些基站的位置所在，然后予以关闭。

24.3.2.4 WEP 数据解密

有些分析软件可以解读 WEP 加密帧，只要在其中提供密钥即可。举例而言。在 **Ethereal** 的 **Edit** 选单点选 **Preferences** 选项，然后选择 **IEEE 802.11 protocol**，就会出现如图 24-6 所示的 WEP 选项。只要键入密钥，**Ethereal** 就会以这些密钥解读经加密的帧。人工 WEP 密钥比较容易取得，动态 WEP 密钥就必须仰赖申请者或者基站方面提供。**iwconfig** 命令可显示出 **Linux** 申请者所使用的加密密钥。有些基站以特定的方式提供密钥表的内容，网管人员可利用它找出工作站所产生的密钥。

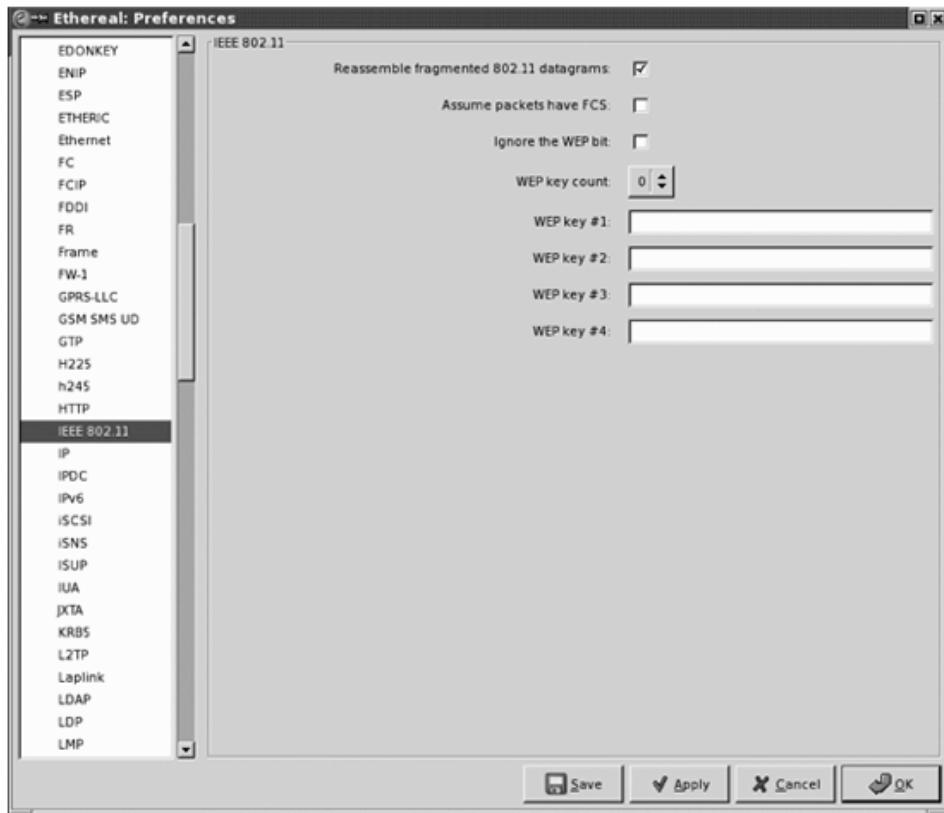
24.3.2.5 RADIUS 分析

虽然不见得与无线局域网络相关，**Ethereal** 事实上也可以解读 RADIUS 帧。在 **Preference** 的 **RADIUS** 协议选项中，可以键入 RADIUS 所使用的共享密码。输入之后，所有经保护的栏位均会被自动还原。如此一来或许可以自动还原动态密钥，不过我尚未听说有任何 **Ethereal** 外挂模组可以达到此目的。

24.4 其它工具

其它工具通常用于网络分析。虽然不限于作为疑难排除工具，不过它们通常被用来评估覆盖范围

Figure 24-6. Entering WEP keys



24.4.1 搜索、量测与对映网络

802.11 网络是与之连接的首要步骤。有些分析工具可以找寻或评估现有网络的覆盖范围。极端的网络搜寻方式称为“扫基站”(wardriving)，亦即使用者以网络搜寻软件记录下所有基站的位置。NetStumbler (<http://www.netstumbler.com>) 与 Kismet (<http://www.kismetwireless.net>) 是其中最著名的两种工具。

网络检测是一种被动的程序。Beacon 帧可以通过 802.11 接收器加以搜集，根本无从防范。假定网络必然会被发现是最好的对策。与其依赖晦涩的网络名称或者隐蔽的网络位置，甚至是较低的传输功率，倒不如使用正确的安全工具，例如使用第六与第七章所提到的身份认证与加密方式来保护网络。就算网络被发现，也无妨于其中的数据。

24.4.2 WEP 密钥还原

目前有些开放源码工具可以用来攻击 WEP 弱点密钥。其中最著名的就是 AirSnort，于 2001 年 8 月首度问世。最新的源码可自 <http://azrsnort.shmoo.com/> 下载。AirSnort 是第五章所提到之「Fluhrer-Martin-Shamir WEP 攻击：最早与最著名的公开实现，不过并非目前惟一的破解工具[注 1]

WEP 密钥还原工具主要是针对某些特定的“弱点”初始向量(IV)。Ethereal 借用 AirSnort 的分类码，目前已经可以显示出弱点 IV。商用软件很早以前就具备这项功能。

要防范 WEP 密钥还原攻击，网管人员可以将密钥使用时间缩短为 5 到 15 分钟。有些厂商已经修改源码，避免使用弱点初始向量(IV)。2002 年初，Inter-op Labs 发现许多厂商以惊人的速度立即做出回应，从此不再使用弱点 IV。到了 2004 年，虽然有两年的时间可以进行修正，列在已修正名单上的几乎还是同一批厂商。

24.4.2.1 估计密钥还原时间

密钥的还原有两个要件。首先，必须搜集到够多带有弱点 IV 的帧，方能进行攻击，我称之为搜集时间(gathering time)。其次，成功的攻击必须处理留存下来的帧，我称之为分析时间(analysis time)。[注 2]

以我自己的经验而言，要搜集到足够的数据远比实际进行攻击要耗费更多的 CPU 时间。只要有足够的样本，分析只不过需要几秒的时间。分析时间系以线性成长，因此较长的密钥只能多提供几秒钟的保护。如果将密钥长度加倍，攻击所需要的 CPU 时间也会倍增，不过将几秒钟加倍仍然是几秒钟。

24.5 身份认证

大多数无线网络的 802.1X 身份认证协议，是以 TLS 管道提供安全防护。ssldump 工具(<http://www.rfn.net/ssldump>)可用来解读 TLS 磋商程序，以及经由管道传输的任何数据。不过解密时需要凭证所使用的密钥副本。

注[1]

实际的范例参见 WEPcrack (<http://wepcrack.sourceforge.net>) 与 Aircrack (www.cr0.net/8040/code/network/aircrack)

注[2]

有关分析时间的探讨，参见 <http://securityfocus.com/iaafocus/1814>

第25 章 802.11 效能比较

过去一段时间，无线网络管理人员已经搭了一阵子顺风车。无线网络不仅新鲜，而且够酷。使用者对它们可以提供什么样的服务，大多没有什么概念。只要可以运作，使用者就已经心满意足，告诉他们不要期待无线网络会提供类似 100BaseT Ethernet 的效能，就可以轻松交待过去。大部分无线设备的使用者并不多，因此不会有好几打，甚至上百部工作站同时连接到由少数基站构成的服务区域。此外，大部分无线网络在逻辑上大多从属于现存的有线网络。在设计上，802.11 是为了弥补现存局域网络的不足，而不是打算取而代之。如果使用上偏重有线局域网络，就算没有无线网络，使用者还是可以完成手上的工作，因此无线网络似乎没那么重要。比较可能发生的问题是，你不知道要如何摆设基站，使它能够覆盖所需要的范围，以及如何安装驱动程序，然后随时更新你的安全配置设置。

不过，网络会随着时间成长，使用者的要求也会愈来愈高。网络效能或许相当差劲，即使只有你注意到这件事。改变外在环境（例如，调整基站的摆设位置，使用外接式天线，等等）或许可以解决某些问题，不过有些问题最好通过调整参数来解决。本章所要讨论的主题，即是加以微调便可改善整个无线网络效能的管理参数。

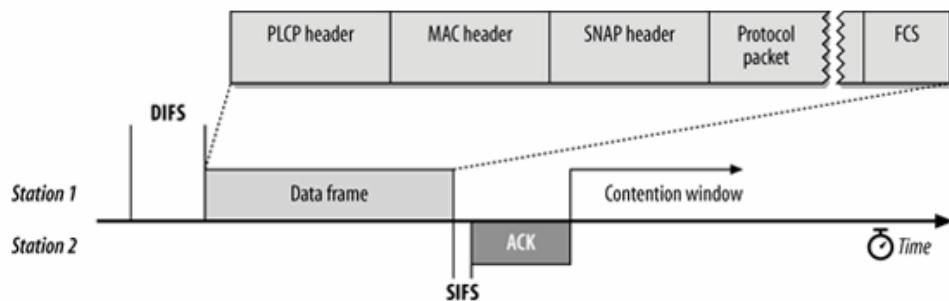
25.1 802.11 效能评估

和其它网络技术一样，802.11 的速率也有两种。一种是名目上“号称”（headline）的速率，另外才是网络上实际传输的速率。大多数情况下，实际的数据传输量一定低于所宣称的数字。在 802.11 领域，实际承载数据（payload）的传输量更是低于其所宣称的数字，主要是因为协议本身的负担就已经很大了。将名目（或额定）速率腰斩一半，大概就是实际的数字。这算是不赖的经验法则。

为了有助于与实际结果的两相比较，通常可以事先计算出理论上的最大传输量。

802.11 的数据传输由一系列基本过程(atomic operation)所组成，如图 25-1 所示。图中所显示的是最简单的帧交换，由一个 802.11 Data 帧及其回应帧所构成。至于基本过程的组成要件，后续会加以说明。当然，如果牵涉到帧分片，或是必须用到第 H 章所提到的 802.11g 防护机制，整个交换程序就会比较复杂。

Figure 25-1. Atomic operation



每个基本过程均由几个帧组成，帧之间以“帧间隔”（inter-frame spacing）加以区隔。访问介质时，通常以分布式帧间隔（Distributed Inter-frame Space，简称 DIPS）开始整个帧交换

序列。之后的帧则以短帧间隔 (Short Inter-frame Space, 简称 SIPS) 加以区隔。DIPS 与 SINS 的实际值取决于所使用的物理层，详见相关章节。

帧必须通过物理层传送至空中，因此每个帧均具备物理层包头，由同步信号以及其它协助解读帧的栏位所组成。一般而言，同步信号乃是物理层包头传输时间的关键组件。物理层帧本体包含 MAC 帧，占用 28 个位组。MAC 帧中包含了长度为 8 个位组的 SNAP 包头，因此封装一个数据帧，就会增加多 6 个位组的额外负担。如果再加上加密包头，MAC 包头的长度就不止如此了。

较上层协议封包本身，是根据所使用的特定物理层规则加以传送的。不同物理层各有其最小区块 (block)，或信号 (symbol) 大小，以位为单位。速率为 11 Mbps 的 802.11b 网络使用长度为 8 个位的讯符。802.11a 与 802.11g 所使用的讯符可以承载更多的数据，至于讯符的大小，则取决于所使用的速率。以 54 Mbps 为例，其所使用的讯符长度为 216 个位。(未来 802.11n 甚至将采用更大的区块。) 数据区块的传送需要固定的时间各种速率之间的差异，主要是各个数据区块所封装的数据位数不同，和传送区块的快慢无关。例如，对物理层帧而言，1,536 个位组的承载数据 Cpayload) 包含 f 12,288 个位。以别 2.11a 物理层来讲，此帧需要个万只符来传递。

要计算一次基本交换过程 (atomic exchange) 需要多少时间，可以先将它拆解成几个步骤，然后加总个别步骤所需时间。首先，我们从帧间隔的加总开始。虽然目前的趋势倾向于采用较复杂的帧结构，不过有些基本交换过程，帧间只包含一个 DIFS 以及一个 SIFS。计算出用掉多少帧间隔后。接下来就可以根据所使用的物理层，开始分析帧的基本成份。每个帧的分析方式通常都一样，只有防护机制是比较明显的例外，因为此时必须用到较旧的传输类型。每个帧均具备一个物理层包头 (physical header)，以及之后的物理层承载数据 (physical payload)。物理层承载数据就是 MAC 帧 (由 MAC 包头 • 任何数据帧特有的 SNAP 包头、较上层协议的封包，以及标尾所组成)。

25.1.1 计算示范

举例而言，假设我们打算在 802.11a 网络上传送 1,500 个位组的单一数据帧。此分析的目的，纯粹是为了示范如何解析帧的成份，并不代表完整的模型，因此较上层协议可能造成的影响均忽略不计。

802.11a 网络中，每个 SIFS 需时 16 微秒，每个 DIFS 需时 40 微秒。交换一个数据帧，工作站需要等候一个 DIFS 时间，接着传递它的数据帧，然后等候回应帧，802.11 回应帧会在经过一个 SIFS 时间后传出。因此帧间隔总共享掉了 50 微秒。

接下来，解析数据帧。802.11a 的 preamble 与 signal 标位需时 20 微秒。1,500 个位组的数据封包被封装于 MAC 帧，加上 SNAP 包头，总长度为 1,536 个位组。如果此帧受到 COMP 的保护，进行封装时就会附加上 16 个位组的包头与完整性检验值，如此一来，物理层帧的承载数据总长度即为 1,552 个位组，相当于 12,416 个位。以 54 Mbps 的速率来讲，物理层帧的承载数据会以每个讯符 216 位的方式进行分片，因此传递此帧会用到 58 个讯符 (12416/216)。每个讯符需时 4 微秒 (216/(54*10^6))，所以传递此数据帧共需时 232 微秒 (58*4)。

802.11 回应帧的长度只有 14 个位组 (112 个位)，因此只需要一个 40 Mbps 讯符即可传送完毕。有些芯片组使用较低的速率 36 Mbps 以上的速率只需用到一个讯符。至于较低速率就需要不止一个讯符。18 Mbps 需要两个讯符，12 Mbps 需要三个讯符，9 Mbps 需要四个讯符，而 6 Mbps 需要用到五个讯符。考虑在传输时间和稳定性之间取得合理的平衡，假设回应信息以

12 Mbps 传送。三个讯符需时 12 微秒，加上包头（20 微秒）总计需时 32 微秒。加总起来，长度 1,500 个位组的承载数据需要用到 50 微秒的帧间隔。232 微秒的传送时间以及 32 微秒的回应时间，总共是 314 微秒。如果没有竞争的情况发生，每秒可进行 3,184 次基本交换过程 ($1/(314*10^6)$)。每次交换可以传递 1,500 个位组的数据，因此总传输量为 38 Mbps ($3184*1500*8$)。在接近理想状况下，协议数据大约耗费理论速率的 30%($((54-38)/54)$)。

25.1.1.1 效能模型的其它成份

上述讨论隐含了许多过于宽松的假定。大多数实际运作的 802.11 网络能够达到理论值的 55% 到 60% 就算不错了。重要的网络通常会用到上层协议，因此会造成封装上额外的负担。例如，TCP/IP 包头就用掉了 40 个位组，同时还会要求对方予以回应。传输量是否进一步往下滑落，取决于 TCP/IP 如何被整合到此一效能模型。

此外，上述范例也隐然假定没有介质竞争的情况发生，然而这并不符实际。虽然 802.11 MAC，会尽量避免碰撞情况发生，但是碰撞终究不可避免。有些工程师认为 TCP/IP 甚至会使得碰撞的情况更加恶化，因为当传送端继续传送数据时，TCP/IP 却已经试图传送会话层（session-layer）的回应信息给传送端。

其它一些来源，例如协议堆叠所造成的负担，也会影响网络的效能。上述计算尚未剔除 Beacon 帧所造成的负担，也未考虑帧丢失对传输量所造成的影响。

25.1.1.2 区块回应

有了上述范例，就比较容易了解“区块回应”（block acknowledgment）这个概念的威力何在。帧间隔与 802.11 回应信息用掉了基本交换过程 10% 以上的传输时间。只要调整数据帧与回应之间的比例，就可以大幅降低这些负担所耗费的时间。

25.2 改善效能

由于频宽有限，无线网络通常背负着效能不彰的罪名。如果有人这样抱怨，在研究出改善效能的策略之前，当务之急就是找出客观评估效能的方法。有些商用的网络分析软件会提供“频道使用率”（channel utilization）报告。报告的内容不外乎是花费在传送与接收帧的时间比例，或是每秒传输多少百万位。比较起来，前者应该比较有用，因为它将「因距离基站的远近所可能产生的速度变动」也纳入考虑。如果所有已连接的工作站均相距甚远，或许只能以 1 Mbps 的速率进行过程。假设频道完全以 1 Mbps 的速率进行传输，根据上例所描述的理想状况，以 100% 的频道使用率而言，可以达到 0.94 Mbps 的传输量。有些分析软件只会提供位传输率报告，但并不会提到使用率有多高..

如果有竞争无线电波资源的情况发生，就应该加以调整，减少竞争的次数。提升效能的最好方法，就是调降基站的功率。只要缩小覆盖范围，工作站和基站的距离就必然较近，如此将（有希望）可以在较高的速率进行过程。

覆盖范围较小还有助于避免共享频道（co-channel）的干扰问题。基站必须在覆盖范围内共享频宽。如果有两部高传输功率的基站使用相同频道，就有可能彼此干扰。虽然通讯协议在设计上已经将此问题纳入考虑，不过两部设备同时进行传输还是会严重拖垮效能。另外指定不同的频道也有助于避免干扰，不过频宽还是受限于目前技术上所容许的频道数。对 802.11b 与 802.11g

而言，完全独立的频道只有三个，但还是可能受到邻近基站相当程度的干扰。**802.11a** 可以使用较多的频道，因此较适合应用在基站密度较高且覆盖区域彼此重叠之处。

改换更好的物理层也是个办法。**802.11b** 网络必须将已经不敷使用的 **6 Mbps** 频宽分配给所有已连接的工作站。**802.11a** 与 **802.11b** 可以提供较高的传输量，一般约有 **30Mbps** 左右。如果可能的话，升级所有工作站也有助于效能的提升，不过要特别注意 **802.11g** 防护机制。防护机制会大幅降低传输量。虽然无法提供精确数据，根据还算不赖的经验法则推估，防护机制大概会降低一半以上的传输量。

如果防护机制真的拖垮了整个传输量，当务之急就是予以停用，不过说的通常比做的简单。只要有任何 **802.11b** 信号就会激发防护机制，不论工作站是否已经连接。既然 **802.11b** 设备的设备量不小，**802.11b** 网络大多被迫启动防护机制，因此大幅降低了整体的效能。【注】

至于高频宽、高密度的网络，最好采用 **802.11a**。它的频道不仅比较多，也不必背负回溯相容的包袱。

有时候，效能其实受限于网络架构本身。如果在无线局域网络与其它网络之间树立一道防护墙，所有流量就会受限于单一瓶颈。如果该瓶颈无法负荷所有流量，效能就会因此大打折扣。安全性协议也会对效能造成负面影响，例如，**Ipsec** 允许上层协议传送最大封包 (**maximum-size packet**)，不过一旦加上 **Ipsec** 包头，反而必须进行封包分片。分片之后，两者（最大封包与零星封包）均必须竞争介质使用权才能进行数据帧的传输，因而会导致传输的迟延。

【注】由此看来，一般使用者该选择 **802.11b/g** 或者 **802.11a** 就再清楚不过了。协助建立 **Supercomputing 2004** 会场的无线局域网络时，我发现 80 部基站山塞满了 1300 位 **802.11b/g** 使用者，而 **802.11a** 使用者只可 100 人。用我的 **802.11 a** 网卡，不仅无须和他人竞争无线介质，也可以全速上网。

效能也有可能因为应用不同，反而被认为差劲。一般而言，数据传输相当具有弹性，对于网络迟延问题比较宽容。数据帧迟到的情况并不构成问题，因为这不过意味着网页载入得较慢。数据传输的流量通常起伏不定，就算瞬间涌进大量封包，也是可以接受的。如果网络需要支持即时传递，工程就变得比较复杂。语音传输必须能够及时送到，次序不能错乱，流量也不能起伏不定。就算网络频宽可以支持数百万比特流量的服务，如果所提供的语音品质低于一般，还是令人无法接受。**802.11** 网络的服务品质 (**Quality of Service**) 系依据刚开始形成的规格。虽然基站承受得住少许的语音通话，一旦网络负载增加，或者语音数据无法及时传送，服务品质就会大打折扣。就算网络未达饱和，语音效能还是有可能十分差劲。

若要榨干每一滴网络效能，最后手段就是微调 **802.11** 规格书所列的各种参数，下一节将针对这些参数做进一步的探讨。不过就我本身经验所及，调校 **802.11** 参数并无法大幅提升效能，因此不值得投注太多时间。基站已经十分便宜，不如多添购几台，反而比较符合经济效益。

25.3 802.11 可调参数

802.11 有一些可供调校之处，可以在比较严峻的情况下，尽可能挤出额外的效能。不过，如要找出最佳数值，不免要经过一番试验。

25.3.1 无线电波管理

和其它类型的无线网络一样，**802.11** 网络最珍贵的资源即是无线频宽。无线频谱受限于管制当局，无法轻易增加。可喜的是，有些参数可以优化网络无线资源的使用状态。

25.3.1.1 信标间隔 (Beacon Interval)

Beacon 帧在“基础型网络”(infrastructure network)里扮演着许多基本角色。基本上，Beacon 帧定义了整个“基本服务组合”(basic service set, 简称 BSS)的覆盖范围。在基础型网络里，所有沟通都必须通过基站，就算在同一个 BSS 当中有两部工作站要传递帧亦然。基站通常会固定地点，如此一来，Beacon 帧的传送距离，便不会因时间而改变。【注】

【注】多重路径干扰(multi-path interference)会在特定时袁}J产生特定的干扰样式(interference pattern)。某些特定地点、有时位于基站的 A 19 ft，有时受到多重路径衰落的影响。不过，类似地点已在芦盖范易的边睡地带，周此不该将迅视为基太服务区域的一部分。此外 802.16(WiMax)极有希望能够在行进间提供连接与数据传输。

工作站通过 Beacon 帧，可以判断出目前所在范围有哪些「延伸服务组合」(Extended Service Set, 简称 ESS) 提供服务，同时利用所收到的信号强度来监视信号品质。

不过，传送 Beacon 帧会耗费无线频宽资源。如果缩短 Beacon 发送间隔，被动式扫描(passive scanning)就会比较稳定，也较为快速，因为 Beacon 帧会较常将网络的存在公布给无线链路。Beacon 间隔较短，有助于提升漫游的效率·因为漫游中的节点收到覆盖信息的频繁度也会因此增加。Beacon 帧岭送得愈频繁，对移动较快的节点而言愈有好处，因为更新信号强度相关信息的速度相对变快。【注】延长 Beacon 发送间隔，间接提高了连接节点的省电能力，因为监听间隔(listen interval)以及 DTIM 间隔都会因此改变，这些在“电源管理调校”一节都会加以探讨·延长 Beacon 发送间隔也可以让传输量有所提升，因为介质的竞争会因而减少。Beacon 帧所占用的时间，是无法用来传送数据的·如果各位使用虚拟基站网络，由于每个网络均需要有自己的 Beacon 参数组合，负担就会急遽倍增。

25.3.1.2 RTS 门槛

802.11 包含 RTS/CTS 净空程序(clearing procedure)，主要在辅助较大帧的传送。任何大于 RTS 门槛的帧，都必须经过净空程序，方能够通过 RTS 由天线加以传送，而且必须收到来自传送对象的 CTS 信号。RTS/CTS 主要在对抗来自隐藏节点的干扰·通过通知邻近地区所有工作站即将进行帧交换，RTS/CTS 交换机制可将来自隐藏节点的干扰降至最低。802.11 标准规定，RTS 门槛应该设置为 2,347 个位组。如果网络传输量相当低，或重传帧比例偏高，就可以降低 RTS 门槛以启动 RTS 净空机制。

第三章曾经提到，所谓的隐藏节点是指网络上存在工作站看不到的节点·在什么情况下会遇到隐藏节点？老实说，其实不少。网络上总是有些角落，虽然节点能够与基站直接通讯，但节点之间却无法彼此对话。想像一个最简单的网络：一部基站位于广场中央，没有其它事物可以反射或阻挡信号。一部行动式工作站，从基站所在位置向东移动，直到信号微弱到几乎无法通讯。另外一部工作站往西移动·两部工作站都可以和基站通讯。不过彼此都无法得知对方的存在。

以上的模拟状况应该可以说服各位，隐藏节点其实不可避免，但并不常见。工作站与最近的基站之间如果都相去甚远，在恶劣的环境下，愈有可能导致隐藏节点。不过，既然无线网络已经十分普及，四处林立的基站实际上已经足以避免大多数的隐藏节点问题。

【注】不过，802.11 原本就不是针对高速移动而设计的。细胞(cellular-based)广域技术在方面较占上风。

25.3.1.3 分片门槛

MAC 层级的帧分片，是由分片门槛（**fragmentation threshold**）这个变量所控制。任何大于分片门槛的帧，都会被分片为较小的单位，再加以传送。分片门槛的预设值是 2,346，或物理层所容许的 MAC 帧最大长度。不过，RF 物理层所使用的 MAC 帧长度通常是 4,096 个位组，因此这个参数通常预设为 2,346。这个值立即会让人联想到，其与 RTS/CTS 净空程序经常一并进行。

在干扰十分严重的环境中，调降此门槛可以提升整体传输量。一旦丢失某个帧片段，需要重传的部分也只有该片段。定义上，丢失的帧片段必然小于整个帧，因此重传所需花费的时间较短。设置这个参数必须特别小心。设得太低，有效传输量反而会下跌，因为回应每个片段必须用掉额外的时间。同样地，设得太高也会降低有效传输量，因为较大帧一旦毁损，便会增加无线频道重传的负担。

25.3.1.4 重传限制

网络中每部工作站都具备两种重传限制（**retry limit**）。其中之一是，丢弃帧之前可以重传的次数限制。长帧重传限制（**long retry limit**）适用大于 RTS 门槛的帧，预设值为 4。需要用到 RTS/CTS 净空机制的帧有四次重传机会，如果该帧遭丢弃，就会通知较上层的协议。短帧重传限制（**short retry limit**）适用小于 RTS 门槛的帧，预设值为 7。

降低重传限制可减少个别系统所必须准备的暂存空间。帧越快超时，丢弃这些超时帧的速度就越快，因此记忆体更新速度也越快。提高重传限制可能会降低传输量，因为与上层协议间的互动会更加频繁。当 TCP 遗失封包，较好的实现方式会放慢速度。较大的重传限制值也可能增加宣告封包遗失所需要的时间。

25.3.2 电源管理调校

从一开始，802.11 就是为行动设备而设计的。行动设备之所以有用，就是因为它不受电源线的限制，因此大多配备电池。802.11 包含了一些参数，可让工作站节省电力，然而代价是牺牲整体传输量，或造成工作站的迟延。

25.3.2.1 监听间隔

当工作站与基站连接，所指定的参数之一即是监听间隔（**listen interval**）。所谓监听间隔，是指工作站两次苏醒之间，历经多少次 Beacon 间隔数。较长的监听间隔可让工作站关闭传送器较长的时间。关闭电源较久，意味着可以省下更多电力，因此显著地延长了电池的使用时间。每部工作站都可以设置自己的监听间隔。

延长监听间隔有两个缺点。基站必须为休眠中的工作站暂存帧，因此较长的监听间隔对基站而言，意味着必须准备更多暂存空间（缓冲区）。如果监听间隔较长的工作站为数甚多，就可能超出基站暂存空间的负荷。其次，增加监听间隔会延迟帧的传递。如果基站准备转送数据给工作站时，工作站正处于休眠状态，该帧只好等到工作站苏醒之后，再加以传送。苏醒之后，工作站必须从所收到的 Beacon 帧中，判断基站上是否有暂存帧，然后送出 PS-Poll 帧以撷取暂存数据。整个暂存与撷取过程会增加帧的传送时间。这种情况是否可以接受，完全取决于对流量的需求。就电子邮件之类异步的传输而言，延长监听间隔不会造成太大的问题。不过对于要求即时陆。时问灵敏度高的应用程序（烦 J 如证券市场即时信息，或未来通过 802.11 界面的 IP phone），

就无法接受较长的监听间隔。延迟时间增加对某些特定的应用程序而言，有可能产生问题。数据库应用程序特别容易受到延迟时间的影响。目前已经有一个任务小组着手 MAC 的改良过程，以便在 802.11 网络中确保传输的服务品质，不过标准目前尚未底定。

25.3.2.2 DTIM 期间

DTIM 期间仅限基础型网络使用，所有与基站连接的节点均会分享此参数。这个参数系由基站管理人员所设置，并且在 Beacon 帧中加以广播。所有 Beacon 帧均包含一个“数据待传指示信息”（traffic indication map，简称 TIM），用以告知工作站是否有暂存帧待传。为个别工作站暂存的单点传播帧，只有在工作站轮询时才会加以传送。这种轮询的方式并不适用于多播或广播帧，因为这样一来必须耗费不少频宽，而且传递多播帧与广播帧要花费一番工夫。基本上，广播与多播帧是在每次 DTIM (Delivery TIM) 时间过后传送的，而不是使用轮询的方式。

改变 DTIM 与改变监听间隔有相同的效果。（这并不值得惊讶，既然 DTIM 如同多播与广播帧的监听间隔。）增加 DTIM 可让行动式工作站节省较多的电力，不过代价同样是必须耗费基站更多的暂存空间，以及回应时间的延迟。增加 DTIM 之前，最好确定一下，所有应用程序均容许延迟时间的增加，以及广播与多播并不是用来同时传递数据给所有工作站。如果应用程序使用广播与多播帧，来确保所有工作站同时收到相同数据，例如即时跑马灯，增加 DTIM 反而会造成反效果。

25.3.2.3 ATIM 期间

在基础型网络里，大部分的省电功能是由基站所提供。在独立型（或特设）网络中，部分省电功能则移交网络适配卡的驱动程序处理。在特设（ad hoc）网络中，工作站必须随时保持清醒，以便传送或接收 Beacon 信号，而且在 ATIM (Announcement TIM) 的过程中也必须处于清醒状态。至于 ATIM 期间，则是以时间单位（TU）来度量。

减少 ATIM 期间可以节省较多的电力，因为行动式工作站所需要的开机时间会因而减少。在两个 Beacon 信号间，工作站可以关闭电源，这段期间不必有任何动作。增加 ATIM 期间同时提高了工作站苏醒的机率，如果其它工作站也有帧待传的话。服务品质也会因此提升，所需要的缓存空间也相对较小。

对同步或即时应用而言，减少或不用 ATIM 期间的效果，相当于在基础型网络里延长 DTIM 期间。换句话说，对于要求即时传递数据的应用，这么种可能会引起问题或导致不稳定。连接游戏是“对等式”（ad hoc）网络最显着的即时应用，不过“对等式连接游戏”（ad hoc gaming）网络在调校上，通常侧重低延迟与高传输量，而非省电功能。

25.3.3 计时过程

计时过程是 802.11 网络中一项要件。许多管理过程都牵涉到好几个步骤，每一项过程都会用到本身的计时器。

25.3.3.1 扫描计时

为了决定要加入哪一个网络，一开始工作站必须先扫描现有网络。有些产品允许使用者设置扫描时间。在这些产品中，可能会同时开放主动扫描计时器（active scan timer）与被动扫描计时器（passive scan timer）供使用者设置。所谓主动计时器，是指工作站送出 Probe Request

帧之后，预计花费多少时间等候回应信息，以 TU 为计时单位。所谓被动式扫描，是指工作站监听各个无线频道的 Beacon 帧；被动式扫描计时器，是指工作站切换到下一个频道前，在每个频道所停留的时间。

25.3.3.2 与加入网络有关的计时器

当工作站要加入基础型网络，就会与基站进行身份认证并与之连接。每个步骤都有相应的超时计时器。认证超时（authentication timeout）在认证过程的每个阶段都会重新设置；如果有哪个步骤超时，认证就算失败。在较忙碌的网络中，可能必须提高超时值。连接超时（association timeout）在连接过程中扮演着类似的角色。

25.3.3.3 停驻时间（只见于跳频网络）

FH PHY 停留在单一频道上的时间称为停驻时间（dwell time）。它通常是由当地管制当局（local regulatory authorities）所规定，因此无法设置，除非通过网卡驱动程序变更为不同的管制区（regulatory domain）。

25.3.4 可调参数一览表

为了便于查询，表 25-1 列出了本章所有内容的一览表，包括每个可调参数可能造成的效果。

Table 25-1. Summary of common tunable parameters

Parameter	Meaning and units	Effect when decreased	Effect when increased
Beacon	Number of TUs between transmission of Beacon frames.	Passive scans complete more quickly, and mobile stations may be able to move more rapidly while maintaining network connectivity.	Small increase in available radio capacity and throughput and increased battery life.
RTS Threshold	Frames larger than the threshold are preceded by RTS/CTS exchange.	Greater effective throughput if there are a large number of hidden node situations.	Maximum theoretical throughput is increased, but an improvement will be realized only if there is no interference.
Fragmentation Threshold	Frames larger than the threshold are transmitted using the fragmentation procedure.	Interference corrupts only fragments, not whole frames, so effective throughput may increase.	Increases throughput in noise-free areas by reducing fragmentation acknowledgment overhead.
Long Retry Limit	Number of retransmission attempts for frames longer than the RTS threshold.	Frames are discarded more quickly, so buffer space requirement is lower.	Retransmitting up to the limit takes longer and may cause TCP to throttle back on the data rate.
Short Retry Limit	Number of retransmission attempts for frames shorter than the RTS threshold.	Same as long retry limit.	Same as long retry limit.
Listen Interval	Number of Beacon intervals between awakenings of powersaving stations.	Latency of unicast frames to station is reduced. Also reduces buffer load on access points.	Power savings are increased by keeping transceiver powered off for a larger fraction of the time.
DTIM Window	Number of Beacon intervals between DTIM transmissions (applies only to infrastructure networks).	Latency of multicast and broadcast data to powersaving stations is reduced. Also reduces buffer load on access points.	Power savings are increased by keeping transceiver powered off for a larger fraction of the time.
ATIM Window	Amount of time each station remains awake after a Beacon transmission in an independent network.	Increases power savings by allowing mobile stations to power down more quickly after Beacon transmission.	Latency to powersaving stations is reduced, and the buffer load may be decreased for other stations in the network.
Active Scan Timer	Amount of time a station waits after sending a Probe Response frame to receive a response.	Station moves quickly in its scan.	Scan takes longer but is more likely to succeed.
Passive Scan Timer	Amount of time a station monitors a channel looking for a signal.	Station may not find the intended network if the scan is too short.	Scan takes longer but is more likely to succeed.
Authentication	Maximum amount of time between successive frames in authentication sequence.	Authentications must proceed faster; if the timeout is too low, there may be more retries.	No significant effect.
Association Timeout	Maximum amount of time between successive frames in association sequence.	Associations must proceed faster; if the timeout is too low, there may be more retries.	No significant effect.

第26 章 结论与展望

我们终于可以一窥 802.11 网络目前发展状况的全貌。本章里，我们打算取出水晶球，看看事情将如何发展。首先，我们关注的是目前正在行而即将完成的标准。之后，我们将采取较长远的观点，试着勾勒出无线局域网络的发展方向。

26.1 标准化过程

802.11 标准的出版，不过是整个无线局域网络标准化过程的开端。为了让标准得以出炉，事实上做了不少妥协，有些工作只是留待未来解决。802.11 s 作小组的过程完全对外公开，任人均可造访该小组的网站

<http://grouper.ieee.org/groups/802/11/>，以得知 802.11 修订过程的最新进展。在标准发展的过程中，任务小组会在网站上发表更详尽的报告，包括各种建议书的票选结果。

标准的修订系由任务小组(Task Groups)负责。任务小组以英文字母来划分，任何标准修订的结果则沿用相应任务小组的英文字母代号。例如，OFDM PHY 标准是由任务小组 A (TGa) 负责，其所修订的标准就称为 802.11a。

本书第一版问世之后，陆续有几份标准的修订通过审核。54 这个数字随着 802.11g 产品行销到世界各地。802.11h 修改了 802.11a 所使用的底层技术，使之适用于欧洲，同时说服美国政府在「全球一致频段」(worldwide harmonized band) 开放新的频谱。目前，802.11i 已经大幅平息使用者对于安全性的疑虑，并且用 AES 加密技术加以取代。

26.1.1 新的标准

目前有几份标准特别值得注意。802.11 依然是新技术开发的沃土。未来，任务小组将必须以两个英文字母命名，由此即可看出 802.11 技术已臻成熟。

26.1.1.1 任务小组 E：服务质量

比起有线网络，无线网络的频宽相对有限。任务小组 E 正着手开发，通过多组伫列过程与保留介质使用权等方式来提供服务品质 (quality of service，简称 QOS) 的相关标准。为了进一步提升服务品质，802.11e 将会定义一种新的协调功能，称为混合式协调功能 (hybrid coordination function，简称 HCF)，以及新的网络访问方式。此外，任务小组 E 也定义出所谓「区块回应协议」(block acknowledgment protocol)，目的是减少容易造成网络负担的零星过程。

802.11e 已经耗费了很长一段开发时间。(原本 802.11e 同时涵盖 QOS 与安全性，后来安全性转由任务小组 I 负责，如今 802.11i 业已完成。) 由于标准久久无法定案，业界于是从目前的草案中挑选出部分功能，好让实现上有个过渡性的依据，亦即所谓的 Wi-Fi 多介质标准 (Wi-Fi Multi-Media，简称 WMM。请参考 <http://www.wi-fi.org/penSection/wmm.asp>)。WMM 之于 802.11e，就好比 WPA 之于 802.11i，两者均属标准制定过程的阶段性成果 (snapshots)。

26.1.1.2 任务小组 K：无线电波资源

移动电话网络广泛使用电波量测技术，让无线电波的频宽效能得以被优化。有些 802.11 产品已经开始尝试监控信号品质，不过目前并没有所谓的标准做法。任务小组 K 正着手开发一项供 802.11 使用的标准，让基站能够搜集信号的相关统计数据，据此决策出较明智的过程方式。其所定义的量测方式，允许 802.11 工作站搜集诸如噪音分布（noise distribution）。隐藏工作站（节点）数目，以及特定过程频道负载等相关信息。

26.1.1.3 任务小组 N：高速（100+ Mbps）MIM. 物理层

TGn 原本收到四份完整的建议书。不过剔除其中两份之后，只剩下本书第 15 章所提到的两项提案。经标准委员会投票表决，TgnSync 的支持度稍微领 WiSE. 由于两者差异颇大，可见在最后标准底定之前，尚会面临一番激战。

根据 TGn 建议书所开发的产品，其实不能宣称该产品符合「802.11n 草案」（draft 802.11）因为所谓的「官方标准草案」根本尚未出炉。更何况，在本书付印之际，也不见得已经决定采用哪份建议书。号称 pre-N 的产品，须冒被撤销 Wi-Fi 认证的风险。因此，有些根据特定建议书所开发的产品遂自称为 MTMO.

26.1.1.4 未来标准

任务小组 P 正着手开发车用 802.11 标准，称为「车用环境无线访问」（Wireless Access in Vehicular Environments，简称 WAVE）。汽车的行进速度较快，需要补强“换手”（handoff）方面的功能。其中亦包含对等式（peer-to-peer）功能，可以在车辆间建构网状（mesh）网络。和其它形式的 802.11 网络不同。未来它可能会使用需要使用执照的频谱。802.11p 原本设计来作为搜集与下载安全信息的一种标准方式，不过有人认为它最终会取代蜂窝式通讯（cellular communications）。

任务小组 R 正着手开发漫游协议（roaming protocols）。802.11i 的事先认证（pre authentication）有其限制，因为它无法减轻漫游的运算负荷。TGr 所定义的协定，主要是通过网络传递密钥素材来避免上述缺点。在 2005 年元月所举行的会议中已经剔除一些建议书，往最后标准的路途迈出重要的一步。

任务小组 S 负责开岭网状网络（mesh networking）标准，主要用在“多中介站”（multi-hop）环境。目前尚处于起步阶段。

任务小组 U 负责修改 802.11，使之能与其它网络技术互通。它的目标与 802.21 工作小组类似。TGn 针对 802.11 做了必要的修改，以便与第三代移动电话等网络技术互通，至于 802.21 则负责开发一种可以兼容所有网络技术的独立架构。

26.1.1.5 相关标准

802.1X 原本是针对有线网络而设计的，不过应用在无线网络时，却一直受限于某些临时性的标准。本质上，这些过渡性的标准只能算是实现上的协议，如何将访问控制整合到无线网络，实际上还是一团混乱。802.1X-200 制定出了新版的 EAPOL，同时厘清了两种状态机（state machine）的过程方式。目前它并未获得广泛采用，不过可以确定的是，市场上应该很快就会推出相关产品。

随着更多使用者采用不同的无线技术，由于这些技术各自拥有覆盖范围和距离上的利基，于是开始浮现这些网络之间的换手问题杂（inter-network handoff）。例如，有些行动玩家在“热点”（hot spots）使用 802.11 网络，在车上则使用移动电话网络传递数据。如何能够在两种截然不同的网络间即时切换，乃是 802.21 工作小组的焦点所在。

26.2 无线网络的当前趋势

长远来看，无线网络的发展将会呈现何种面貌？在家用市场，802.11 几乎已经逐退其它对手（例如 HomeRF），也巩固它在短距离数据访问的地位。不过就长期而言，移动性与安全性方面的议题还是比较重要，虽然两者尚有一些不易解决的问题。然而，在安全性方面，目前已经从纯粹防御性的封闭模型，转为拥抱弹性的无线网络，同时快速导入应用。

26.2.1 安全性

安全性向来是无线局域网络的主要议题，不过近来所提出的协议已经平息了许多针对无线网络的抱怨。网络与使用者之间的交互认证，如今可以通过 802.1X 与 EAP 达成。802.11i 为无线局域网络提供了网络管理人员所期盼之坚固。可信赖的加密方案。WPA 则为网络提供了实用上足够的安全性，而业界也允诺设计出符合严格安全标准的协议。

目前网络设计的新趋势，是将无线网络与既有网络整合在一起，而不是将无线网络置于孤立的环境，导致它未能发挥应有功能。无线网络让使用者摆脱空间的限制，进而提高生产力。早期的无线网络在有线与无线网络间设置了访问控制，迫使用户必须学习新的数据访问方式，白白浪费许多应有的生产力。较坚固的安全性协议让使用者得以将网络视为单一整体。使用者访问数据时，可将之视为局域网络，不需要通过麻烦的远端访问程序。

能否改变无线局域网络的安全性模型，绝大部分取决于「使用者身份认证」功能。在使用者账号与网络活动间建立密切的关联性，才有所谓的“可课责性”（accountability），足以消弭各种形式的网络误用。同时，身份认证也让无线局域网络安全不再只是着眼于一般的防堵机制，转而将重点放在类似局域网络所使用的安全模型。

26.2.1.1 身份认证协议

如今，RADIUS 几乎已经成为身份认证的代名词。无线局域网络赋予了 RADIUS 新的生命，不过事实上，RADIUS 是 Internet 之真空管时期的产物。大多数使用者已经不再使用数据机拨接，不过这个原本为拨接用户而设计的协议，如今却成为了局域网络介质（LAN medium）的基础。RADIUS 之所以不适合应用在局域网络的访问（LAN access），是因为加诸其上的种种复杂性。用过市面上 RADIUS 服务器的人都知道，叠层架屋与晦涩难解的配置设置可说是复杂无比。

认证协议本身需要与时俱进，方能跟得上 IP 传输的商品化。无线网络已经驱使大部分组织开放某种程度的网络访问供访客使用。当 IP 传输愈来愈便宜，供给愈来愈容易，使用者就会开始期待能够在更多地方访问更多数据。认证协议需要适应更加开放的环境。使用户能够在任何地方访问网络。特定的服务供应商，如 iPass，已经开始提供类似的服务，打造 Internet2 的研究大学（research universities）【编注】，也开始进行类似的专案。

【编注】研究大学（research universities）系指提供完整学士课程并且能够授予硕士及博士学位的大学。“研究”为学校的发展重心。

要组建所谓的「联盟网络」(**federated networks**)，先决条件是身份认证系统必须具备延伸代理能力(**extensive proxy capability**)，这样网络系统才有办法确认来自不同组织的访客身份。如果未来 Internet 身份认证系统演变成类似 DNS 的功能，可以让组织找到能够验证访客的服务器，不必预先建立信任关系，我也会因此感到惊讶。

26.2.1.2 权限控制

当网络更加开放且容许访客访问，网络安全就具备了一种崭新的含义。确保组织设备安全是项艰巨的任务，但并非没有现成的解决方案。通过平台标准化、随时注意是否需要进行安全性修补。为网络部署防火墙以及随时更新防毒与入侵监测定义档，将可确保一定程度的安全。不过，如果危安因素来自外部的机器，这种“随时保持更新”的安全模型就有可能失灵。虽然公司可以为内部设备提供安全防护软件，访客的机器却只能自求多福。有些新的软件解决方案将网络授权(**network authorization**)的概念加以延伸，亦将访客机器的使用状态涵盖在内。只有被验证为「干净」的机器才可以访问网络。权限控制(**admission control**)是延伸授权的一种方式，不仅考虑到使用者的权限，也包含了使用者运算平台的安全状态。

26.2.1.3 私设设备之监控

如何防范未经授权的无线局域网络部署以控制无线频谱，向来是无线局域网络安全课题的一个主轴。虽然其中牵涉到一堆工程过程，理论上还是和过去没有什么两样。基本做法除了监控无线频谱，检测是否出现不该有的 AP，如有必要，还可以采取适当的步骤予以关闭。近年来，这项工作进一步扩及监控内部网络是否遭人盗用，有时也及于用户端设备。

如果发现身份不明的设备，首先必须加以分析，决定威胁的程度。连接到其它骨干的无线网络不致构成威胁，不太可能成为攻击的目标。如果和其它公司共享办公室，信号必然会泄露到邻近区域。攻击别人的网络不仅会破坏彼此关系，也有可能触犯电脑犯罪法(**computer crime laws**)。为了提供网络安全，必须将各种威胁加以分级。没有连接至贵公司网络的免照无线设备，不在你的监督与安全性控管范围，必须排除在外。访客或其它人所使用的 Ad-hoc 网络也不该予以干涉。只要受到适当保护，连结到贵公司网络的基站也可以排除在外。

和其它领域没什么两样，巩固网络安全是每日的基本功课。检测与评估私设基站的功能，已经逐渐内建到无线基础建设当中。虽然有些公司开始使用额外的设备来提供监测效能与安全服务，大多数网络部署实际上已经整合进所需要的基本功能。

26.2.2 网络部署与管理

无线局域网络一直依循之前两种创新的典范。个人电脑与局域网络的发展，一开始都不在 IT 人员的雷达检测范围(**under-the-radar**)。不过，这两种技术最后都演变成通过中央控管的服务，提供网管人员不少信息。无线局域网络已经脱离这段远离雷达检测范围的阶段，迅速成为标准的连接方式。

如今，网络部署的主要挑战，在于如何超越简单的覆盖模型(**coverage model**)。早期的无线网络在设计上只是为了涵盖特定区域。不过随着用量的增加，定点覆盖已经不敷使用。如何确保较高的频宽乃是协议开发与部署的首要课题，特别是针对使用者已经习惯宽带有线网络的地区。

26.2.2.1 网络规划

传统的 802.11 网络规划是件吃力不讨好的事，不但要到处走透透，也得手动量测一堆数据。和其它技术创新一样，当人们更了解底层机制，就会开列出一些工具来改善规划程序。这些工具相当于将无线电专长外包出去（**outsourcing**），毕竟大多数网管人员都不是无线专家。

其中一类工具将会藉助楼板规划（**floor plans**）以及建筑知识（**architectural knowledge**），计算出需要多少基站及其摆设位置。另外一些工具则是使用动态电波校正，好让网络适用于该环境。有些产品同时采用两者。不论如何，过去昂贵费时的实地探勘（**site survey**）已经没有必要。实地探勘不仅是劳力密集，价格也过于昂贵。

就像以往设计师必须学习如何将网络布线整合到建筑规划，他们也得学习如何将 802.11 整合到设计程序。如同以往，尽早确定需求绝对有帮助。对于需求有了初步的概念后，就可藉助工具计算出初步的 AP 摆设位置。将取得的信息回给建筑师与室内设计师后，建筑的规划就可以提升网络效能，同时也将麻烦降至最低。如果 AP 摆设位置纯粹迁就美感诉求或安装的容易度，网络的覆盖范围就相当堪虑。

不过并非经过规划之后，整个程序就此结束。由于计算出来的模型不见得完美，可以想见后续还得变更原始设计。组建无线局域网络时，通常必须经过好几个回合的反复测试与优化。幸好，随着基站价格的滑落，如今已经不必斤斤计较可以省掉几部基站。

规划出实体架构后，接着必须厘清打算采用何种逻辑网络架构。随着无线网络逐渐普及，无间隙的移动性就成为了众所期盼的重点。无间隙移动性的需求通常与机构大小无关。如果建筑物相当庞大，规划起来可是饶富趣味的挑战。

26.2.2.2 后端骨干

互通实验室（**Interpol Labs**）有一则流传已久的话，内容是说・有些无线局域网络新手需要大量的 Ethernet 网线与电源线，以便供电以及连接所有基站。事实上，无线网络所使用的缆线比起其它技术丝毫不遑多让。截至目前，无线网络还是依靠后端的布线来提供网络连接与供电。

一般而言，布置网线要比电源线简单，理由如下。为了简便，基站通常只用一条线同时连网与供电。不过，有时候情况并不允许。例如在较大的会场里，天花板布有电源线供照明之用，但却没有网线。因此有些公司着手研究如何以无线网络为骨干，不必为了无线局域网络再去设备网线。双模基站（**dual-radio access point**）可以使用其中一种信号提供服务，另一种信号做为上链（**uplink**），电源线仅用来供电。网状骨干技术在一些布线困难的环境中特别有用。在超过 100 公尺 Ethernet 网线派不上用场的情况下，这可能是惟一的解决方案。

26.2.2.3 迷你「管制当局」与仲裁者

使用 802.11 很容易爆发频谱方面的争议，特别是 802.11b 与 802.11g 所使用的 2.4GHz 频段已经拥塞不堪。频谱免照意味所有人均可使用，没有所谓先占先赢的事情。2002 年末，T-Mobile 在 Portland 的「个人电信公司」（**Personal Telco**）【编注】的地盘上装设新的基站。由于两家的基站使用相同的过程频道，造成彼此互相干扰。既然技术上无法解决干扰问题，双方遂互相提出诉讼。

【编注】

这是无线网络的自愿型或社区型应用。拥有宽带上网线路的电脑用户，利用某种系统来建立无线网络，让一定范围内有上网需求的任何人通过他们的宽带网络上网，而不必向宽带运营商

申请宽带上网。这种宽带上网服务是免费提供或以比个人宽带费用低很多的价格来提供。在美国供类似服务的有 bay Area Wireless Group, Seattle Wireless , Portland's Personal Telco Pro, NYGWireless.:Net 以及 Boston's Guerilla Net 。

虽然 Portland 事件是最早曝光的频谱之争，可以想见往后还是会陆续发生更具争议的问题。有些机构试图以特定方式控制无线频谱。小型办公室林立的建筑物，可能会使用单一无线局域网络，搭配多个虚拟无线网络。有些机场只允许单一实体无线网络，然后将频宽出租给旅客、航空公司与商店。由于不少的协议内容已经侵犯到电磁频谱的管辖权，因此 FCC 宣告这些协议均属无效，除了某些少数的特例。【注 1】

无线电波自动微调技术(automatic radio tuning technology)只能算是部分的解决方案。既然频道有限，有时候就不可能将干扰排除至最佳状况。（打造远距 802.11 网络的热潮使得问题更加严重。如此一来有更多 802.11 信号会被传至壅塞地区。）有时候，技术达人(*technically competent individual*)可以协助解决使用者间的争端。有些高科技社区已经出现类似问题，亦即左邻右舍均使用相同频道。有些自愿之士已经在邻居间成立频率配置委员会（*frequency allocation committee*），协调四周邻居所使用的频道以便改善效能。【注 2】既然不具法律公权力，这些仲裁者或管制者其实并没有法律强制权力所依靠的只是技术上的权威。

【注 1】详见 FCC 于 2004 年 6 月所发布的文件 DA-04-1844A1(网址位于 <http://hraunfoss.fcc.gov/edocs-public/attachmatch/DA-04-1844A1.pdf>)中，这段文字“重申”(reaffirm)不论立场为何，惟独 FCC 有权裁决免照设备的无线频率干扰(RFI)争议。……[以及]……消费者安装与操作客制化天线时必须遵循 FCC 法规这些规定适晨于免照器材的使用，例如 Wi-Fi 基站。

【注 2】

详见 Associated Press 以下的报导 <http://community.bouldernews.com/business/02bwire.html>。

26.2.2.4 访客访问

不过更重要的是，未来将会需要各种不同的访问控管方式。许多早期的无线局域网络只是附属于公司网络。现有的身份认证概念是针对已知。静态的使用群组（如公司员工）而设计的。为员工提供网络访问服务是项重大的任务，不过这只是冰山一角。就像移动电话，无线网络当初的承诺是，不论多么偏远，不论使用者身在何处，均能够随时连接。

公共空间（如机场或车站）的 802.1<Z 网络设计，必须将「允许谁使用网络：以及“这些人享有什么种权力”等相关问题纳入考虑。网络服务必须经过身份认证，同时必须保护使用者彼此间的安全。要提供牢靠的服务给不同的使用群组，同时群组间必须彼此独立，需要在网络架构上加以思考。

高等教育机构就不断在测试访客访问的底线。研究小组通常跨越多个研究机构，学者也常常在不同地方进行访问。有个专案计划打算建构一个「联盟」(federation)，让加入联盟的机构用户也可以使用其它成员的网络，不必在各个机构分别申请账号。这项计划的挑战涵盖纯技术性的议题，技术与程序之间的调校，以及纯政策上的议题。在技术层面上，各成员间必须建立某种形式的信赖身份认证链路(trusted authentication link)。【注 1】虽然有其限制，这些联盟仍习于使用 RADIUS。

然而，就算用户交由自家机构进行身份认证，还是必须将此用户与参访网络内部人员区隔开来。为了提供可课责性，该用户的身份数据必须传给参访机构。受参访网络的管理人员所要求的可能不只是用户姓名而已。如果某个访客染上蠕虫或病毒，就必须将该访客的电脑隔离，通知该用户手动加以清除。不过如果访客来自远方，可能无法联系该访客的在藉机构以取得联系。举例而言，在身份认证程序中，主动提供移动电话号码就可以协助管理人员。不过，主动提供特定信息同时兼顾隐私，本来就是目前身份认证协议所面临的主要技术挑战。【注 2】

【注 1】

EduRoam 泌即 alwww eduroamb 曙）即属此类专案。其它地区也有类似专案正在进行。

【注 2】

正因为缺乏适用的商业解决方案、因此 Internet2 联盟着手开发了一套称为 Shibboleth(<http://shibboleth. irate aet..edu>)的软件系统。

26.2.3 应用程序

无线网络的首要应用乃是自由一免于有线的自由以及免于没有网络可用的自由。使用者可以四处移动，网络插座可不然。第一代的应用采用虚拟的 Ethernet，这让许多应用程序无须更动即可使用。当应用程序开发人员逐渐累积经验，就会开始在应用程序中暂存一些数据，也知道网络连接可能转瞬即逝。

无线网络在促进公用运算(utility computing)方面也扮演重要的推手。既然各种应用就挂在线路上，就需要更普遍的网络访问方式。通过身份认证方式的改良，以及运算设备的无线局域网络接口，网络本身就成为这些应用的中介。较佳的身份认证系统也有助于驱使各式应用采行单一登入机制(single-sign-on)。

26.2.3.1 定位

早期无线网络的应用通常只是移植自有线网络。新式应用则是运用到比较多的位置信息。会议通常是在较大型的建筑物中进行，为了引导与会人员，通常花费不少投资在标示牌上。目前，有些会场已经开始以无线网络来提供位置信息，可以让与会人员自订路径，同时也提供“最近场所”(what's near me)的预览应用。IBM Research 开发出一套办公室系统，可以追踪人员以及更新所在位置信息。【注】（还好，未来定位相关发明可以比较不那么“老大哥”）

26.2.3.2 语音

期待多年之后，网络语音（voice over IP）的时代终于来临。有些服务供应商现在已经能够在 DSL 上，提供比移动电话更好的语音品质。经过多年的抗拒，如今消费者开始拥抱这种科技，虽然通话品质说不上顶尖，但是较有弹性。

802.11 是下一代无线电话(cordless phone)通讯协议的强势竞争者。目前，打算同时使用无线电话与 802.11 网络的使用者请注意，无线电话必须使用不同的频段（有时候可以趁清仓大拍卖或者到 eBay 上看看还有没有旧式的 900 MHz 无线电话！），不然就得祈盼买来的无线电话能与 802.11 和平共存。利用 VOIP，无线电话可以分享相同网络，如此一来就可不需担心上述问题。未来消费性电子产品如果搭配 802.11，将会进一步降低芯片成本，带来良性循环。

在我看来，802.11 VoIP 手机缺少身份认证功能的缺点很快就可以得到解决。到目前为止，大多数手机除了过滤 MAC 外，都还没有什么安全功能。802AX 身份认证搭配 EAP 加密模式是

最起码的安全性要求。如果话机采用会话始协议：（Session Initiation Protocol，简称 SIP），就可以在具备 802AX 能力的 hot spot 使用。电信业者可以在通话密集的区域组建较便宜的 802.11 网络来分担移动电话的话务，不用另外购置昂贵的移动电话设备。不过，要在两种截然不同的基础设施之间切换话务，显然没有那么简单。

26.2.3.3 资料广播

无线网络本质上属于广播介质。和 Ethernet 一样，工作站会接收到往来于 802.11 网络的所有帧，帧过滤规则于此同样适用。Ethernet 与 802.11 的主要差异，在于无线电波（radio）很难与交换(switching)类比。802.11 帧会传递到四面八方，无法像雷射一样聚焦，将数据传递给特定接收对象。多播帧可以用来提供一些特殊应用，提供数据广播给某个群组。只要有适当可靠的协议，就可以赋予无线局域网络小规模的广播能力。就像有些电视台利用数位电视的闲置频宽来传送数据，无线局域网络也可以成为短距离的影像广播机制。有些消费性电子厂商已经开始参与 802.11 标准的制定，因此通过 802.11 进行影像传输并非全然遥不可及。

【注】

这就是与办公家具制造商 Steelcase 合作开发的 cubicle 专案，详见 <http://www.research.ibm.com/bluespace/>

26.2.4 协议架构

用户端拥有太多权限是 802.11 常见的议题。在 802.11 中，所有工作站可说是“生而平等”。假设有 19 个用户连接到基站，而基站却只负责 5% 的协议处里事宜。基本上，要求网络基础设施负责 50% 的协议处理事宜并不为过。后续成立的任务小组已经朝这个方向进行，使控制权更加集中。希望在漫游，换手与服务品质方面能有所改进。

26.2.4.1 联盟与移动性

从协议架构的角度来看，联盟（federation）与移动性（mobility）密不可分，因为两者相关“网络分享或设备在管辖权不同之网络间的可携性”。借用移动电话的术语，这些概念开始导致数据层面（负责传递数据）与控制层面（负责提供身份认证与权限管理，以及为数据层面设置网络）之间的分工。

当欧洲电信专家撰写第二代“蜂窝式行动网络”（cellular network）相关标准时，显然没有任何一家电信业者有足够的资源，可以组建一整个“泛欧蜂窝式行动网络”（pan-European cellular network）。无线电话的发展，起初受限于缺乏一种可以涵盖欧洲所有区域的共通标准。这些专家了解，移动电话的价值与其可使用的范围成正比。因此，当 GSM 标准最后被采用时，特别强调漫游功能，允许用户使用不同的网络，而由单一电信业者收费。

当 802.11 的使用率逐渐成长，身份认证与跨网络漫游标准就愈加重要。3G 执照惊人的成本已经迫使一些电信业者面临破产边缘。为了找寻出路，有些电信业者已经计划共同分担基础建设，以便分摊昂贵的 3G 网络组建成本与风险。许多 802.11 热点服务供应商同样面临类似的处境，共组联盟之后，就可以让使用者访问其它业者的网络。

当类似情况变得更为普遍，结盟的效果就会超越服务供应商的层次，进而涵盖策略联跟公司以及研究机构。由于 RADIUS 不敷使用（does not scale），或是无法提供必要的功能，因此必须另外开发用来辨识与管理访客的相关协议。

随着 802.11 逐渐普及，熟悉其它网络技术的组织所具备的优势就更加明显。受到便宜，频谱免照的吸引，许多电话公司已经开始筹组自己的供应商体系，以提供 802.11 服务。现有的电话公司则是利用 802.11 网络来推销 V'AN 宽带业务·移动电话业者也开始利用 802.11 作为延伸行动通讯网络便宜的替代方案。目前这项服务已经推出，也发表了几款 802.11136 双模手机。802.11 与广域技术的结合其实自然不过，毕竟它可以在通话密集之地提供充足便宜的频宽，将长途网络留给更适合的技术服务。

允许快速移动同时又能降低网络负担，是许多标准制定小组的目标。虽然 802.11 i 事先身份认证协议可以大幅缩减切换基站所需要的时间，但是并不能减轻网络处理所必须的负担。要产生对私钥(pairwise master key)，还是需要进行完整的 802.1X 身份认证。因此，对 RADIUS 服务器而言负担并没有改变，何况跨广域网络 (WAN) 的事先身份认证，可能必须得到千里之外的回应。要提供网际网络规模 (Internet-scale) 的移动性，能够在网络间传递（而不是等到每次基站进行换手才取得）密钥，就变得十分重要，这些协议是由任务小组 R 开发。

26.2.4.2 未来的协议

虽然无线网络具有相当大的弹性，却也因此造成管理上不小的负担。要能自动搜寻网络具备何种能力，就不能局限于低价的无线参数，如此网络方能发布身份认证进行的方式。

以往，基站的功能受限于底层的硬件。新式的电波产品比较侧重软件功能，甚至基站本身也更加软件导向。当基站功能逐渐倾向完全由软件定义，市场就进一步区隔为高价与低价两个等级·低价产品大概就是将公版 (reference design) 稍作修改随即大量生产，至于高价产品，则是在其参考设计 (reference design) 上执行高度客制化的软件。

为了让 AP 成为执行 802.11 程序码的执行平台，IETF 已经成立一个工作小组，负责开发「无线基站控制与供应」(Control and Provisioning of Wireless Access

Points，简称 CAPWAP)协议。【注】CAPWAP 已经在 RFC 3990 提出问题陈述 (problem statement)，目前处于网络架构与目标的定义阶段，主要是针对使用「轻量级基站：(lightweight access points) 的网络。基站控制协议可望在 2006 年元月出炉。当基站逐渐商品化，或许架构在 Linux 之上的基站只要通过韧体更新，就可以使用标准的通隧协议 (tunneling protocol)。此外，若是有人为了让开放源码基站能够使用新的控制芯片，而着手开岭新的韧体，我也不感到惊讶。

26.3 结语

如今，Wi-Fi 的蔓延已经势不可挡。自从本书第一版发行以来，无线网络已经从一种有趣的玩意，变成不可或缺的技术。许多公司用它来提高生产力以及吸引员工，就像有些大学利用它来吸引学生。随着芯片与网卡的成本滑落，让用户均负担得起使用无线网络的笔记型电脑。

网线依然会继续留在最适当的工作岗位。无法移动的固定运算资源以及频宽需求较高的网络依然受制于网线。不过，无线网络似乎泰然自若地往连接标准 (standard method of network connection) 的目标迈进。未来，“你们有 Wi-Fi 吗？”“将会取代”网络孔在哪“成为连网时的标准问题。

【注】

此工作小组的首页是 <http://www.ietf.org/html.charters/capwap-charter.html>