

9160 G2

无线网关

用户手册

2009 年 11 月 2 日 P/N 8000349.A



通过 ISO 9001 认证的
质量管理体系



© 版权所有 2009 by Psion Teklogix Inc.

2100 Meadowvale Boulevard, Mississauga, Ontario, Canada L5N 7J9

<http://www.psionteklogix.com>

本文档及其包含的信息均为 Psion Teklogix Inc. 的财产，其发布严格保密，不得全部或部分再现或复制，但以推动 Psion Teklogix 制造产品及提供服务的销售为唯一目的时除外。此外，本文档不得用作设计、制造或分包的基础，也不得以任何方式损害 Psion Teklogix Inc 的利益。

免责声明

我们尽一切努力确保本材料是完整、准确和最新的。此外，会定期添加更改；这些更改将纳入新版本的出版物中。

Psion Teklogix Inc. 保留对本文档中所述的产品和/或程序进行改进和/或更改的权利，且无需另行通知；并且对于因材料依赖性（包括但不限于排版错误）而导致的任何损坏，包括但不限于间接损害，Psion Teklogix Inc. 概不负责。

Windows® 和 Windows 徽标是 Microsoft Corporation 在美国和/或其它国家（地区）的商标或注册商标。

所有商标和商标名称均为其各自所有者的财产。

返厂保修

根据 www.psionteklogix.com/warranty 提供的有限保修及责任限制声明，Psion Teklogix 为本产品提供为期十二 (12) 个月的返厂保修服务。

为 Psion Teklogix 制造的设备提供的保修服务不延伸至经过非授权的 Psion Teklogix 维修部门员工的任何人篡改、修改或维修的任何产品。请参阅 Psion Teklogix 销售条款及条件了解完整详情。



重要说明：*Psion Teklogix 的担保自发货之日起生效。*

服务和信息

Psion Teklogix 向全球范围内的客户提供一整套产品支持服务和信息。这些服务包括技术支持和产品维修。要查找您所在地区的支持服务，请转至

www.psionteklogix.com/service-and-support.htm

要访问当前和停产产品的更多信息，请访问 <https://teknet.psionteklogix.com>，然后登录或点击 “Not Registered?”（未注册？），具体取决于您之前是否注册过 Teknet。在线提供了一部分存档产品信息。



废弃电子电气设备 (WEEE) 指令 2002/96/EC

本产品及其配件符合废弃电子电气设备 (WEEE) 指令 2002/96/EC 的要求。如果寿命到期的 Psion Teklogix 产品或配件贴有如上所示的标签，请联系当地代表，解有关如何进行回收的详情。

有关国际子公司的列表，请访问：

www.psionteklogix.com/EnvironmentalCompliance

危害性物质限制 (RoHS) 指令 2002/95/EC

什么是 RoHS ?

欧盟规定，对于在欧洲出售的电子和电气产品，其设计和制造应符合较高的环境标准，以减少有害物质进入环境。“危害性物质限制 (RoHS) 指令”规了产品中可能包含的铅、镉、汞、六价铬以及阻燃剂 PBB 和 PBDE 的最高跟踪等级。2006 年 7 月 1 日起，只有符合上述高环境标准的产品才能“进入欧成员国市场”。



RoHS 徽标

尽管并没有法律要求对符合 RoHS 的产品进行标记，但 Psion Teklogix Inc. 会按如下所述指示其产品符合该指令：

RoHS 徽标位于产品背面或电池盒（或相关配件，例如充电器或充电坞站）内的电池下方，表示该产品符合欧盟指令 RoHS。除如下所示外，未贴有 RoHS 徽标的 Psion Teklogix 产品表示其在 2006 年 7 月 1 日前已进入欧盟市场，因此免于遵守该指令。



注释： 由于物理空间限制或豁免状态，因此并非所有配件或外围设备都贴有 RoHS 徽标。

目录

认证和安全摘要	xiii
---------------	------

第 1 章：简介

1.1 关于本手册	3
1.2 联机帮助功能、支持的浏览器和限制	5
1.3 文本转换	6
1.4 9160 G2 无线网关概述	7
1.4.1 射频	7
1.4.2 接入点的功能	8
1.4.3 基站的功能	9
1.4.4 微型控制器的功能	9
1.5 功能和优点	9
1.5.1 IEEE 标准支持和 Wi-Fi 兼容性	9
1.5.2 无线功能	9
1.5.2.1 Psion Teklogix 802.IQ 协议	10
1.5.3 安全功能	11
1.5.4 开箱即用的访客接口	11
1.5.5 形成集群和自动管理	12
1.5.6 网络	12
1.5.7 SNMP 支持	12
1.5.8 可维护性	13
1.6 接下来该做什么呢？	13

第 2 章：安装要求

2.1 选择合适的安装位置	17
2.1.1 环境	17
2.1.2 维护	18
2.1.3 射频	18

2.1.4	电源线和天线	18
2.1.4.1	电源	18
2.1.4.2	天线	18
2.2	连接至外部设备	19
2.2.1	端口	20
2.2.2	LAN 的安装：概述	20
2.2.3	LAN 安装：以太网	20
2.2.3.1	以太网布线	21
2.2.3.2	100Base-FX 光纤以太网端口	21
2.2.4	状态指示灯 (LED)	21
2.2.5	连接视频显示终端	22
2.3	使用 Web 浏览器更改配置	22

第 3 章：启动前检查清单

3.1	产品名称	25
3.1.1	产品名称的默认设置	25
3.1.2	接入点不提供哪些功能	28
3.2	管理员的计算机	28
3.3	无线客户端计算机	29
3.4	了解产品名称上的动态和静态 IP 寻址	30
3.4.1	启动时接入点如何获取 IP 地址？	30
3.4.2	动态 IP 寻址	31
3.4.3	静态 IP 寻址	31
3.4.4	恢复 IP 地址	31

第 4 章：设置和启动的快速步骤

4.1	拆开 9160 G2 无线网关的包装	35
4.1.1	9160 G2 无线网关的硬件和端口	35
4.1.2	9160 G2 无线网关里面都有些什么？	35
4.2	将接入点连接到网络和电源	36
4.2.1	设置访客网络连接时的注意事项	38
4.2.1.1	访客 VLAN 的硬件连接	38
4.3	打开接入点的电源	38
4.4	登录到管理 Web 页面	38
4.4.1	查看接入点的基本设置	39

4.5	配置基本设置并启动无线网络.....	40
4.5.1	默认配置	40
4.6	接下来该做什么呢?	40
4.6.1	确保接入点已连接到 LAN.....	40
4.6.2	使用无线客户端测试 LAN 的连接性.....	41
4.6.3	使用高级功能保证接入点的安全并进行微调.....	41

第 5 章：配置基本设置

5.1	导航至基本设置	45
5.2	查看/描述接入点	46
5.3	提供网络设置.....	47
5.4	更新基本设置.....	48
5.5	独立接入点的基本设置	48
5.6	网络概览：了解指示器图标	48
5.7	查看显示不同颜色和样式的用户界面	48

第 6 章：管理接入点和集群

6.1	概述.....	53
6.2	导航至接入点管理	53
6.3	了解集群.....	53
6.3.1	什么是集群?	53
6.3.2	一个集群支持多少个 AP?	54
6.3.3	什么类型的 AP 可以形成一个集群?	54
6.3.4	协调 AP 与其他集群成员之间是什么关系?	54
6.3.5	哪些设置可以/不可以作为集群配置的组成部分进行共享?	54
6.3.5.1	在集群配置中共享的设置	55
6.3.5.2	集群不共享的设置	55
6.3.6	集群的形成.....	56
6.3.7	集群大小和成员资格	56
6.3.8	Intra-Cluster 安全	56
6.4	了解接入点设置.....	56
6.4.1	修改位置描述	58
6.4.2	设置集群名称	58
6.5	开始形成集群.....	58
6.6	停止形成集群.....	58

6.7	特定 AP 和管理独立 AP 的配置信息	59
6.7.1	在 URL 中使用 AP 的 IP 地址导航至 AP	59
6.8	会话监控	59
6.8.1	导航至会话监控	60
6.8.2	了解会话监控信息	60
6.8.3	查看接入点的会话信息	62
6.8.4	对会话信息进行排序	62
6.8.5	刷新会话信息	62

第 7 章: 管理用户帐户

7.1	概述	65
7.2	导航至用户管理	65
7.2.1	查看用户帐户	66
7.2.2	添加用户	67
7.2.3	编辑用户帐户	68
7.2.4	启用和禁用用户帐户	68
7.2.5	启用用户帐户	68
7.2.6	禁用用户帐户	68
7.2.7	删除用户帐户	69
7.3	备份和还原用户数据库	69
7.3.1	备份用户数据库	69
7.3.2	从备份文件还原用户数据库	69

第 8 章: 信道管理

8.1	导航至信道管理	73
8.2	了解信道管理	73
8.2.1	工作原理概述	73
8.2.2	了解有关重叠信道的更多信息	74
8.2.3	示例: 信道管理前后的网络	74
8.3	配置和查看信道管理设置	75
8.3.1	停止/启动自动信道分配	76
8.3.2	查看当前的信道分配和设置锁定	76
8.3.2.1	更新当前信道设置 (手动)	77
8.3.3	查看上次建议的信道组更改	77

8.3.4	配置高级设置（自定义/安排信道计划）	77
8.3.4.1	更新高级设置	79
第 9 章：无线邻居		
9.1	导航至无线邻居	83
9.2	了解无线邻居的信息	84
9.3	查看无线邻居	84
9.4	查看集群成员的详细信息	86
第 10 章：配置安全性		
10.1	了解无线网络的安全问题	91
10.1.1	如何知道使用的是哪一种安全模式？	91
10.1.2	比较安全模式的密钥管理、身份验证及加密算法	92
10.1.2.1	何时使用未加密（无安全性）	92
10.1.2.2	何时使用静态 WEP	93
10.1.2.3	何时使用 IEEE 802.1x	94
10.1.2.4	何时使用 WPA 个人版	95
10.1.2.5	何时使用 WPA 企业版	96
10.1.3	是否禁止了广播 SSID 增强安全性？	97
10.1.4	如何通过站点隔离保护网络？	97
10.2	配置安全设置	98
10.2.1	广播 SSID、站点隔离和安全模式	98
10.2.2	安全模式	100
10.2.2.1	None (Plain-text)（无（纯文本））	100
10.2.2.2	Static WEP（静态 WEP）	101
10.2.2.3	IEEE 802.1x	106
10.2.2.4	WPA Personal（WPA 个人版）	109
10.2.2.5	WPA Enterprise（WPA 企业版）	112
10.3	更新设置	116
第 11 章：维护和监控		
11.1	接口	119
11.1.1	以太网（有线）设置	120
11.1.2	无线设置	120
11.2	事件日志	120

11.2.1	启用或禁用持久性	121
11.2.2	严重程度	121
11.2.3	深度	122
11.2.4	用于内核消息的日志中继主机	122
11.2.4.1	了解远程记录	122
11.2.4.2	设置日志中继主机	123
11.2.4.3	在状态、事件页面上启用/禁用日志中继主机	124
11.2.5	事件日志	124
11.3	发射/接收统计数据	125
11.4	关联的无线客户端	127
11.4.1	链路完整性监控	127
11.5	相邻接入点	128

第 12 章：以太网（有线）接口

12.1	导航至以太网（有线）设置	135
12.1.1	DNS 主机名	136
12.1.2	访客接入	136
12.1.2.1	配置内部 LAN 和访客网络	136
12.1.2.2	启用或禁用访客接入	137
12.1.2.3	指定虚拟访客网络	137
12.1.3	虚拟无线网络	138
12.1.4	内部接口设置	138
12.1.5	访客接口设置	141
12.1.6	更新设置	141

第 13 章：设置无线接口

13.1	导航至无线设置	145
13.2	配置 802.11d 监管域支持	146
13.3	802.11h 监管域控制	146
13.4	配置射频接口	147
13.5	配置“内部”无线 LAN 设置	149
13.6	配置“访客”网络无线设置	149
13.7	更新无线设置	150

第 14 章：设置访客接入

14.1 了解访客接口.....	153
14.2 配置访客接口.....	153
14.2.1 在虚拟 LAN 上配置访客网络	154
14.2.2 配置欢迎屏幕（强制网络门户）.....	154
14.3 将访客网络用作客户端	155
14.4 部署示例.....	156

第 15 章：配置 VLAN

15.1 导航至虚拟无线网络设置.....	159
15.2 配置 VLAN	160
15.3 更新设置.....	161

第 16 章：配置 802.11 射频设置

16.1 了解无线通信设置	165
16.2 导航至无线通信设置.....	165
16.3 配置无线通信设置	167
16.4 更新设置.....	171

第 17 章：MAC 地址过滤

17.1 导航至 MAC 过滤设置	175
17.2 使用 MAC 过滤.....	176
17.3 更新设置.....	176

第 18 章：负载均衡

18.1 了解负载均衡.....	179
18.1.1 识别不平衡：使用过度或使用过少的接入点.....	179
18.1.2 指定利用率和客户端关联的限值.....	179
18.1.3 负载均衡和 QoS.....	179
18.2 导航至负载均衡设置.....	179
18.3 配置负载均衡.....	180
18.4 更新设置.....	181

第 19 章: 服务质量 (QoS)

19.1 了解 QoS.....	185
19.1.1 QoS 和负载平衡.....	185
19.1.2 802.11e 和 WMM 标准支持.....	185
19.1.3 QoS 队列和协调流量的参数.....	186
19.1.3.1 QoS 队列和数据包上的服务类型 (ToS).....	186
19.1.3.2 数据帧的 EDCF 控制和仲裁帧间间隔.....	187
19.1.3.3 随机退避和最小/最大竞争窗口.....	188
19.1.3.4 更佳性能的数据包突发.....	189
19.1.3.5 客户端工作站的传输机会 (TXOP) 间隔.....	189
19.1.4 802.1p 和 DSCP 标记.....	189
19.1.4.1 VLAN 优先级.....	191
19.1.4.2 DSCP 优先级.....	192
19.2 配置 QoS 队列.....	192
19.2.1 配置 AP EDCA 参数.....	194
19.2.2 启用/禁用 Wi-Fi 多媒体.....	196
19.2.3 配置工作站 EDCA 参数.....	196
19.3 更新设置.....	197

第 20 章: 无线分布系统

20.1 了解无线分布系统.....	201
20.1.1 使用 WDS 桥接远距离有线 LAN.....	201
20.1.2 使用 WDS 将网络扩展到有线覆盖区域之外.....	202
20.1.3 使用 WDS 创建备份链路.....	202
20.2 与 WDS 链路相关的安全考虑事项.....	203
20.2.1 了解静态 WEP 数据加密.....	203
20.2.2 了解 WPA (PSK) 数据加密.....	203
20.3 配置 WDS 设置.....	204
20.3.1 配置 WDS 链路的示例.....	206
20.4 更新设置.....	207

第 21 章: 配置 SNMP

21.1 了解 SNMP 设置.....	211
21.2 导航至 SNMP 设置.....	213
21.3 配置 SNMP 设置.....	214
21.3.1 配置 SNMP 陷阱.....	216
21.3.2 更新 SNMP 设置.....	216

第 22 章: 9160 G2 用作基站

22.1 概述.....	219
22.2 无线电协议.....	220
22.2.1 自适应轮询/争用协议.....	220
22.3 窄带菜单.....	220
22.3.1 窄带射频配置设置.....	220
22.3.1.1 RA1001A 射频参数.....	222
22.3.2 Connectivity Options (连接选项).....	223
22.3.3 Connectivity Options (连接选项): Base Station (基站) 模式.....	223
22.3.3.1 Polling Protocol Parameters (轮询协议参数).....	225
22.3.3.2 Radio Parameters (射频参数).....	227
22.3.4 Connectivity Options (连接选项): RRM 模式.....	228
22.4 Connectivity (连接) 菜单.....	228
22.4.1 基站配置设置.....	230
22.4.2 RRM 组配置设置.....	231
22.4.2.1 RRM Groups (RRM 组).....	233
22.4.2.2 Polling Protocol Parameters (轮询协议参数).....	234
22.4.2.3 Radio Parameters (射频参数).....	235
22.4.2.4 Group Parameters (组参数).....	236
22.4.2.5 Remote Radio Modules (远程无线电模块).....	237
22.4.3 无线电链路功能配置设置.....	237
22.4.3.1 Radio Link Features (无线电链路功能).....	239
22.4.3.2 Automatic Radio Address (自动射频地址).....	240
22.4.3.3 Automatic Terminal Number (自动终端号).....	241
22.4.4 Hosts (主机) 菜单.....	242
22.4.4.1 9010 Configuration (9010 配置).....	245

第 23 章: 微型控制器配置

23.1	概述	249
23.2	微型控制器配置菜单	250
23.3	主机菜单	250
23.4	主机菜单选项	253
23.4.1	3274 仿真	254
23.4.1.1	仿真选项	254
23.4.1.2	TESS Options (TESS 选项)	255
23.4.1.3	Telnet Protocol Options (Telnet 协议选项)	265
23.4.1.4	Function Key Mappings (功能键映射)	268
23.4.2	5250 仿真	269
23.4.2.1	Emulation Options (仿真选项)	269
23.4.2.2	TESS Options (TESS 选项)	270
23.4.2.3	Telnet Protocol Options (Telnet 协议选项)	279
23.4.2.4	Function Key Mappings (功能键映射)	283
23.4.3	ANSI 仿真	284
23.4.3.1	仿真选项	284
23.4.3.2	Telnet Protocol Options (Telnet 协议选项)	287
23.4.3.3	Auto-Telnet/Auto-login (自动 Telnet/自动登录)	289
23.4.3.4	Function Key Mappings (功能键映射)	292

第 24 章: 802.IQ 设置

24.1	802.IQ 的功能	295
24.1.1	802.IQ v1/v2 通用功能	295
24.1.2	802.IQ v1 功能	298
24.1.3	802.IQ v2 Features (802.IQ v2 功能) 菜单	299
24.2	更新 802.IQ 设置	299

第 25 章: 网络时间协议服务器

25.1	导航至时间设置	303
25.2	启用或禁用网络时间协议 (NTP) 服务器	304
25.3	更新设置	304

第 26 章：备份和还原配置

26.1 导航至 AP 的配置设置	307
26.2 重置出厂默认配置	308
26.3 将当前配置保存到备份文件	308
26.4 从之前保存的文件还原配置	308
26.5 重启接入点	309
26.6 升级固件	309
26.6.1 更新	310
26.6.2 验证固件升级	311

第 27 章：规格

27.1 外形描述	315
27.2 环境要求	315
27.3 AC 电源要求	315
27.4 以太网供电要求	316
27.5 处理器和内存	316
27.6 网络接口	316
27.7 射频	316

附录 A： 端口引脚分配和接线图

A.1 控制台端口	A-1
A.2 串行电缆描述	A-1
A.3 RJ-45 连接器引脚分配（10BaseT/100BaseT 以太网）	A-3

附录 B： 无线客户端 /RADIUS 服务器上的安全设置

B.1 网络基础设施：在内置或外部身份验证服务器之间进行选择	B-7
B.1.1 使用内置身份验证服务器 (EAP-PEAP)	B-8
B.1.2 使用具有 EAP-TLS 证书或 EAP-PEAP 的外部 RADIUS 服务器	B-8
B.2 确保无线客户端软件是最新的	B-8
B.3 访问 Microsoft Windows 无线客户端安全设置	B-9
B.4 配置客户端以访问不安全的网络（无安全性）	B-11
B.5 在客户端上配置静态 WEP 安全性	B-12
B.6 在客户端上配置 IEEE 802.1x 安全性	B-15
B.6.1 使用 EAP/PEAP 的 IEEE 802.1x 客户端	B-15
B.6.2 使用 EAP/TLS 证书的 IEEE 802.1x 客户端	B-19

- B.7 在客户端上配置 WPA/WPA2 Enterprise (RADIUS) 安全性..... B-23
 - B.7.1 使用 EAP/PEAP 的 WPA/WPA2 Enterprise (RADIUS) 客户端 B-23
 - B.7.2 使用 EAP-TLS 证书的 WPA/WPA2 Enterprise (RADIUS) 客户端..... B-27
- B.8 在客户端上配置 WPA/WPA2 Personal (PSK) 安全性..... B-30
- B.9 配置外部 RADIUS 服务器以识别 9160 G2..... B-33
- B.10 获取客户端的 TLS-EAP 证书 B-37
- B.11 配置 RADIUS 服务器用于 VLAN 标记 B-42
 - B.11.1 配置 RADIUS 服务器 B-42

附录 C: 故障排除

- C.1 无线分布系统 (WDS) 问题和解决方案..... C-45
- C.2 集群恢复..... C-45
 - C.2.1 重启或重置接入点 C-46

附录 D: 术语表

索引 1

认证和安全摘要

符合声明

产品:	9160 G2 无线网关 - RA2050、 RA2060 和 RA1001A	
采用的 理事会指令:	EMC 指令:	2004/108/EC
	低电压指令:	2006/95/EC
	RoHS 指令:	2002/95/EC
	R&TTE 指令:	1999/5/EEC
声明符合 标准:	EN 55022: Class B EN 61000-3-2; EN 61000-3-3 EN 55024 ETSI EN 300 113-1: V1.6.1 (2006-08) EN 301 893: 2003-08 V1.2.3 EN 300 328: 2004-11 V1.6.1 EN 301 489-1/17: 2004-11 V1.5.1/ 2002-08 V1.2.1 ETSI EN 301 489-5 V1.3.1 (2002-08) EN 60950-1	
制造商	PSION TEKLOGIX INC. 2100 Meadowvale Blvd. Mississauga, Ontario; Canada L5N 7J9	
制造年份:	2006	
制造商在欧洲共同体 的地址:	PSION TEKLOGIX Bourne End Business Centre Cores End Road, Bourne End, SL8 5AR United Kingdom	
设备类型:	信息技术设备	
设备类别:	商业和轻工业	

FCC 声明

FCC 符合声明 (DoC)	
申请方的名称和地址：	PSION TEKLOGIX 2100 Meadowvale Blvd. Mississauga, Ontario, Canada L5N 7J9 电话：(905) 813-9900
美国代表的 名称和地址：	Psion Teklogix Corp. 1810 Airport Exchange Blvd., Suite 500 Erlanger, Kentucky, 41018, USA 电话：(859) 372-4329
设备类型/使用环境：	计算设备
商品名称/型号：	9160 G2 无线网关
制造年份：	2005
声明符合标准：	
9160 G2 无线网关由 Psion Teklogix 提供，经过测试证明符合 FCC 第 15 部分，子部分 B - 无意辐射体，可供家庭和办公室使用的 B 级计算设备的要求。	
申请方：	Psion Teklogix Inc. Mississauga, Ontario, Canada
美国法定代理：	Psion Teklogix Corp. Erlanger, Kentucky, USA

9160 G2 无线网关经过测试，符合 FCC 规则第 15 部分中关于 B 级数字设备的规格要求。设备的操作满足以下两个条件：

- 1. 此设备不会产生有害干扰，并且
- 2. 此设备必须抗任何外部干扰，包括可能导致意外操作的干扰。

这些限制旨在提供合理保护，防止此设备在居住区安装时产生有害干扰。此设备可产生、使用并会发射无线电频率能量，而且，如果未按说明进行安装和使用，可能会对无线电通讯造成有害干扰。但并不保证进行特定安装时不产生干扰。如果本设备确实对收音机或电视机接收造成有害干扰（可以通过关闭和打开本设备来判断），我们鼓励用户通过采取以下一种或多种措施消除干扰：

- 重新定向或定位接收天线。
- 增加设备或装置之间的间距。
- 将设备连接至插座而不是接收器。
- 咨询经销商或有经验的收音机/电视技术人员，以寻求帮助。



重要说明： 未经 *Psion Teklogix* 明确授权，对此产品所做的任何更改或修改都可能导致用户无权操作此设备。

RF 辐射暴露声明

为符合 FCC 和 ANSI C95.1 RF 暴露限制，此设备的天线必须符合以下要求：

- 所有接入点天线在工作时与使用随附电缆的所有人员的距离至少应达到 25 厘米（9.8 英寸），且不得为共置天线或与任何其他天线和发射器一起工作。
- Gabriel 碟形天线 (P/N 9002006) 要求间隔距离至少应达到 63.2 厘米（24.9 英寸）。



注释： 用于多种操作的双天线不被视为共置天线。

加拿大工业部 (IC) 通信须知

此 B 级数字仪器符合加拿大 ICES-003 和 RSS-210 的规定。

“为防止对授权服务产生无线电干扰，应在室内操作本设备，且将其远离窗户，以提供最大程度的屏蔽。安装在室外的设备（或其发射天线）取决于可。”

Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada. “Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence.”

安全认证

CSA、NRTL/C 和 CB。

CE 标记

在住宅、商业或轻工业环境中使用时，该产品及其经过英国和欧洲认证的外围设备符合 CE 标记的所有要求。

R&TTE 指令 1999/5/EC

本设备符合欧盟指令1999/5/EC 的基本要求（声明详见：www.pSIONteklogix.com）。

Cet équipement est conforme aux principales caractéristiques définies dans la Directive européenne RTTE 1999/5/CE. (Déclaration disponible sur le site: www.pSIONteklogix.com).

Die Geräte erfüllen die grundlegenden Anforderungen der RTTE-Richtlinie (1999/5/EG). (Den Wortlaut der Richtlinie finden Sie unter: www.pSIONteklogix.com).

Questa apparecchiatura è conforme ai requisiti essenziali della Direttiva Europea R&TTE 1999/5/CE. (Dichiarazione disponibile sul sito: www.pSIONteklogix.com).

Este equipo cumple los requisitos principales de la Directiva 1995/5/CE de la UE, “Equipos de Terminales de Radio y Telecomunicaciones”. (Declaración disponible en: www.pSIONteklogix.com).

Este equipamento cumpre os requisitos essenciais da Directiva 1999/5/CE do Parlamento Europeu e do Conselho (Directiva RTT). (Declaração disponível no endereço: www.pSIONteklogix.com).

Ο εξοπλισμός αυτός πληροί τις βασικές απαιτήσεις της κοινοτικής οδηγίας EU R&TTE 1999/5/EK. (Η δήλωση συμμόρφωσης διατίθεται στη διεύθυνση: www.pSIONteklogix.com)

Deze apparatuur voldoet aan de noodzakelijke vereisten van EU-richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur 199/5/EG. (verklaring beschikbaar: www.pSIONteklogix.com).

Dette udstyr opfylder de Væsentlige krav i EU's direktiv 1999/5/EC om Radio- og teleterminaludstyr. (Erklæring findes på: www.pSIONteklogix.com).

Dette utstyret er i overensstemmelse med hovedkravene i R&TTE-direktivet (1999/5/EC) fra EU. (Erklæring finnes på: www.pSIONteklogix.com).

Utrustningen uppfyller kraven för EU-direktivet 1999/5/EC om ansluten teleutrustning och ömsesidigt erkännande av utrustningens överensstämmelse (R&TTE). (Förklaringen finns att läsa på: www.pSIONteklogix.com).

Tämä laite vastaa EU:n radio- ja telepäätelaitedirektiivin (EU R&TTE Directive 1999/5/EC) vaatimuksia. (Julkilausuma nähtävillä osoitteessa: www.pSIONteklogix.com).

Psion Teklogix tímto prohlašuje, že 9160 G2 Wireless Gateway je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1995/5/ES (NV č. 426/2000 Sb.) a Prohlášení o shodě je k dispozici na www.pSIONteklogix.com.

Toto zařízení lze provozovat v České republice na základě generální licence č. GL-12/R/2000.

Psion Teklogix týmto vyhlasuje, že 9160 G2 Wireless Gateway spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1995/5/ES (NV č. 443/2001 Z.z.) a Vyhlásenie o zhode je k dispozícii na www.psionteklogix.com.

Toto zariadenie je možné prevádzkovať v Slovenskej republike na základe Všeobecného povolenia č. VPR-01/2001.



重要安全说明

此安全信息旨在为操作和维修人员提供保护。

- 必须由合格的 Psion Teklogix 人员来安装 9160 G2。若 9160 G2 的安装不正确，将导致制造商的保修服务失效。
- 电源线（如果单独出售）应符合使用该设备所在国家/地区的国家安全条例。
- 使用非制造商推荐或出售的附件可能会导致火灾、触电或人身伤害。
- 为了减少损坏电插座和电源线的风险，断开 9160 G2 时请拉拔插头而不是电源线。
- 连接线应放置在适当的位置，以防踩到、绊倒、受损或挤压。
- 电源线或插头损坏时，请勿使用 9160 G2。立即更换。
- 如果 9160 G2 受到重击、掉落或有其他任何损坏，请勿使用，并交由合格的维修人员进行检查。
- 切勿自行拆卸 9160 G2；应交由合格的维修人员进行维修。不正确的拆卸可能导致电击或火灾。
- 为了减少电击的危险，在尝试对充电器进行维护或清洁前，请将 9160 G2 从交流插座中拔下。
- 除非绝对必要，否则请勿使用电源延长线。使用不合适的延长线可能会导致火灾或触电发生。如果必须使用延长线，请确保：
 - 延长线插脚的数量、尺寸和形状必须和适配器相同。
 - 延长线已正确布线且电气状况良好，线径大于 16 AWG。
- 9160 G2 仅可在室内使用；请勿将 9160 G2 暴露在雨雪环境下。

9160 G2 无线网关的光纤选件是：

1 级 LED 产品
APPAREIL À LED DE CLASSE 1

请勿在易爆气体环境下使用

在有爆炸性气体的环境下使用 Psion Teklogix 设备会导致发生爆炸。

请勿拆卸护盖或打开外壳

为避免受伤，仅可由合格的维修人员拆卸设备护盖和外壳。请勿在护盖和外壳未正确安装的情况下操作该设备。

请勿触摸天线

为了避免由于射频能量的局部加热效应而导致的不适，9160 G2 发射时请勿触摸天线。

连接至室外天线

仅可由 Psion Teklogix 专业的维修人员来安装室外天线。

以太网供电和室外天线的安装



接地

警告： 进行室外天线连接或 POE 连接时，需要连接接地导线。

1. 除电源线中的设备接地导线外，还需要在 9160 和接地之间安装一根辅助的设备接地导线。
2. 辅助设备接地导线的尺寸应大于未接地的分支电路供电导线（标称最小横截面积为 0.75 平方毫米或 18AWG）。辅助设备接地导线应在随附的端子上连至 9160，并且连至接地的方式应确保在 9160 通过以太网供电 (POE) 或使用室外天线时仍可保留接地连接。辅助接地导线的接地连接应符合使用国家/地针对跨接线终接的适用规定。允许对建筑钢筋、金属电气管槽系统或永久可靠地连至接地电气维修设备的任何接地物件进行辅助设备接地导线的终接。
3. 可以使用裸露、带胶套或绝缘的接地导线。带胶套或绝缘的接地导线的外表面应为绿色，或绿色兼有一根或多根黄色胶带。
4. 闪电暴雨期间请勿使用。否则会有遭受闪电电击的风险。

1.1 关于本手册	3
1.2 联机帮助功能、支持的浏览器和限制	5
1.3 文本转换	6
1.4 9160 G2 无线网关概述	7
1.4.1 射频	7
1.4.2 接入点的功能	8
1.4.3 基站的功能	9
1.4.4 微型控制器的功能	9
1.5 功能和优点	9
1.5.1 IEEE 标准支持和 Wi-Fi 兼容性	9
1.5.2 无线功能	9
1.5.2.1 Psion Teklogix 802.IQ 协议	10
1.5.3 安全功能	11
1.5.4 开箱即用的访客接口	11
1.5.5 形成集群和自动管理	12
1.5.6 网络	12
1.5.7 SNMP 支持	12
1.5.8 可维护性	13
1.6 接下来该做什么呢？	13

1.1 关于本手册

本手册介绍了无线网络上一个或多个 9160 G2 无线网关的设置、配置、管理及维护。

第1章：简介

提供本手册概述并介绍 9160 G2 无线网关的功能。

第2章：“安装要求”

介绍 9160 G2 无线网关的物理安装方式，以及如何连接至 9160 G2 进行诊断。

第3章：“启动前检查清单”

提供对所需硬件组件、软件、客户端配置以及兼容性问题的快速检查。

第4章：“设置和启动的快速步骤”

是设置您的 9160 G2 无线网关并创建无线网络的逐步指南。

第5章：“配置基本设置”

说明如何配置管理员访问设置和新接入点设置。

第6章：“管理接入点和集群”

介绍接入点集群以及如何导航至集群内的特定接入点。

第7章：“管理用户帐户”

介绍可用于控制接入点的客户端访问权限的用户管理功能。

第8章：“信道管理”

介绍 9160 G2 无线网关如何自动分配集群接入点使用的无线电信道，以减少相互干扰或对集群外部其他接入点的干扰。

第9章：“无线邻居”

详细介绍相邻接入点，包括识别信息、集群状态和统计数据信息。

第10章：“配置安全性”

提供大量身份验证和加密方法，确保只有预期用户才能访问您的无线基础设施。详细介绍各种安全模式。

第11章：“维护和监控”

介绍单个接入点（而不是集群配置）的维护和监控任务。

第12章：“以太网（有线）接口”

介绍如何在 9160 G2 无线网关上配置有线接口设置。

第13章：“设置无线接口”

介绍如何在 9160 G2 无线网关上配置无线地址和相关设置。

第14章：“设置访客接入”

允许配置 9160 G2 无线网关，以控制访客对独立网络的访问。

第15章：“配置VLAN”

介绍如何在虚拟 LAN (VLAN) 上配置多个无线网络。

第16章：“配置802.11 射频设置”

介绍如何在 9160 G2 无线网关上配置无线通信设置。

第17章：“MAC 地址过滤”

说明如何使用 MAC 地址过滤以控制客户端对无线网络的访问。

第18章：“负载均衡”

介绍如何配置无线网络上的负载均衡，从而平衡多个接入点上无线客户端连接的分布。

第19章：“服务质量(QoS)”

说明如何配置多个队列上的参数，以提高吞吐量以及差异化无线流量的性能。

第20章：“无线分布系统”

介绍如何配置 9160 G2 无线网关上的无线分布式系统 (WDS)，使您能够连接多个接入点，这些接入点之间以标准化方式进行无线通信。

第21章：“配置SNMP”

介绍如何在 9160 G2 无线网关企业管理器 API 上配置 SNMP 及相关设置。

第22章：“9160 G2 用作基站”

介绍如何将 9160 G2 无线网关配置为有线或无线基站，或远程无线通信模块 (RRM)。本章还介绍窄带无线通信配置设置。

第23章：“微型控制器配置”

介绍 9160 G2 无线网关用作微型控制器时的配置。

第24章：“802.1Q 设置”

介绍适用于 9160 G2 基站和迷你控制器的 802.1Q 专有无线协议的设置。

第25章：“网络时间协议服务器”

介绍如何配置 9160 G2 无线网关，以使用指定的网络时间协议 (NTP) 服务器同步网络上的计算机时钟时间。

第26章：“备份和还原配置”

介绍如何备份配置文件，以便稍后用于将接入点还原为之前保存配置。

第27章：“规格”

详细介绍 9160 G2 无线网关及其射频的物理、环境及各种工作规格。

附录 A：端口引脚分配和接线图

包括 9160 G2 的端口和电缆的引脚分配及布线图。

附录 B：无线客户端/RADIUS 服务器上的安全设置

详细介绍如何配置客户端上的安全设置，以匹配各个网络 (AP) 连接当前使用的安全模式。

附录 C：故障排除

介绍如何解决在多个集群接入点服务的网络上更新网络配置时可能遇到的常见问题。

附录 D：术语表

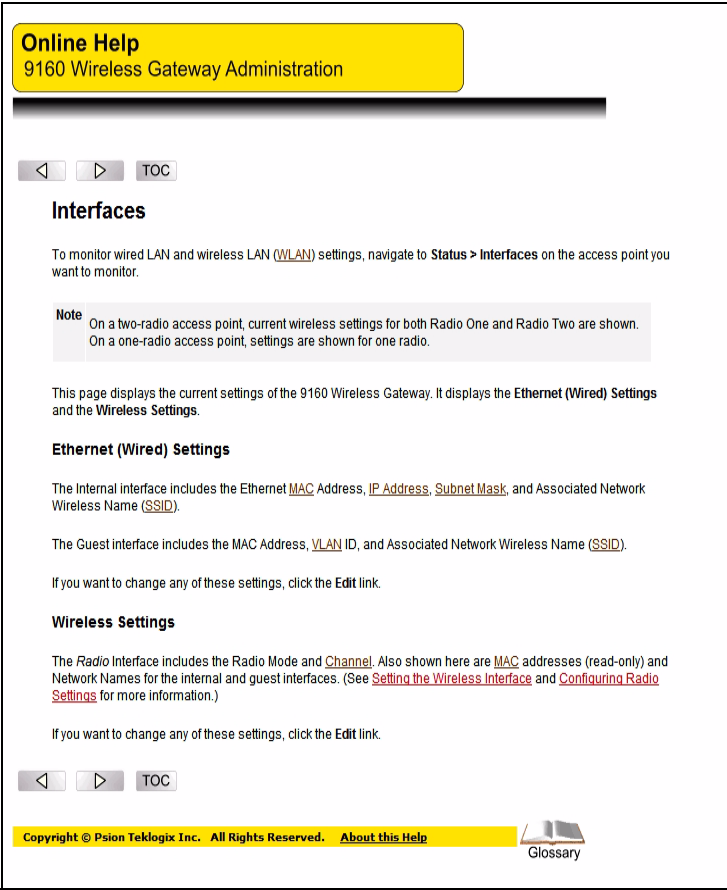
提供对本手册中以加粗斜体形式显示的术语的定义及更多详情。

1.2 联机帮助功能、支持的浏览器和限制

9160 G2 无线网关联机帮助提供有关用户界面上出现的所有字段和功能的信息。联机帮助中的信息是《用户手册》所提供信息的子集。

联机帮助信息与 9160 G2 无线网关管理用户界面上的各个选项卡相对应。单击选项卡上的 **Help**（帮助）按钮或 UI 上联机帮助面板底部的“More...”（更多...）链接，获取当前选项卡上的设置的帮助信息。

图 1.1 联机帮助屏幕



1.3 文本转换



注释：“注释”强调了其他有用信息。



重要说明： 这些语句提供非常重要的说明或对操作移动数据终端或其他设备而言至关重要的其他信息。



警告： 这些语句提供可防止人员受伤、设备损坏或数据丢失的重要信息。



字段描述信息旁边的箭头（通常在表格中出现）表示针对**接入点 (AP)** 上某个选项的推荐或建议配置。

加粗斜体

对于本手册中显示为**加粗斜体**的术语，您可在附录 D：“术语表”中找到其相关条目，其中提供定义及更多详情。本手册中并非所有术语都是突出显示的，但术语表涵盖的术语更多，因此如果遇到不熟悉的词语或表述，请参阅术语表。

1.4 9160 G2 无线网关概述

9160 G2 无线网关提供无线和以太网设备之间连续、高速的访问。它是先进的、基于标准的解决方案，适用于中小型企业内的无线网络部署。9160 G2 无线网关实现了零管理无线局域网 (**WLAN**) 部署，同时提供最先进的无线网络功能。

9160 G2 无线网关无需额外的管理和安全服务器软件，即可提供独立且完全安全的无线网络，因此实现了最佳安全性，易于管理并提供了行业标准。

9160 G2 专为支持各种系统配置而设计。9160 G2 使用 IEEE 802.11 无线 LAN 标准，因此可用作无线和有线网络之间的透明网桥（接入点）。这样，无线客户端就能够访问网络，并能够在网络中的各个 9160 G2 之间无缝移动。9160 G2 可用作微型控制器、基站和远程无线通信模块 (RRM)，并成为 mapRF 系统的组成部分。

1.4.1 射频

9160 G2 能够支持单射频或双射频操作。可用的射频模块包括 802.11a/g 射频、802.11g 射频和 RA1001A 窄带射频。有关这些射频的详细规格，请参阅第 316 页的“射频”。

根据安装的射频，接入点能够在下列模式下运行：

- IEEE **802.11b** 模式。
- IEEE **802.11g** 模式。
- IEEE **802.11a** 模式。
- Atheros Turbo 5 GHz。
- Atheros Dynamic Turbo 5 GHz。
- Atheros Turbo 2.4 GHz。
- Atheros Dynamic Turbo 2.4 GHz。
- 扩展范围。
- Psion Teklogix 窄带轮询协议。



重要说明： *Psion Teklogix 移动数据终端不支持 Atheros Turbo 模式，并且为了防止不必要的无线通信开销，不建议使用 Turbo 模式。*

9160 G2 无线网关支持四种不同的射频配置：802.11g、802.11g + 802.11ag、NB（窄带）和 NB + 802.11ag。

根据“型号”值识别这些不同的变量，该值显示在 *Maintenance（维护） > Upgrade（升级）* Web 页面上（请参阅第 8 页的图 1.2）。型号定义如下：

- 9160 无线网关 = 802.11g。
- 9160 无线网关（双射频） = 802.11g + 802.11ag。
- 9160 无线网关 NB = NB。
- 9160 无线网关 NB（双射频） = NB + 802.11ag。



注释：对于“仅 NB”情况，Web 页面会显示单个 802.11 射频的配置页面。但是，如果您尝试配置不存在的射频，则可以忽略，因为这不会在 9160 G2 中导致任何问题。

图 1.2 升级固件 Web 页面

Upgrade firmware

Model

9160 Wireless Gateway NB (Dual Radio)

Platform

PTX9160G2

Firmware Version

E187k

New Firmware Image

Browse...

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

Upgrade

1.4.2 接入点的功能

接入点连接至有线网络时，9160 G2 无线网关便形成了 Psion Teklogix RF 移动数据终端或无线接入点客户端与 Psion Teklogix 网络控制器或主机之间的通信链路。它通过 IEEE 802.11 RF 数据链路与移动数据终端通信，并通过一根电缆与网络控制器或主机通信。9160 G2 可通过以太网连接连接至网络。

1.4.3 基站的功能

用作基站或远程无线通信模块 (RRM) 时，9160 G2 使用 Psion Teklogix 专有无线通信协议，提供局域网和的无线移动数据终端之间的链路。在局域网上，9160 G2 基站（或 RRM）使用通过 TCP/IP 的专有 9010 协议，与 9500 通信服务器（或使用 Psion Teklogix 软件开发套件的主机）进行通信。

有关将 9160 G2 配置为基站或 RRM 的信息，请参阅第 22 章：“9160 G2 用作基站”。

1.4.4 微型控制器的功能

9160 G2 配备一些仿真功能，因此可用作微型控制器。将 9160 G2 配置为微型控制器时，Psion Teklogix 移动数据终端可以通过 9160 G2（而不是 9500 通信服务器）仿真 ANSI、5250 或 3274 移动数据终端。

要将 9160 G2 无线网关配置为微型控制器，请参阅第 23 章：“微型控制器配置”。

1.5 功能和优点

1.5.1 IEEE 标准支持和 Wi-Fi 兼容性

- 支持 *IEEE 802.11a*、*IEEE 802.11b*、*IEEE 802.11g*、*IEEE 802.11i* 和 *IEEE 802.3af* 无线网络标准。
- 为 *IEEE 802.11a* 或 *IEEE 802.11g* 提供高达 54 Mbps 的带宽（对于 *IEEE 802.11b*，提供 11 Mbps 的带宽；对于 *Atheros 802.11a Turbo*，提供 108 Mbps 的带宽）。
- 认证所需的 Wi-Fi 兼容性。

1.5.2 无线功能

- 启动时自动选择信道。
- 发射功率调整。
- 用于无线连接多个接入点的无线分布式系统 (*WDS*)。通过更少的布线扩展您的网络。
- 服务质量 (*QoS*) 提高了对时间敏感的无线通信（例如视频、音频、IP 语音 (VoIP) 和流媒体）的吞吐量和性能。我们的 QoS 与 Wi-Fi 多媒体 (WMM) 兼容。
- 负载平衡。
- 内置对同一接入点上多个 *SSID*（网络名称）和多个 *BSSID*（基本服务集 ID）的支持。
支持两个专用 BSSID，其中一个用于内部（主要和管理）网络，另一个用于访客网络。使用 VLAN 支持 6 个额外的通用 BSSID（被称为虚拟无线网络或 VWN）。

- 信道管理可自动协调无线通信信道的分配，从而减少网络上 AP 之间的干扰并实现 Wi-Fi 带宽最大化。
- 相邻接入点检测（也被称为“非法”AP 检测）。
- 支持 **IEEE 802.11d** 监管域的选择（用于全球运行的国家/地区代码）。
- 支持 **IEEE 802.11h**，采用 TPC 和 DFS。
IEEE 802.11h 是提供满足 5GHz 频段的特定监管域所需的两项服务的标准。这两项服务分别是传输功率控制 (TPC) 和动态频率选择 (DFS)。
- 支持扩展范围 (XR)。
- SpectraLink 语音优先级 (SVP)。
SpectraLink 语音优先级 (SVP) 是用于部署 Wi-Fi 的 QoS 方法。SVP 是开放式规范，与 IEEE 802.11b 兼容。SVP 最大限度地减少了延迟，并优先于数据包安排无线 LAN 上的语音包，因此增加了提高网络性能的可能性。

1.5.2.1 Psion Teklogix 802.IQ 协议

802.IQ 是 Psion Teklogix 专有协议，它使得移动数据终端能够在同时支持 TCP/IP 和 802.IQ 协议的网络中的无线 LAN 下运行。802.IQ 协议提供两个版本：802.IQ v1 和 802.IQ v2。9160 G2 无线网关可以同时支持协议的两个版本（移动数据终端只能使用一个）。

802.IQ v1 协议是无线 LAN 路由方案，在 802.11 无线网络中提供比 TCP/IP 路由更高的性能。移动数据终端可以使用 TCP/IP 或 802.IQ v1 协议与 9160 G2 接入点通信，这样便实现了系统的双操作性。

802.IQ v2 协议是 802.IQ v1 协议的增强版本，通过 UDP 层传输数据包。它提供 802.IQ v1 具有的所有功能，此外还增添了一些新的功能，包括通过 RF 进行软升级，在控制器和移动数据终端之间添加第三方接入点，以及集成进 mapRF 系统（如果需要）。

有关 802.IQ 的更多信息和配置菜单，请参阅第 24 章：“802.IQ 设置”。

1.5.3 安全功能

- 禁止 SSID 广播。
- 忽略 SSID 广播。
- 避免弱 IV。
- 无线等效隐私 (**WEP**)。
- 符合以下标准的 Wi-Fi 认证：
 - IEEE 标准：802.11b、802.11g、802.11d
 - 安全性：
 - WPA™ - 个人版
 - WPA™ - 企业版
 - WPA2™ - 个人版
 - WPA2™ - 企业版
 - EAP 类型：
 - EAP-TLS
 - EAP-TTLS/MSCHAPv2
 - PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
 - EAP-SIM
- 高级加密标准 (**AES**)。
- 通过本地身份验证服务器实现基于用户的访问控制。
- 本地用户数据库和用户生命周期管理。
- MAC 地址过滤。
- 通过 **WDS** 的 WPA/WPA2。
- 安全套接字壳 (SSH)。
- 安全套接字层 (SSL)。

1.5.4 开箱即用的访客接口

- 访客接口的唯一网络名称 (**SSID**)。
- 指导访客前往可自定义、仅限访客访问的 Web 页面的强制网络门户。
- VLAN 和以太网选项。

1.5.5 形成集群和自动管理

- 通过形成集群和集群会合，设置和自动配置 AP。

管理员可以指定新的接入点在添加到网络前的配置方式。添加新的接入点时，它们会自动与集群会合，并安全地下载正确的配置。该过程不需要人工干预，但却是在管理员的控制下进行的。

- 集群接入点和集群配置设置的单个通用视图。

集群中的所有接入点的配置可以在一个界面管理。对通用参数所做的更改会自动反映在该集群的所有成员中。

- 具有自动配置同步功能的自我管理 AP。

集群中的接入点会定期检查集群配置是否一致，并检查该集群其他成员的状态和可用性。管理员可以通过用户界面监控此信息。

- 使用 802.1x 的增强型本地身份验证，无需其他 IT 设置。

集群可以维护接入点上存储的用户身份验证服务器和数据库。这样，就无需再安装、配置和维护 **RADIUS** 基础设施，简化了部署安全无线网络的管理任务。

1.5.6 网络

- 支持动态主机配置协议 (**DHCP**)，以动态获取网络配置信息。
- 支持虚拟局域网 (VLAN)。
- 虚拟无线网络（动态 VLAN）。
- 生成树协议 (**STP**)。
- **802.1p**
- 支持 100Base-FX 光纤。

1.5.7 SNMP 支持

9160 G2 无线网关包括以下标准：简单网络管理协议 (**SNMP**) 管理信息库 (**MIB**)：

- 桥接 MIB 802.1d (RFC 1493)。
- SNMPv2 MIB (RFC 3418)。
- IEEE 标准 802.11 MIB（基础）。
- 接口组 MIB (RFC 2233)。

- 基于即将推出的 IEEE 802.11k MIB 的两个专有 MIB（无线 MIB 和系统 MIB）。它们分别提供 9160 G2 无线网关客户端关联列表和 AP 检测表的相关信息。专有系统 MIB 提供维护功能，例如系统重启或固件升级。

1.5.8 可维护性

- 网络的状态、监控和跟踪视图，包括会话监控、客户端关联、发射/接收统计数据 and 事件日志。
- 链路完整性监控，不断地验证与客户端的连接，无论网络通信活动处于哪个级别。
- 重置配置选项。
- 固件升级。
- 备份和还原接入点配置。
- 备份和还原内置 RADIUS 服务器的用户数据库（适用于 IEEE 802.1x 和 WPA/WPA2 企业版 (RADIUS) 安全模式）。

1.6 接下来该做什么呢？

准备好开始使用无线网络了吗？安装 9160 G2 无线网关后（请参阅第 2 章：“安装要求”），请阅读第 3 章：“启动前检查清单”，然后按照第 4 章：“设置和启动的快速步骤”中的步骤进行操作。

安装要求

2

2.1 选择合适的安装位置	17
2.1.1 环境	17
2.1.2 维护	18
2.1.3 射频	18
2.1.4 电源线和天线	18
2.1.4.1 电源	18
2.1.4.2 天线	18
2.2 连接至外部设备	19
2.2.1 端口	20
2.2.2 LAN 的安装：概述	20
2.2.3 LAN 安装：以太网	20
2.2.3.1 以太网布线	21
2.2.3.2 100Base-FX 光纤以太网端口	21
2.2.4 状态指示灯 (LED).	21
2.2.5 连接视频显示终端	22
2.3 使用 Web 浏览器更改配置	22



警告： 必须由合格的 Psion Teklogix 人员来安装 9160 G2。

2.1 选择合适的安装位置

通常情况下，Psion Teklogix 会对现场进行勘察，并建议最适合安装 9160 G2 的位置。这些位置需提供良好的无线电覆盖范围，最大程度缩短与主机或网络制器的距离，并达到环境要求。

2.1.1 环境

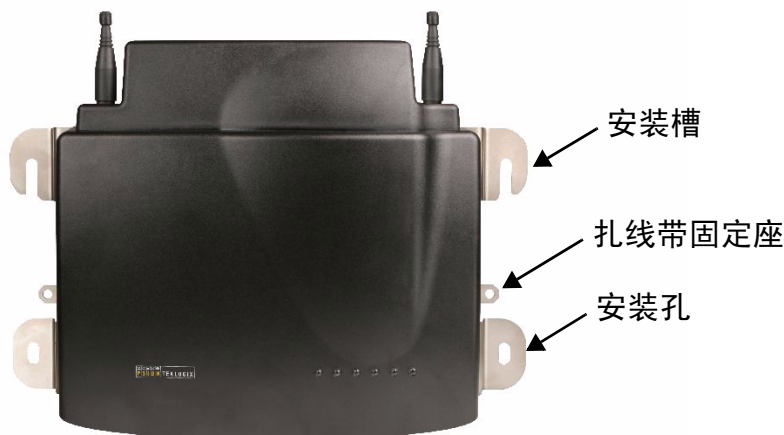
9160 G2 应放置在通风良好的区域，且应避免极端温度波动（例如直接加热器输出、装运门或直射阳光）。如果需要保护盖，则必须有足够的通风才能证设备的正常运行。

请参阅第 27 章：“规格”了解有关环境要求的更详细介绍。请谨记，如果环境条件没有本手册中所列的环境条件那么严重，那么本设备的长期稳定性将得到增强。

9160 G2 的位置应远离车辆行驶通道，避免洒水或灰尘散落。仅可将 9160 G2 安装为竖直姿态，如第 17 页的图 2.1 所示。这种安装方向最大程度地降低了 9160 G2 进水的风险，除非设备被意外洒上了水。

使用后面板上的四个紧固件将 9160 G2 固定到竖直表面上（紧固件类型取决于安装表面）。后面板上最上面的两个孔是插槽，这样将可以先将设备悬挂位，然后再安装剩余的螺栓，令安装变得非常简单。安装中使用的螺栓是 SAE 1/4-20。

图 2.1 9160 G2 安装姿态



2.1.2 维护

9160 G2 没有内部选择开关，并且不需要物理访问；所有配置设置都远程进行（请参阅第 45 页的“导航至基本设置”）。环境和无线电通信注意事项仍然适用。

2.1.3 射频

- 不带集成天线的 802.11g 射频。
- 不带集成天线的 802.11a/g 射频（可选的第二台射频）。
- RA1001A - 窄带 (NB) 射频。

2.1.4 电源线和天线

2.1.4.1 电源

为了防止连接意外断开并对 9160 G2 产生压力，应将天线和电源线固定到距离设备 30 厘米内的位置。使用扎线带将线缆固定到 9160 G2 上的扎线带固定座（参见图 2.1）。单相电源插座（从 100 到 240 VAC，最小额定电流 1.0A）应安装在距离 9160 G2 1 米（3.1 英尺）以内的位置。9160 G2 自动进行调整，确保输入在电源范围内。电源线可拔掉，提供了适于您的设备安装位置的电源类型。9160 G2 AC 电源支持通过标准 IEC320 接头的通用输入。

9160 G2 无线网关与 IEEE 802.3af 兼容，并且可以通过其以太网连接供电，因此无需再使用 AC 布线。有关详细信息，请参阅第 316 页的“以太网供电要求”。



警告： 为避免触电，必须始终将电源线保护接地导线连至接地。

2.1.4.2 天线

每次安装所需的天线类型取决于覆盖要求和使用的频率。最多可以使用四个天线元件。这些天线可以与反向螺纹 SMA “螺口式”多用途天线或高增益 WDS 天线组合使用。Psion Teklogix 提供多种全指向天线以及特殊的定向天线。一般来说，现场勘查会确定适用的天线。要了解详细信息，请咨询 Psion Teklogix 服务人员。



警告： 绝不要在天线不合适或虚负载的情况下使用 9160 G2。

连接到室外天线 (Kit P/N 1916641)

必须由合格的服务人员根据当地的电气安装规范来安装天线。天线的安装位置应至少 15 英尺（4.6 米）高，且距离用户以及该区域内其他工作人员至 10 英尺（3 米）远。

对于连接到室外天线的 9160 G2，以下所有注意事项都适用：

1. 在建筑物上安装时，室外天线同轴电缆的屏蔽线应连到接地（独立于 9160 G2），前提是所在国家/地区的当局部门接受这种安装方式。
2. 除电源线的设备接地导线外，还需要在 9160 G2 和接地之间安装一根辅助的设备接地导线。
3. 辅助设备接地导线的尺寸应大于未接地的分支电路供电导线（标称横截面积最小为 0.75 平方毫米或 18AWG）。辅助设备接地导线应连接至 9160 G2 的随附端子，并且在连接到接地时应确保在拔掉电源线时仍可保留接地连接。辅助接地导线的接地连接应符合使用时所在国家/地区针对搭接线端接的适用规定。允许对建筑钢筋、金属电气管槽系统或永久可靠地连至接地电气维修设备的任何接地物件进行辅助设备接地导线的端接。
4. 可以使用裸露、带胶套或绝缘的接地导线。带胶套或绝缘的接地导线的外表面应为绿色（仅限美国和加拿大）或绿黄相间（所有国家/地区）。
5. 闪电暴雨期间请勿使用。否则会有遭受闪电电击的风险。
6. 对于芬兰、挪威和瑞典，该设备在采用等电位联结的访问受限区域使用。永久连接的保护接地导线由服务人员安装。



警告： 出于射频安全考虑，用户不得接近天线。

Psion Teklogix 提供将 9160 G2 连接到天线所需的同轴电缆。确定天线的安装位置时，应同时考虑天线的覆盖范围要求和 9160 G2 的环境要求。

必须使用拉线桩和/或同轴电缆固定夹。在靠近天线和 9160 G2 的位置需要多使用几英寸电缆，以便更容易断开连接。

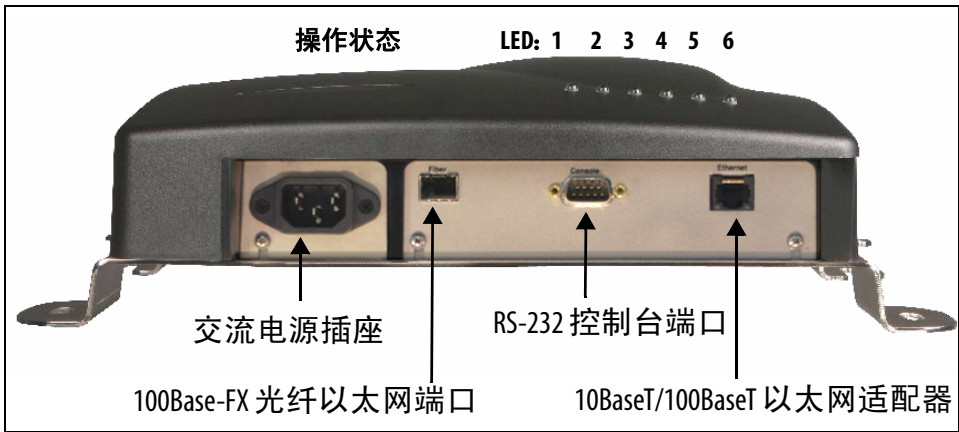
2.2 连接至外部设备

本节介绍将 9160 G2 连接至网络控制器、基站、主机、PC 和视频显示终端等外部设备的一般指南。

2.2.1 端口

第 20 页的图 2.2 显示了 9160 G2 底座上端口和电源接头的位置。端口引脚分配如附录 A：“端口引脚分配和接线图”中所述。

图 2.2 9160 G2 端口和 LED 位置



* 注：较旧版本的 9160 G2 没有光纤端口。

2.2.2 LAN 的安装：概述

由于 9160 G2 提供以太网连接，因此可将它添加到现有 LAN。一般来说，需要在网络管理员的帮助下处理 LAN 的安装，因为他们对网络及其配置较为熟悉。在安装、连接好 9160 G2 并打开电源后，系统管理员可访问该设备以检查配置并为 9160 G2 分配唯一的 IP 地址。此操作可通过网络完成（参阅第 22 页的“使用 Web 浏览器更改配置”）。网络中的后续更改（例如添加工作站或用户）也将需要更改 9160 G2 配置。



重要说明：配置好 9160 G2 且第一次重启后，应禁用 DHCP，直到 9160 G2 从服务器获取其 IP 地址。

2.2.3 LAN 安装：以太网

9160 G2 是高性能接入点，通过全双工和半双工通信来支持 100Mb/s 快速以太网 LAN 以及 10Mb/s。它配备了：

- 一个 10BaseT/100BaseT 卡（使用 5 类双绞线，一个 RJ-45 连接器，运行速率为 10 或 100Mb/s）。对于端口引脚分配，请参阅附录 A：“端口引脚分配和接线图”。
- 一个 100Base-FX 光纤端口（有关详情请参阅第 2.2.3.2 节）。



注释：9160 G2 不支持除以太网 10BaseT、100BaseT 和 100Base-FX 外的任何连接类型。

2.2.3.1 以太网布线

9160 G2 的中继器之间允许的最长电缆段长度（10BaseT/100BaseT 以太网布线）为 100 米。

2.2.3.2 100Base-FX 光纤以太网端口

9160 G2 无线网关提供 100Base-FX 光纤联网支持。要使用光纤以太网端口，用户必须在 9160 G2 光纤扩展槽中安装一个小型可插拔 (SFP) 100Base-FX 模块。SFP 是紧凑型光学模块收发器，实现了高速传输。

安装硬件后，启用此功能：无需对端口进行配置，9160 G2 软件会在启动时自动检测是否存在 SFP 模块，并使用它取代标准的 10/100BaseT 端口。

在手指的按压下，模块将首先插入电接口。SFP 模块不可热插拔。只能在 9160 G2 的电源关闭时插入或取出。

启动时，9160 G2 将在串行控制台端口输出以下两条消息中的一条，具体取决于是否安装了 SFP 模块：

ixp425_eth: 检测到 100BASE-FX SFP 光纤模块

ixp425_eth: 未检测到 100BASE-FX SFP 光纤模块

使用光纤接口时，9160 G2 仅支持 100Mb/s 通信。无论使用哪个以太网端口，9160 G2 都使用相同的有线 MAC 地址。

不支持同时使用两个以太网端口。支持使用 PoE（通过 10/100BaseT 端口）和光纤接口。在此配置中，10/100BaseT 端口只能用于供电。

2.2.4 状态指示灯 (LED)

该高性能 9160 G2 的外壳前面有六个状态指示灯，如第 20 页的图 2.2 中所示。设备前面带编号的彩色 LED 表示各个端口的工作状态，如第 21 页的表 2.1 中所述。

表 2.1 9160 G2 LED 功能：外壳前面

LED 编号	名称	功能	颜色
1	以太网链路	10BaseT/100BaseT 链路指示灯： 亮起 = 链路良好；熄灭 = 无链路	黄色 *
2	以太网活动	以太网 LAN 活动 (Rx/Tx)	绿色

表 2.1 9160 G2 LED 功能：外壳前面 （续）

3	第一个 802.11 射频状态	第一个 802.11 射频活动 (Rx/Tx)	绿色
4	第二个 802.11 射频状态	第二个 802.11 射频活动 (Rx/Tx)	绿色
5	NB 射频状态	NB 射频活动 (Rx/Tx)	绿色
6	电源	LED 常亮 = 设备已通电 LED 熄灭 = 设备没有接通电源	绿色

* LED 1 颜色表示远距离查看时 LED 的方向。

2.2.5 连接视频显示终端

ANSI 兼容的视频显示终端 （例如 DEC VT220 或更高版本），或运行终端仿真的 PC，用于诊断目的。

该终端连接至 9160 G2 上的 RS-232 端口 （参阅第 20 页的图 2.2.2）。通常情况下，此端口设置为使用 115,200 波特率、8 位、1 个停止位、无奇偶校验。为符合 FCC 规则第 15 部分中关于 B 级计算设备的要求，只能使用随附的电缆 (P/N 19387)。

2.3 使用 Web 浏览器更改配置

可以使用标准 HTML Web 浏览器，例如 MS Internet Explorer （版本 4.0 或更高版本）或 Firefox，通过网络远程重新配置 9160 G2 闪存。请参阅第 4 章：“设置和启动的快速步骤”，了解有关更改参数和一般配置设置的说明。

启动前检查清单

3

- 3.1 产品名称 25
 - 3.1.1 产品名称的默认设置 25
 - 3.1.2 接入点不提供哪些功能 28
- 3.2 管理员的计算机 28
- 3.3 无线客户端计算机 29
- 3.4 了解产品名称上的动态和静态 IP 寻址 30
 - 3.4.1 启动时接入点如何获取 IP 地址? 30
 - 3.4.2 动态 IP 寻址 31
 - 3.4.3 静态 IP 寻址 31
 - 3.4.4 恢复 IP 地址 31

插入并启动新的接入点前，请阅读以下部分，快速检查所需的硬件组件、软件、客户端配置以及兼容性问题。确保成功启动并测试新的（或扩展）无线网络所需的一切工作准备就绪。

3.1 产品名称

产品名称是网络上设备的无线通信中心。它提供 IEEE 802.11a、802.11b、802.11g 和 802.11a Turbo 模式下无线设备和以太网设备之间连续、高速的访问。

产品名称提供开箱即用的访客接口功能，允许您使用虚拟 LAN 配置接入点，以便控制访客对无线网络的访问。

有关访客接口的更多信息，请参阅第 14 章：“设置访客接入”和第 38 页的“设置访客网络连接时的注意事项”。

3.1.1 产品名称的默认设置

表 3.1 9160 G2 默认设置

选项	默认设置	相关信息
System Name (系统名称)	PTX9160-Wireless-AP	第 136 页的“DNS 主机名”中的第 133 页的“以太网（有线）接口”
User Name (用户名)	admin 用户名是只读的，不可修改。	
Password (密码)	admin	第 47 页的“提供网络设置”中的第 43 页的“配置基本设置”
Network Name (SSID) (网络名称 (SSID))	内部接口为“TEKLOGIX” 访客接口为“TEKLOGIX Guest”	第 46 页的“查看/描述接入点”中的第 43 页的“配置基本设置” 第 149 页的“配置“内部”无线 LAN 设置”中的第 143 页的“设置无线接口” 第 149 页的“配置“访客”网络无线设置”中的第 143 页的“设置无线接口”
Network Time Protocol (NTP) (网络时间协议 (NTP))	None（无）	第 301 页的“网络时间协议服务器”

表 3.1 9160 G2 默认设置 （续）

选项	默认设置	相关信息
<i>IP Address</i> (IP 地址)	192.168.1.10 如果您未使用 <i>动态主机配置协议 (DHCP)</i> 服务器，则使用默认的 IP 地址。您可以通过管理 Web 页面分配一个新的静态 IP 地址。 如果网络上有 <i>DHCP</i> 服务器，则 AP 启动时服务器会动态分配一个 IP 地址。	第 30 页的 “了解产品名称上的动态和静态 IP 寻址”
<i>Connection Type</i> (连接类型)	<i>Dynamic Host Configuration Protocol (DHCP)</i> (动态主机配置协议 (DHCP)) 如果您的内部网络上没有 <i>DHCP</i> 服务器且打算使用，则连接接入点后第一件要做的事就是将 Connection Type (连接类型) 从 “DHCP” 更改为 “Static IP” (静态 IP)。 访客网络必须有一个 DHCP 服务器。	第 30 页的 “了解产品名称上的动态和静态 IP 寻址” 有关如何重新配置 Connection Type (连接类型) 的信息，请参阅第 138 页的 “内部接口设置”。
<i>Subnet Mask</i> (子网掩码)	None (无) 这是由您的网络设置和 DHCP 服务器配置决定的。	第 133 页的 “以太网 (有线) 接口”
<i>Radio</i> (射频)	On (打开)	第 163 页的 “配置 802.11 射频设置”
<i>IEEE 802.11 Mode</i> (IEEE 802.11 模式)	802.11g 或 802.11a+g	第 163 页的 “配置 802.11 射频设置”
<i>802.11g Channel</i> (802.11g 通道)	Auto (自动)	第 163 页的 “配置 802.11 射频设置”
<i>Beacon Interval</i> (信标间隔)	100	第 163 页的 “配置 802.11 射频设置”

表 3.1 9160 G2 默认设置 （续）

选项	默认设置	相关信息
<i>DTIM Period</i> (DTIM 周期)	2	第 163 页的 “配置 802.11 射频设置”
<i>Fragmentation Threshold</i> (分段阈值)	2346	第 163 页的 “配置 802.11 射频设置”
<i>Regulatory Domain</i> (合规区域)	FCC	第 163 页的 “配置 802.11 射频设置”
<i>RTS Threshold</i> (RTS 阈值)	2347	第 163 页的 “配置 802.11 射频设置”
<i>MAX Stations</i> (最大工作站数量)	2007	第 163 页的 “配置 802.11 射频设置”
<i>Transmit Power</i> (发射功率)	100%	第 163 页的 “配置 802.11 射频设置”
<i>Rate Sets Supported (Mbps)</i> (支持的速率设置)	<ul style="list-style-type: none"> • IEEE 802.1a: 54、48、36、24、18、12、9、6 • IEEE 802.1g: 54、48、36、24、18、12、11、9、6、5.5、2、1 • IEEE 802.1b: 11、5.5、2、1 	第 163 页的 “配置 802.11 射频设置”
<i>Rate Sets (Mbps)</i> (速率设置) (基本/广告)	<ul style="list-style-type: none"> • IEEE 802.1a: 24、12、6 • IEEE 802.1g: 11、5.5、2、1 • IEEE 802.1b: 2、1 	第 163 页的 “配置 802.11 射频设置”
<i>Broadcast SSID</i> (广播 SSID)	Allow (允许)	第 98 页的 “配置安全设置”。
<i>Security Mode</i> (安全模式)	None (plain-text) (无 (纯文本))	第 98 页的 “配置安全设置”。

表 3.1 9160 G2 默认设置 （续）

选项	默认设置	相关信息
<i>Authentication Type</i> (身份验证类型)	None （无）	
<i>MAC Filtering</i> (MAC 过滤)	Allow any station unless in list (允许列表之外的任何工作站)	第 173 页的 “MAC 地址过滤”
<i>Guest Login and Management</i> (访客登录和管理)	Disabled （禁用）	第 151 页的 “设置访客接入”
<i>Load Balancing</i> (负载平衡)	Disabled （禁用）	第 177 页的 “负载平衡”
<i>WDS Settings</i> (WDS 设置)	None （无）	第 199 页的 “无线分布系统”

3.1.2 接入点不提供哪些功能

产品名称不能用作 Internet 的网关。要将您的无线 LAN (*WLAN*) 连接到其他 *LAN* 或 Internet，需要有一台网关设备。

3.2 管理员的计算机

产品名称的配置和管理通过基于 Web 的用户界面 (UI) 来完成。表 3.2 介绍了管理员的计算机的最低要求。

表 3.2 AP 管理员必需的硬件和软件

必需组件	描述
与第一个接入点的以太网连接	必须通过一根以太网电缆将用来配置第一个接入点的计算机连接到该接入点（直接连接或通过集线器）。 有关详细信息，请参阅“设置和启动的快速步骤”中的第 36 页的“将接入点连接到网络和电源”。

表 3.2 AP 管理员必需的硬件和软件 （续）

必需组件	描述
与网络的无线连接	<p>在完成初始配置并启动新无线网络上的第一个接入点后，您可以使用与“内部”网络的无线连接，通过管理 Web 页面进行以后的配置更改。要无线连到该接入点，您的管理员设备需要具备与以下任何无线客户端类似的 Wi-Fi 功能：</p> <ul style="list-style-type: none">支持您打算运行接入点的一种或多种 IEEE 802.11 模式的便携式或内置 Wi-Fi 客户端适配器 （支持 IEEE 802.11a、802.11b802.11a、802.11g802.11b、802.11a Turbo802.11g 802.11a Turbo 模式）。Microsoft® Windows® XP 等无线客户端软件或配置为与产品名称相关的 Funk Odyssey 无线客户端。 <p>有关 Wi-Fi 客户端设置的更多详情，请参阅第 29 页的“无线客户端计算机”。</p>
Web 浏览器/操作系统	<p>通过在接入点上托管的基于 Web 的用户界面配置和管理 产品名称。我们建议使用下列支持的 Web 浏览器之一，访问接入点管理 Web 页面：</p> <ul style="list-style-type: none">Microsoft Windows XP 或 Microsoft Windows 2000 上的 Microsoft Internet Explorer 版本 5.5 或 6.x （主要版本的最新补丁级别）Redhat Linux 版本 2.4 上的 Netscape® Mozilla 1.7.x <p>管理 Web 浏览器必须启用 JavaScript，才能支持管理界面的交互功能。它还必须支持 HTTP 上传，才能使用固件升级功能。</p>
安全设置	<p>确保在初始配置接入点时使用的无线客户端上，已禁用安全性。</p>

3.3 无线客户端计算机

产品名称为具备正确配置的 Wi-Fi 客户端适配器的任何客户端提供 802.11 模式的无线访问，接入点也是以此模式运行。

支持多种客户端操作系统。客户端可以是便携式计算机、台式机、个人数字助理 (PDA)，或配备 Wi-Fi 适配器和相应的驱动程序的任何其他手持式、便携式或固定设备。

要连接到接入点，无线客户端需要具有表 3.3 中所述的硬件和软件。

表 3.3 AP 客户端必需的硬件和软件

必需组件	描述
Wi-Fi 客户端适配器	<p>支持您打算运行接入点的一种或多种 IEEE 802.11 模式的便携式或内置 Wi-Fi 客户端适配器（支持 IEEE 802.11a、802.11b 和 802.11g）。</p> <p>Wi-Fi 客户端适配器的差别较大。适配器可以是内置到客户端设备的 PC 卡、便携式 PCMCIA 或 PCI 卡（NIC 类型）、USB 等外部设备，或者您通过电缆连接至客户端的以太网适配器。</p> <p>接入点支持 802.11a/b/g 模式，但是您可以在网络设计阶段正确选择使用哪种模式。对客户端的基本要求是，它们均具备配置好的适配器，这些适配器应与接入点配置的 802.11 模式相匹配。</p>
无线客户端软件	Microsoft Windows Supplicant 等无线客户端软件或配置为与产品名称相关联的 Funk Odyssey 无线客户端。
客户端安全设置	<p>在用来执行接入点初始配置的客户端上，应禁用安全设置。</p> <p>如果将接入点的安全模式设置为纯文本外的任何设置，则无线客户端需要将配置文件设置为接入点所使用的身份验证模式，并提供有效的用户名和密、证书或类似的用户身份证明。安全模式包括静态 WEP、IEEE 802.1x、带 RADIUS 服务器的 WPA 以及 WPA2PSK。</p> <p>有关配置接入点安全性的信息，请参阅第 89 页的“配置安全性”。</p>

3.4 了解产品名称上的动态和静态 IP 寻址

产品名称设计为能够自动配置，只需对第一个接入点进行很少的设置，对于随后加入预先配置**集群**的其他接入点无需进行任何配置。

3.4.1 启动时接入点如何获取 IP 地址？

部署该接入点后，它会查找网络 **DHCP** 服务器，如果找到一个，便会从 DHCP 服务器获取 **IP 地址**。如果在网络上未发现任何 DHCP 服务器，AP 会继续使用其默认的**静态 IP 地址**(192.168.1.10)，直到您为它重新分配一个新的静态 IP 地址（并指定静态 IP 寻址策略）或直到 DHCP 服务器在线。



注释: 如果您配置**内部**和**访客网络**，并计划为两者使用**动态寻址策略**，则必须在各个网络上运行单独的**DHCP 服务器**。

访客网络必须有 DHCP 服务器。

3.4.2 动态 IP 寻址

产品名称通常期望在部署 AP 的网络上有一个 **DHCP** 服务器在运行。大多数家庭和小型企业网络都已经通过网关设备或中央服务器提供 DHCP 服务。但是，如果内部网络上没有 DHCP 服务器，AP 将在首次启动时使用默认的**静态 IP 地址**。

同样地，无线客户端及其他网络设备（例如打印机）将从 DHCP 服务器获得它的 IP 地址（如有）。如果该网络上不存在任何 DHCP 服务器，您必须手动向无线客户端及其他网络设备分配静态 IP 地址。

访客网络必须有一个 DHCP 服务器。

3.4.3 静态 IP 寻址

产品名称随附默认的**静态 IP 地址** 192.168.1.10（参阅第 25 页的“产品名称的默认设置”）。如果网络上未发现任何 **DHCP** 服务器，则 AP 会在首次启动时保留此静态 IP 地址。

AP 启动后，您可以选择在产品名称上指定静态 IP 寻址策略，并通过接入点管理 Web 页面向内部网络上的 AP 分配静态 IP 地址。（参阅第 138 页的“内部接口设置”中有关“Connection Type”（连接类型）字段和相关字段的信息。）



重要说明：如果您的内部网络上没有 DHCP 服务器且不打算使用，则连接接入点后第一件事就是将 Connection Type（连接类型）从“DHCP”更改为“Static IP”（静态 IP）。您可以向该 AP 分配新的静态 IP 地址，或继续使用默认的地址。我们建议分配新的静态 IP 地址，这样，当您以后在相同的网络上连接另一个 9160 G2 无线网关时，各 AP 的 IP 地址将是唯一的。

3.4.4 恢复 IP 地址

如果与接入点通信时遇到问题，可以通过将 AP 配置重置为出厂默认值来恢复**静态 IP 地址**（请参阅第 308 页的“重置出厂默认配置”），或者通过将 AP 连接到拥有 **DHCP** 的网络来获取动态分配的地址。

设置和启动的快速步骤

4

4.1 拆开 9160 G2 无线网关的包装	35
4.1.1 9160 G2 无线网关的硬件和端口	35
4.1.2 9160 G2 无线网关里面都有些什么?	35
4.2 将接入点连接到网络和电源	36
4.2.1 设置访客网络连接时的注意事项	38
4.2.1.1 访客 VLAN 的硬件连接	38
4.3 打开接入点的电源	38
4.4 登录到管理 Web 页面	38
4.4.1 查看接入点的基本设置	39
4.5 配置基本设置并启动无线网络	40
4.5.1 默认配置	40
4.6 接下来该做什么呢?	40
4.6.1 确保接入点已连接到 LAN	40
4.6.2 使用无线客户端测试 LAN 的连接性	41
4.6.3 使用高级功能保证接入点的安全并进行微调	41

设置和部署一个或多个产品名称，实际上就是创建和启动 *无线网络*。Basic Settings（基本设置）管理 Web 页面简化了这一过程。以下是设置您的产品名称以及所创建的无线网络的逐步指南。如果尚未准备好，请先熟悉第 3 章：“启动前检查清单”的内容。

涵盖的主题包括：

- 第 1 步：**拆开 9160 G2 无线网关的包装。**
- 第 2 步：**将接入点连接到网络和电源。**
- 第 3 步：**打开接入点的电源。**
- 第 5 步：**登录到管理 Web 页面。**
- 第 6 步：**配置基本设置并启动无线网络。**
- **接下来该做什么呢？**

4.1 拆开 9160 G2 无线网关的包装

拆开 9160 G2 无线网关的包装并熟悉它的硬件端口、相关缆线以及配件。

4.1.1 9160 G2 无线网关的硬件和端口

9160 G2 无线网关包括：

- 用于通过以太网网线连接局域网 (LAN) 的以太网端口。
- 电源端口和电源适配器。
- 电源开关。
- 一个或两个射频，具体取决于您所使用的产品型号。

4.1.2 9160 G2 无线网关里面都有些什么？

9160 G2 无线网关作为一个 **接入点 (AP)**，是一个专用的数据终端，可起到无线集线器的作用。该接入点内部有一个 Wi-Fi 无线通信系统和一个微处理器。该接入点使用驱动固件从 FlashROM 启动，具备第 7 页的“9160 G2 无线网关概述”中概述的可配置的、运行时功能。

当有新的功能和增强功能可用时，您可以升级该固件以添加新的功能，以及提升构成无线网络的接入点的性能。（请参阅第 309 页的“升级固件”。）

4.2 将接入点连接到网络和电源

下一步就是设置网络和电源连接。

1. 执行以下任一操作，创建接入点和计算机之间的以太网连接：

将以太网电缆的一端连接到接入点上的网络端口，将电缆的另一端连接到 PC 所连的集线器上。（请参阅第 37 页的图 4.2。）

或

将跨接¹ 电缆的一端连接到接入点上的网络端口，将电缆的另一端连接到 PC 上的以太网端口。（请参阅 第 37 页的图 2。）



注释： 如果您使用集线器，则您使用的设备必须允许从接入点广播信号，以便到达网络上的所有其他设备。使用标准的集线器即可。但某些交换机不允许定或子网广播通过。您必须将交换器配置为允许定向广播。

对于使用以太网直连且没有 DHCP 服务器的初始配置，请确保将 PC 设为与接入点上的默认 IP 地址位于同一子网的静态 IP 地址（接入点的默认 IP 地址 192.168.1.10）。

如果对于初始配置，您在接入点和计算机之间使用以太网直连（有线，通过跨接电缆连接），则需要重新配置用于接入点随后启动和部署的布线，以接入点不再直接连接到 PC，而是连接到 LAN（通过图 4.2 中所示的集线器，或直接连接）。

¹ 如果接入点硬件支持 **MDI 和 MDI-X** 自动功能，您可以使用常规的以太网电缆直接连接 PC 和 AP。使用跨接电缆也可以，但是如果您有 MDI 和 MDI-X 自动感应端口，就没有必要使用跨接电了。

图 4.1 使用 DHCP 的以太网连接

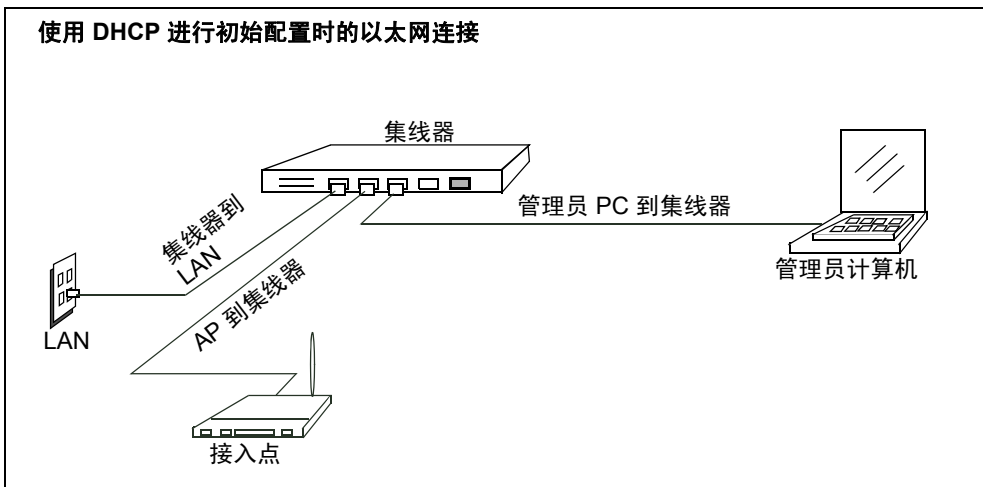
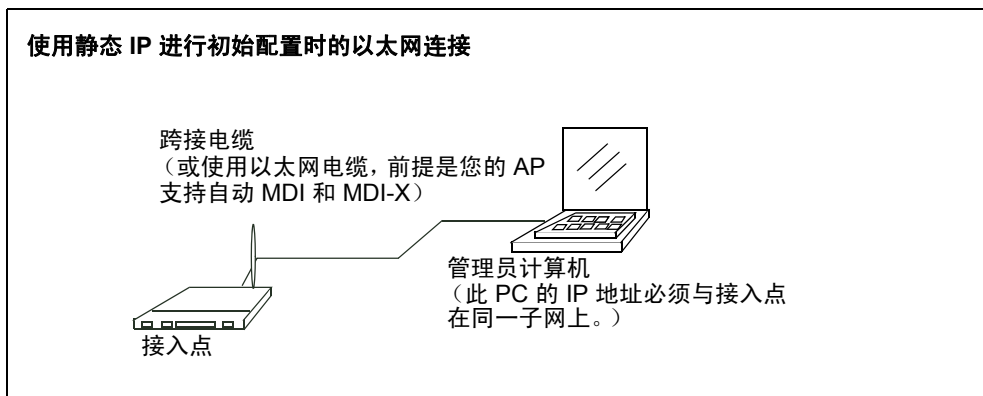


图 4.2 使用静态 IP 的以太网连接



2. 将电源适配器连接到接入点背面的电源端口，然后将电源线的另一端插入电源插座（最好是通过浪涌保护器）。

4.2.1 设置访客网络连接时的注意事项

产品名称提供开箱即用的访客接口，允许您配置一个接入点，以便控制访客对网络的访问。同一接入点还可用作两个不同的无线网络的桥接：安全的“内部”LAN 和公共的“访客”网络。事实上，可通过管理 UI 定义两个不同的虚拟 LAN 来实现。

有关在管理 UI 上配置访客接口设置的信息，请参阅第 14 章：“设置访客接入”。

4.2.1.1 访客 VLAN 的硬件连接

如果您计划使用 VLAN 配置访客网络，请执行以下操作：

- 将接入点上的网络端口连接到支持 VLAN 的交换机。
- 定义该交换机上的 VLAN。

4.3 打开接入点的电源

插入产品名称时，它将开机并进行初始化。

4.4 登录到管理 Web 页面

当您连接到产品名称管理 Web 页面的 IP 地址时，系统会提示您输入用户名和密码。



默认的用户名和密码如下所述。

表 4.1 用户名和密码

字段	默认设置
<i>User name</i> （用户名）	admin
<i>Password</i> （密码）	admin （用户名是只读的，不可修改。）

输入用户名和密码，然后单击 **OK** （确定）。

4.4.1 查看接入点的基本设置

首次登录后，会显示产品名称管理的 *Basic Settings* （基本设置）页面。以下是组成集群的所有接入点的全局设置，如果指定了自动配置，后来添加的所有新接入点也将使用这些设置。

图 4.3 接入点的基本设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Provide basic settings

▶ Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.128.75.4

MAC Address: 00:08:A2:01:4B:52

Firmware Version: E187k

2 ▶ Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password

New Password

Confirm new password

Network Name (SSID)

3 ▶ Settings ...

Click "Update" to save the new settings.

4.5 配置基本设置并启动无线网络

通过定义无线网络的基本设置，提供了一组最低配置信息。这些设置均显示在管理 Web 页面的 *Basic Settings*（基本设置）上，并且分为 Web 页面上的步骤 1-3。

有关这些基本设置以及如何正确配置它们的详细说明，请参阅第 5 章：“配置基本设置”。在这里作简要说明，包括以下步骤：

1. 查阅此接入点的说明。

提供 IP 寻址信息。有关详细信息，请参阅第 46 页的“查看/描述接入点”。

2. 提供网络设置。

为集群接入点提供新的管理员密码。有关详细信息，请参阅第 47 页的“提供网络设置”。

3. 设置。

单击 **Update**（更新）按钮，使用这些新设置激活无线网络。有关详细信息，请参阅第 48 页的“更新基本设置”。

4.5.1 默认配置

如果您按照上述步骤操作并接受所有默认值，则接入点将具有第 25 页的“产品名称的默认设置”中所述的默认配置。

4.6 接下来该做什么呢？

接下来，确保接入点连接到 LAN，然后将出现一些无线客户端，将这些客户端连接到网络。测试完无线网络的基本设置后，您可以通过修改接入点上的高级配置功能，提高安全性，进行微调。

4.6.1 确保接入点已连接到 LAN

如果您通过将接入点和管理员 PC 连接到一个网络集线器对它们进行了配置，则您的接入点已连接到 LAN。这样，您就可以正常使用了！下一步是对一无线客户端进行测试。

如果您通过计算机和接入点之间的跨接电缆，使用有线直连方式配置接入点，请执行以下操作：

1. 断开跨接电缆与计算机和接入点之间的连接。
2. 使用一根常规的以太网电缆将接入点连接到 **LAN**。
3. 通过以太网电缆或无线客户端卡将您的计算机连接到 LAN。

4.6.2 使用无线客户端测试 LAN 的连接性

通过尝试检测产品名称并将其与一些无线客户端设备相关联，对其进行测试。
(请参阅*启动前检查清单*中第 29 页的“无线客户端计算机”，了解有关对这些客户端的要求的信息。)

4.6.3 使用高级功能保证接入点的安全并进行微调

一旦无线网络正常运行并通过一些无线客户端对接入点进行测试后，您可以添加更多安全层、添加用户、配置访客接口并微调性能设置。

配置基本设置

5

5.1 导航至基本设置	45
5.2 查看/描述接入点	46
5.3 提供网络设置	47
5.4 更新基本设置	48
5.5 独立接入点的基本设置	48
5.6 网络概览：了解指示器图标	48

5.1 导航至基本设置

要配置初始设置，请单击 **Basic Settings**（基本设置）。

如果您在浏览器中输入接入点的 IP 地址，则 *Basic Settings*（基本设置）页面是显示的默认页面。

图 5.1 基本设置

PSION TEKLOGIX
Information in motion

9160 Wireless Gateway

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Provide basic settings

1

Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address:

10.128.75.4

MAC Address:

00:08:A2:01:4B:52

Firmware Version:

E187k

2

Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password

New Password

Confirm new password

Network Name (SSID)

Psion Teklogix

3

Settings ...

Click "Update" to save the new settings.

Update

按照第 46 页的“查看/描述接入点”中所述填写 *Basic Settings*（基本设置）页面中的字段。

5.2 查看/描述接入点



表 5.1 Basic Settings （基本设置）屏幕选项

字段	描述
<i>IP Address</i> (IP 地址)	显示分配给此接入点的 IP 地址。此字段不可编辑，这是因为该 IP 地址已分配（通过 DHCP，或如第 141 页的“访客接口设置”中所述通过以太网（有线）静态分配）。
<i>MAC Address</i> (MAC 地址)	<p>显示接入点的 MAC 地址。</p> <p>MAC 地址是代表网络接口的任何设备的永久性、唯一的硬件地址。MAC 地址由制造商分配。您无法更改 MAC 地址。作为接口的唯一标识符，在此仅出于信息目的提供。</p> <p>此处显示的地址是桥接 (br0) 的 MAC 地址。通过此地址，其他网络便可在外部知道该接入点。</p> <p>要查看 AP 上访客和内部接口的 MAC 地址，请参阅 <i>Status</i>（状态）> <i>Interfaces</i>（接口）选项卡。</p>
<i>Firmware Version</i> (固件版本)	<p>有关接入点当前所安装固件的版本信息。</p> <p>当产品名称固件的新版本可用时，您可以在接入点上升级该固件，以使用新功能和增强功能。</p> <p>有关如何升级固件的说明，请参阅第 309 页的“升级固件”。</p>

5.3 提供网络设置

2

Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password


New Password

Confirm new password

Network Name (SSID)

Psion Teklogix

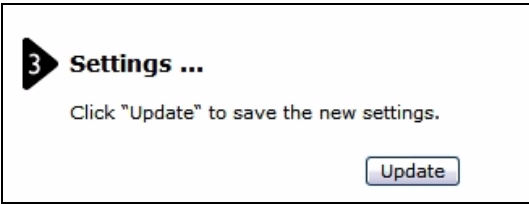
表 5.2 管理员密码和无线网络

字段	描述
<i>Current Password</i> (当前密码)	输入当前的管理员密码。您必须正确输入当前的密码，才能更改密码。
<i>New Password</i> (新密码)	输入新的管理员密码。您输入的字符将显示为 “*” 字符，以防止其他人看到您输入的密码。 管理员密码必须是不超过 8 位的字母数字字符串。请勿使用特殊字符或空格。  作为保证无线网络安全的第一步，我们建议您更改默认的管理员密码。
<i>Confirm New Password</i> (确认新密码)	重新输入新的管理员密码，以确认输入的密码符合预期。
<i>Network Name (SSID)</i> (网络名称 (SSID))	以字符串的形式输入无线网络的名称。该名称将应用到此网络上的所有接入点。添加更多接入点时，它们将共享此 SSID 。 <i>服务集标识符(SSID)</i> 是一个最长 32 个字符的字母数字字符串 注： 如果您作为无线客户端连接到管理的相同 AP，则重置 SSID 会导致您丢失与 AP 的连接。保存新设置后，您需要重新连接至新的 SSID。



注释: 9160 G2 无线网关不适用于多个同步配置更改。如果您的网络包含多个接入点，且有多位管理员登录到管理 Web 页面并更改配置，则集群中的所有接入点将会同步，但不保证应用多个用户指定的所有配置更改。

5.4 更新基本设置



检查新配置后，单击 **Update**（更新）应用设置并将接入点作为无线网络部署。

5.5 独立接入点的基本设置

独立接入点的 *Basic Settings*（基本设置）选项卡仅表示当前模式为独立。如果您想要将当前的接入点添加到现有集群，请导航至 *Cluster*（集群）> *Access Point*（接入点）选项卡。

有关详细信息，请参阅第 58 页的“开始形成集群”。

5.6 网络概览：了解指示器图标

管理 Web 页面上的所有集群设置选项卡包括显示当前网络活动的指示器图标。

5.7 查看显示不同颜色和样式的用户界面

表 5.3 指示器图标




图标	描述
	网络上的一个或多个 AP 可用于服务时，显示“Wireless Network Available”（无线网络可用）图标。集群图标表示当前接入点是“Clustered”（已集群）还是Not Clustered”（未集群）（即，独立还是正在更改状态）。 有关集群的信息，请参阅第 53 页的“了解集群”。
	使用“Access Points”（接入点）图标来表示此网络上可用于服务的接入点的数量。 有关管理接入点的信息，请参阅第 6 章：“管理接入点和集群”。

表 5.3 指示器图标 (续)

图标	描述
	<p>使用“User Accounts”（用户帐户）图标来表示在此网络上创建并启用的客户端用户帐户数量。</p> <p>有关如何在接入点上设置用于内置身份验证服务器的用户帐户的信息，请参阅第 7 章：“管理用户帐户”。还可参阅第 106 页的“IEEE 802.1x”和第 112 页的“WPA Enterprise（WPA 企业版）”，它们是提供使用内置身份验证服务器选项的两种安全模式。</p>

产品名称的管理 Web 页面提供两种不同的配色和样式：(1) Corporate（公司）样式和 (2) Home（家庭）样式。

您可以更改正在查看的 UI 样式，以适合您的偏好。

要切换样式，请在任何管理 Web 页面的底部找到“Style: Corporate, Home”（样式：企业、家庭）按钮，并单击 **Corporate**（企业）或 **Home**（家庭）。



管理接入点和集群

6

6.1 概述	53
6.2 导航至接入点管理	53
6.3 了解集群	53
6.3.1 什么是集群?	53
6.3.2 一个集群支持多少个 AP?	54
6.3.3 什么类型的 AP 可以形成一个集群?	54
6.3.4 协调 AP 与其他集群成员之间是什么关系?	54
6.3.5 哪些设置可以/不可以作为集群配置的组成部分进行共享?	54
6.3.5.1 在集群配置中共享的设置	55
6.3.5.2 集群不共享的设置	55
6.3.6 集群的形成	56
6.3.7 集群大小和成员资格	56
6.3.8 Intra-Cluster 安全	56
6.4 了解接入点设置	56
6.4.1 修改位置描述	58
6.4.2 设置集群名称	58
6.5 开始形成集群	58
6.6 停止形成集群	58
6.7 特定 AP 和管理独立 AP 的配置信息	59
6.7.1 在 URL 中使用 AP 的 IP 地址导航至 AP	59
6.8 会话监控	59
6.8.1 导航至会话监控	60
6.8.2 了解会话监控信息	60
6.8.3 查看接入点的会话信息	62
6.8.4 对会话信息进行排序	62
6.8.5 刷新会话信息	62

6.1 概述

产品名称显示集群接入点当前的基本配置设置（位置、IP 地址、MAC 地址、状态和可用性），并且为属于集群成员的特定 AP 提供了导航至完整配置的方式。

独立接入点或并非此集群成员的接入点不显示在此列表中。要配置独立接入点，您必须知道接入点的 IP 地址并在 URL (<http://IPAddressOfAccessPoint>) 中使用。



注释：9160 G2 无线网关不适用于多个同步配置更改。如果您的网络包含多个接入点，且有多位管理员登录到管理 Web 页面并更改配置，则集群中的所有接入点将会同步，但不保证应用多个用户指定的所有配置更改。

6.2 导航至接入点管理

要查看或编辑集群中的接入点的信息，请单击 **Cluster**（集群）> **Access Points**（接入点）选项卡。

图 6.1 接入点的集群设置

Manage access points in the cluster

Access Points...

Status: Clustering is online...

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

[Stop Clustering](#)

Clustering Options...

Enter the location of this AP.
Location:

Enter the name of the cluster for this AP to join.
Cluster Name:

[Update](#)

Clustering Status: **Clustering is online...**

1 Access Points

6.3 了解集群

产品名称的关键功能是形成动态、配置感知组（被称为**集群**），而其他产品名称位于同一子网中。接入点可以参与自组织集群，使您能够更轻松地部署、管理无线网络并保证其安全。集群提供单点管理，让您作为单个无线网络查看接入点的部署，而不是作为一系列单独的无线设备查看其部署。

6.3.1 什么是集群？

集群是通过产品名称管理作为单个组进行协调的一组接入点。如果您有多个集群且它们有不同的集群“名称”，则它们可以位于同一子网中。

6.3.2 一个集群支持多少个 AP？

目前，对于一个集群中的接入点数量没有硬性限制。经验证测试证明，相同子网上支持十几个或更多接入点。任何时间您都可以在一个集群中包含尽可能多的 AP。

6.3.3 什么类型的 AP 可以形成一个集群？

一个产品名称可以与自己（“包含一个 AP 的集群”）形成集群，也可以与其他产品名称形成集群。要成为同一集群的成员，接入点必须满足以下要求：

- 制造商指定的兼容设备（接入点必须有兼容的设计功能）。
- 采用相同的无线通信配置（均为单射频 AP 或均为双射频 AP）。
- 采用相同的频段配置（均为单频段 AP 或均为双频段 AP）。
- 在相同的 *LAN* 上。

网络上混用 AP 不会对产品名称集群的形成产生负面影响。然而出于管理目的，它有助于了解集群行为：

- 加入集群的接入点必须有相同的名称。有关设置集群名称的更多信息，请参阅第 58 页。
- 其他品牌的接入点不会加入该集群。必须使用 AP 自己关联的管理工具对其进行管理。

6.3.4 协调 AP 与其他集群成员之间是什么关系？

由从集群成员之间选择的 *协调* AP 管理集群配置、配置更新的共享以及加入或离开该组的新 AP 的跟踪。如果协调 AP 不可用，将会向新的集群成员分配协调职责。根据考虑帐户使用时间、集群大小及确定 AP 是否在指定时间最适合于该任务的其他因素的规则集，完全实现此流程的自动化。

无需跟踪或注意那个 AP 是协调 AP，这是因为此状态会随时发生更改，具体取决于集群的需求。在这里提到这一概念，仅仅是因为您会注意到协调 AP 其他集群成员在管理 Web 页面上显示的配置之间略有不同。

6.3.5 哪些设置可以/不可以作为集群配置的组成部分进行共享？

通过产品名称管理 Web 页面定义的大多数配置设置将会作为 *集群配置* 的组成部分应用到其他集群成员。

6.3.5.1 在集群配置中共享的设置

集群配置包括：

- 网络名称 (SSID)。
- 管理员密码。
- 用户帐户和身份验证。
- 无线接口设置。
- 访客欢迎屏幕设置。
- 网络时间协议 (NTP) 设置。
- 射频设置
仅可在集群上同步模式、信道、分段阈值、RTS 阈值和速率设置。信标间隔、DTIM 周期、最大数量工作站和发射功率不形成集群。



注释：启用 *Channel Planning*（信道规划）时，不在集群上同步无线通信信道。请参阅第 76 页的“停止/启动自动信道分配”

- 安全设置。
- *QoS* 队列参数。
- MAC 地址过滤。

6.3.5.2 集群不共享的设置

极少数例外情况（集群接入点之间不共享的设置）如下所示，其中大多数就本质而言必须是唯一的：

- IP 地址。
- MAC 地址。
- 位置描述。
- 负载均衡设置。
- WDS 网桥。
- 以太网（有线）设置。
- 访客接口配置。

必须在各个接入点的管理页面上单独配置不共享的设置。要访问组成当前集群的某个接入点的管理页面，请在当前 AP 的 *Cluster*（集群）> *Access Points*（接入点）页面上，单击 IP Address（IP 地址）链接。

6.3.6 集群的形成

在启用集群的情况下部署第一个 AP 时，形成集群。该 AP 尝试与现有集群会合。如果无法通过相同的集群名称查找子网上的任何其他 AP，则该 AP 会自己建立新的集群。

6.3.7 集群大小和成员资格

目前，对于一个集群中的 AP 数量没有硬性限制。经验证测试证明，相同子网上支持十几个或更多接入点。任何时间您都可以在一个集群中包含尽可能多的 AP。

根据以下条件确定集群成员资格：

- 集群名称 - 具有相同名称的 AP 将加入相同的集群（请参阅第 58 页的“设置集群名称”）。
- 是否启用集群 - 仅启用集群的 AP 才会加入集群（请参阅第 58 页的“开始形成集群”和第 58 页的“停止形成集群”）。

6.3.8 Intra-Cluster 安全

出于易于使用的目的，形成集群的组件旨在让新设备无需经过繁杂的身份验证即可加入集群。但使用安全套接字层 (SSL) 保护集群中接入点之间的所有数据通信不会被随意窃听。前提是假设设备连接的私人有线网络是安全的。在使用 SSL 的接入点之间传输集群配置文件和用户数据库。

6.4 了解接入点设置

Access Points（接入点）选项卡提供有关集群中的所有接入点的信息。在此选项卡上，您可以查看位置描述、MAC 地址、IP 地址，启用（启动）或禁用（关闭）集群接入点，以及删除集群中的接入点。您还可以修改接入点的位置描述。使用 IP 地址链接，可导航至接入点的配置设置及数据。

此页面不显示独立接入点（不属于集群成员的接入点）。

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Manage access points in the cluster

Access Points...

Status: Clustering is online...

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

Stop Clustering

Clustering Options...

Enter the location of this AP.

Location:

Enter the name of the cluster for this AP to join.

Cluster Name:

Update

表 6.1 详细说明了接入点的设置和显示的信息。

表 6.1 接入点设置

字段	描述
<i>Location</i> (位置)	描述接入点的物理位置。
<i>MAC Address</i> (MAC 地址)	<p>接入点的媒体访问控制 (MAC) 地址。</p> <p>MAC 地址是代表网络接口的任何设备的永久性、唯一的硬件地址。MAC 地址由制造商分配。您无法更改 MAC 地址。在这里出于信息目的提供，用作接入点的唯一标识符。</p> <p>此处显示的地址是桥接 (br0) 的 MAC 地址。通过此地址，其他网络便可在外部知道该接入点。</p> <p>要查看 AP 上访客和内部接口的 MAC 地址，请参阅 <i>Status</i> (状态) > <i>Interfaces</i> (接口) 选项卡。</p>
<i>IP Address</i> (IP 地址)	指定接入点的 IP 地址。各个 IP 地址是该接入点的管理 Web 页面的链接。您可以使用该链接导航至特定接入点的管理 Web 页面。它可用于查看特定接入上的数据，从而确保集群成员得知集群配置更改，在特定接入点上配置高级设置，或将独立接入点切换为集群模式。

6.4.1 修改位置描述

要对位置描述进行修改：

1. 导航至 *Cluster*（集群）> *Access Points*（接入点）选项卡。
2. 在 *Clustering Options*（集群选项）部分下的 *Location*（位置）字段中输入该 AP 的新位置。
3. 单击 **Update**（更新）按钮应用更改。

6.4.2 设置集群名称

要设置您希望 AP 加入的集群的名称，请执行以下操作：

1. 导航至 *Cluster*（集群）> *Access Points*（接入点）选项卡。
2. 在 *Clustering Options*（集群选项）部分下的 *Cluster Name*（集群名称）字段中输入新的集群名称。
3. 单击 **Update**（更新）按钮应用更改。



注释：如果希望多个 AP 加入一个特定集群，则所有这些 AP 应在 *Cluster Name*（集群名称）字段指定相同的集群名称。如果集群名称不同，AP 将无法加入该集群。

6.5 开始形成集群

要开始形成集群并将特定的接入点添加到集群，请执行以下操作。

1. 转至独立接入点的管理 Web 页面。（请参阅第 59 页的“在 URL 中使用 AP 的 IP 地址导航至 AP”。）

显示独立接入点的管理 Web 页面。

2. 单击独立接入点的 **Cluster**（集群）> **Access Points**（接入点）选项卡。
3. 单击 **Start Clustering**（开始形成集群）按钮。
该接入点现在为集群成员。它显示在 *Cluster*（集群）> *Access Points*（接入点）选项卡页面上的集群接入点列表中。



注释：在某些情况下，集群可能会不同步。添加接入点至集群后，AP 列表不反映添加的 AP 或显示不完整；请参阅附录 C：“故障排除”中的集群恢复的相关信息。

6.6 停止形成集群

要停止形成集群并删除集群中的特定接入点，请执行以下操作。

1. 转至您想要从集群中删除的接入点的管理 Web 页面。

2. 单击 **Cluster**（集群）> **Access Points**（接入点）选项卡。
3. 单击 **Stop Clustering**（停止形成集群）按钮，从集群中删除该接入点。

将在该接入点的 *Status*（状态）下反映更改；该接入点现在将显示为 **独立**（而不是 **集群**）。



注释：在某些情况下，集群可能会不同步。从集群中删除接入点后，AP 列表仍然反映删除的 AP 或显示不完整，刷新您的浏览器。如果您仍然遇到问题，请参阅附录 C：“故障排除”中的集群恢复的相关信息。

6.7 特定 AP 和管理独立 AP 的配置信息

通常情况下，产品名称专为 **集群** 接入点的集中管理而设计。对于集群中的接入点，集群中的所有接入点反映相同的配置。在这种情况下，您实际连接至哪个接入点进行管理无关紧要。

但可能存在这样的情况，您想要查看或管理特定接入点上的信息。例如，您可能想要查看客户端关联或接入点事件等状态信息。或者，您想要配置和理以 **独立** 模式运行的接入点上的功能。在这些情况下，您可以通过单击 **Access Point**（接入点）选项卡上的 IP 地址链接，导航至接入点的管理 **Web** 界面。

所有集群接入点显示在 *Cluster*（集群）> *Access Points*（接入点）页面中。要导航至集群接入点，您只需单击列表中显示的特定集群成员的 IP 地址。

6.7.1 在 URL 中使用 AP 的 IP 地址导航至 AP

您还可以通过直接在 Web 浏览器地址栏中输入以下形式的 IP 地址，链接到特定接入点的管理 Web 页面：

`http://IPAddressOfAccessPoint`

其中，*IPAddressOfAccessPoint* 是您想要监控或配置的特定接入点的地址。对于独立接入点，这是导航至其配置信息的唯一方式。

6.8 会话监控

产品名称提供实时会话监控信息，包括与特定接入点关联的客户端、数据速率、发射/接收统计数据、信号强度和空闲时间。

6.8.1 导航至会话监控

要查看会话监控信息，单击 **Cluster**（集群）> **Sessions**（会话）选项卡。

图 6.2 会话监控信息

Manage sessions associated with the cluster

Sessions...

You may sort the following table by clicking on any of the column names.

Display

All

Go

User	AP Location	User MAC	Idle	Rate (Mbps)	Signal	Utilization	Rx Total	Tx Total	Error Rate	Idle
Ciara	not set	00:90:4b:93:f4:35	150	54	44	0.1 %	78944	107640	0	150
Sean	not set	00:0c:f1:3e:99:ae	190	11	44	0.4 %	4462	3147	0	190

You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By selecting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

Clustered

1 Access Points

0 User Accounts

6.8.2 了解会话监控信息

Sessions（会话）页面显示与集群中的接入点相关联的客户端工作站的信息。通过用户名和用户 *MAC* 地址，以及当前连接的 *AP*（地址）识别各个客户端。

要查看客户端会话的特定统计数据，从 *Display*（显示）下拉列表中选择一个项目，并单击 **Go**（执行）。您可以查看 *Idle Time*（空闲时间）、*Data Rate*（数据速率）、*Signal*（信号）、*Utilization*（利用率）等信息；第 61 页的表 6.2 中详细介绍了所有这些字段。

在本文中，“会话”是指用户在具有唯一 *MAC* 地址的客户端设备（工作站）上保持与无线网络的连接的时间段。客户端登录到网络时，会话开始；客端故意注销或出于某些其他原因丢失连接时，会话结束。



注释： 会话与关联不同，关联是指客户端连接到某个特定的接入点。客户端网络连接可以从一个集群 *AP* 移动到同一会话中的另一个集群 *AP*。可以在 *AP* 之间游客户端工作站并保留会话。
有关监控关联和链接完整性监控的信息，请参阅第 127 页的“关联的无线客户端”。

表 6.2 会话信息

字段	描述
User Name (用户名)	表示 IEEE 802.1x 客户端的用户名。 注： 此字段仅与使用 IEEE 802.1x 安全模式的 AP 和本地身份验证服务器的客户端关联。(有关此模式的更多信息，请参阅第 106 页的“IEEE 802.1x”。) 对于使用具有 RADIUS 服务器的 IEEE 802.1x 或其他安全模式，则此处不显示任何用户名。
AP Location (AP 位置)	表示接入点的位置。 此位置来源于在 Basic Settings（基本设置）选项卡上指定的位置描述。
User MAC Address (用户 MAC 地址)	表示用户的客户端设备（工作站）的 MAC 地址。 MAC 地址是唯一标识网络各节点的硬件地址。
Idle Time (空闲时间)	表示此工作站处于不活动状态的时间量。 工作站不收发数据时，会被视为“空闲”。
Data Rate (数据速率)	此接入点传输数据至指定客户端的速度。 以兆位/秒(Mbps) 为单位测量数据传输速率。 在接入点上使用时，此值应在为 IEEE 802.1x 模式设置的宣传速率范围内。例如，802.11a 的数据速率为 6 到 54Mbps。
Signal（信号）	表示客户端从接入点接收的射频 (RF) 信号的强度。 用于此的测量方法是被称为接收信号强度指示 (RSSI) 的 IEEE 802.1x 值，该值范围介于 0 和 100 之间。 通过在客户端工作站的网络接口卡 (NIC) 上实施的 IEEE 802.1x 机制来确定 RSSI。
Utilization (利用率)	此工作站的利用率。 例如，如果工作站处于“活动”（收发数据）状态的时间占 90%，不活动的时间占 10%，则“利用率”为 90%。
Receive Total (接收总包数)	表示当前会话期间客户端接收到的总包数。
Transmit Total (发射总包数)	表示此会话期间发射至客户端的总包数。
Error Rate (错误率)	表示在此接入点上传输时，掉落的时间帧百分比。

6.8.3 查看接入点的会话信息

您可以同时查看网络上所有接入点的会话信息，或设置为显示从屏幕顶部的下拉菜单中选择的指定接入点的会话信息。

要查看所有接入点的信息，选择页面顶部的 **Show all access points** （显示所有接入点）单选按钮。

要查看特定接入点的信息，选择 **Show only this access point** （仅显示此接入点）单选按钮，并从下拉菜单中选择该接入点的名称。

6.8.4 对会话信息进行排序

要按照特定指示符对表格中显示的信息进行排序，则单击您想要对其进行排序的列标签。例如，如果要查看按利用率排序的表格行，单击 **Utilization** （利用率）列标签。将按利用率对条目进行排序。

6.8.5 刷新会话信息

通过单击 **Refresh** （刷新）按钮，可以更新 *Session Monitoring* （会话监控）页面上显示的信息。

管理用户帐户

7

7.1 概述	65
7.2 导航至用户管理	65
7.2.1 查看用户帐户	66
7.2.2 添加用户	67
7.2.3 编辑用户帐户	68
7.2.4 启用和禁用用户帐户	68
7.2.5 启用用户帐户	68
7.2.6 禁用用户帐户	68
7.2.7 删除用户帐户	69
7.3 备份和还原用户数据库	69
7.3.1 备份用户数据库	69
7.3.2 从备份文件还原用户数据库	69

7.1 概述

产品名称包括可用于控制接入点的客户端访问权限的用户管理功能。

用户管理和身份验证必须始终与以下两种安全模式结合使用，它们要求使用 **RADIUS** 服务器进行用户身份验证和管理。

- IEEE 802.1x 模式（请参阅第 106 页的“IEEE 802.1x”中的第 10 章：“配置安全性”）。
- 带 RADIUS 的 WPA 模式（请参阅第 112 页的“WPA Enterprise（WPA 企业版）”中的第 10 章：“配置安全性”）。

您可以选择使用产品名称中嵌入的内部 **RADIUS** 服务器或您提供的外部 **RADIUS** 服务器。如果您使用嵌入式 **RADIUS** 服务器，使用接入点上的管理 Web 页面即可设置并管理用户帐户。果您使用的是外部 **RADIUS** 服务器，需要在该服务器的管理界面上设置并管理用户帐户。

在 **User Management**（用户管理）页面上，您可以创建、编辑、删除和查看客户端的 *用户帐户*。每个用户帐户都是由用户名和密码组成。在这里指定的用户组代表得到批准可登录并使用一个或多个接入点，通过您的无线网络访问本地（也可能外部）网络的 *客户端*。



注释：在这里指定的用户是使用 AP 作为连接中心的接入点客户端，而不是无线网络管理员。只有那些具有管理员用户名和密码并知道管理 URL 的客户端可以为管理员登录，并查看或修改配置。

7.2 导航至用户管理

要设置或修改用户帐户，单击 **User Management**（用户管理）选项卡。

图 7.1 管理用户帐户

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Manage user accounts

User Accounts...

0 User Accounts

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

☐ Edit

Username

Real name

Status

Selected users:

Enable

Disable

Remove

[\[backup or restore the user database\]](#)

Add a user...

To add a user, fill in the fields below and click: "Add Account".

Username

Real name

Password

Password (again for safety)

Cancel

Add Account

7.2.1 查看用户帐户

用户帐户显示在屏幕顶部的 *User Accounts...*（用户帐户...）下面，显示了用户的 Username（用户名）、Real name（真实姓名）和 Status（状态）（启用或禁用）。您先选中用户名旁的复选框，然后选择一项操作，即可对现有的用户帐户进行修改。（请参阅第 68 页的“编辑用户帐户”。）

66 Psion Teklogix 9160 G2 无线网关用户手册

7.2.2 添加用户

要创建新用户，请执行以下操作：

- 1. 在 *Add a User...*（添加用户...）下，在以下字段中提供信息。

表 7.1 新用户字段

字段	描述
<i>Username</i> (用户名)	提供用户名。 用户名是限长 237 个字符的字母数字字符串。请勿使用特殊字符或空格。
<i>Real name</i> (真实姓名)	仅作信息用途，请提供用户的全名。 真实姓名限制在 256 个字符之内。
<i>Password</i> (密码)	指定此用户的密码。 密码是限长 256 个字符的字母数字字符串。请勿使用特殊字符或空格。

- 2. 填充这些字段后，单击 **Add Account**（添加帐户）以添加帐户。

然后，新用户显示在 *User Accounts...*（用户帐户...）中。第一次创建用户帐户时，默认情况下该用户帐户为*启用*状态。



注释: *Administration*（管理）用户界面限制每个接入点 100 个用户帐户。网络使用可能实施更实际的限制，具体取决于用户的需求。

7.2.3 编辑用户帐户

创建用户帐户后，它会显示在 *User Management*（用户管理）管理 Web 页面顶部的 *User Accounts...*（用户帐户...）下方。要对现有的用户帐户进行修改，先单击用户名旁的复选框以选中该框。

User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions. **Note:** These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

<input type="checkbox"/>	Edit	Username	Real name	Status
<input type="checkbox"/>	[Edit]	Engineer	Mary SMith	enabled
<input type="checkbox"/>	[Edit]	Manager	Tom Jones	enabled
<input type="checkbox"/>	[Edit]	Tester	Joe Bloggs	enabled

Selected users: Enable Disable Remove

[\[backup or restore the user database\]](#)

然后，选择一项操作，例如 **Edit**（编辑）、**Enable**（启用）、**Disable**（禁用）或 **Remove**（删除）。

7.2.4 启用和禁用用户帐户

必须启用用户帐户，该用户才能作为客户端登录并使用接入点。

您可以**启用**或**禁用**任何用户帐户。使用此功能，您可以维护一组用户帐户并授权或阻止用户访问网络，且无需删除或重新创建帐户。用户偶尔需要访问网络时，此功能可以派上用场了。例如，断断续续而非定期为贵公司工作的承包商有时可能需要获得 3 个月的网络访问权限，然后离开 3 个月，分配了另一项任务又回来工作。您可以根据需要启用并禁用这些用户帐户，并酌情控制访问。

7.2.5 启用用户帐户

要启用某个用户帐户，请单击用户名旁的复选框并单击 **Enable**（启用）。帐户已启用的用户可以作为客户端登录到您网络中的无线接入点。

7.2.6 禁用用户帐户

要禁用某个用户帐户，请单击用户名旁的复选框并单击 **Disable**（禁用）。

帐户已禁用的用户无法作为客户端登录到您网络中的无线接入点。但是，该用户保留在数据库中，可在稍后需要时启用。

7.2.7 删除用户帐户

要删除某个用户帐户，请单击用户名旁的复选框并单击 **Remove**（删除）。

如果您认为自己需要在稍后的时间重新添加此用户，可考虑禁用该用户，而不是删除帐户。

7.3 备份和还原用户数据库

您可以将当前用户帐户组的副本保存在备份配置文件中。可以在稍后的时间使用该备份文件，将 AP 上的用户帐户还原为之前保存的配置。

7.3.1 备份用户数据库

要创建此接入点的用户帐户的备份副本：

1. 单击 **[backup or restore the user database]**（备份或还原用户数据库）链接。

将显示 *File Download or Open*（下载或打开文件）对话框。

2. 在第一个对话框中，选择 **Save**（保存）选项。

将显示文件浏览器。

使用文件浏览器导航至您想要保存该文件的目录，然后单击 **OK**（确定）保存文件。

您可以保留默认的文件名 (wirelessUsers.ubk) 或重命名该备份文件，但务必使用 .ubk 扩展名保存文件。

7.3.2 从备份文件还原用户数据库

要从备份文件还原用户数据库，请执行以下操作：

1. 通过在 **Restore**（还原）字段中输入完整路径和文件名，或单击 **Browse**（浏览）并选择该文件，选择您想要使用的备份配置文件。

（只有那些使用用户数据库备份功能创建并另存为 .ubk 备份配置文件的文件才能使用还原功能，例如 wirelessUsers.ubk。）

2. 单击 **Restore**（还原）按钮。

备份还原过程完成后，会显示一条消息，表明用户数据库已成功还原。（此过程并不耗时，还原几乎是立即完成的。）

单击 **User Management**（用户管理）选项卡，查看还原的用户帐户。

8.1 导航至信道管理	73
8.2 了解信道管理	73
8.2.1 工作原理概述	73
8.2.2 了解有关重叠信道的更多信息	74
8.2.3 示例：信道管理前后的网络	74
8.3 配置和查看信道管理设置	75
8.3.1 停止/启动自动信道分配	76
8.3.2 查看当前的信道分配和设置锁定	76
8.3.3 查看上次建议的信道组更改	77
8.3.4 配置高级设置（自定义/安排信道计划）	77

8.1 导航至信道管理

要查看会话监控信息，请单击 **Cluster**（集群）> **Channel Management**（信道管理）选项卡。

图 8.1 管理信道分配

The screenshot displays the 'Channel Management' interface. On the left is a sidebar menu with options: Basic Settings, User Management, Cluster, Access Points, Sessions, Channel Management (selected), Wireless Neighborhood, Security, Status, Interfaces, Events, Transmit/Receive, Client Associations, Neighboring Access Points, Manage, Ethernet Settings, 802.11 Settings, and 802.11 Advanced Settings.

The main content area is titled 'Automatically manage channel assignments'. It includes a 'Channels ...' section with a 'Start' button and the text 'automatically re-assigning channels'. Below this is a table for 'Current Channel Assignments' with columns: IP Address, Radio, Band, Channel, and Locked. The table lists two entries: 10.10.100.238 (Radio: 00:0C:41:16:A3:12, Band: G, Channel: 2) and 10.10.100.245 (Radio: 00:00:04:7F:00:00, Band: G, Channel: 3). An 'Apply' button is at the bottom right of the table.

On the right side, there are three status boxes: 'Clustered' with a radio icon, '2 Access Points' with a group of people icon, and '3 User Accounts' with a group of people icon.

Below the current assignments is a section for 'Proposed Channel Assignments (3 hours, 40 minutes and 52 seconds old)' with a table showing IP Address, Radio, and Proposed Channel. It lists one entry: 10.10.100.238 (Radio: 00:0C:41:16:A3:12, Proposed Channel: 2).

At the bottom is an 'Advanced' section with two settings: 'Change channels if interference is reduced by at least 5%' (with a dropdown arrow) and 'Determine if there is better set of channel settings every 1 Minute' (with a dropdown arrow). An 'Update' button is at the bottom right of this section.

8.2 了解信道管理

启用 *信道管理* 后，产品名称会自动分配集群接入点使用的无线电信道，以减少相互干扰（或对集群外部其他接入点的干扰）。这样，便可最大程度提高 Wi-Fi 带宽，并帮助维持无线网络通信的效率。

（您必须启动信道管理才能进行信道的自动分配，在新的 AP 上，默认情况下禁用此功能。请参阅第 76 页的“停止/启动自动信道分配”。）

8.2.1 工作原理概述

在指定时间间隔（默认值为 **1 小时**）或需要时（单击 **Update**（更新）），信道管理器会将 AP 映射到信道使用，并测量集群中的干扰水平。如果发现信道干扰严重，信道管理器会根据效率算法（或 *自动信道计划*），将一些或所有 AP 重新分配至新的信道。

8.2.2 了解有关重叠信道的更多信息

射频 (RF) 广播信道定义接入点上射频用于收发无线电信号的射频频谱部分。接入点可用的信道范围由接入点的 **IEEE 802.11** 模式（也称为频段）确定。

IEEE 802.11b/802.11g 模式 (802.11 b/g) 支持使用信道 1 至 11（两者也包括在内），而 **IEEE 802.11a** 模式支持使用更大范围的非连续信道（36、40、44、48、52、56、60、64、149、153、157、161、165）。

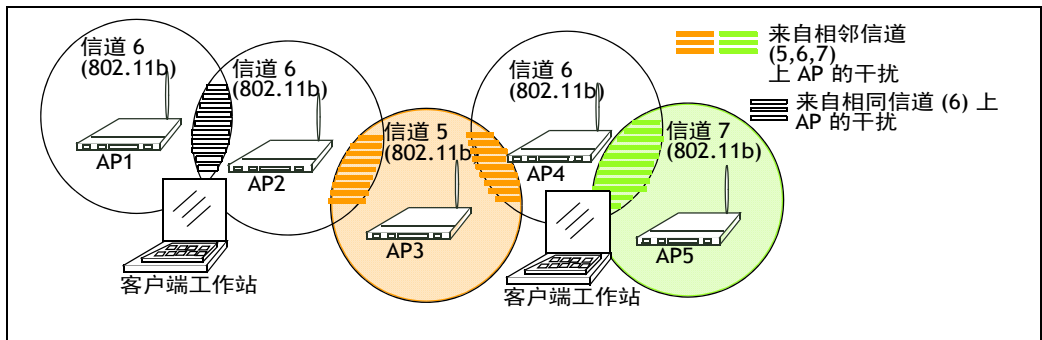
当位于彼此范围内的多个接入点在相同或重叠信道上广播时，会发生干扰。在大量数据和媒体流量争用带宽的繁忙时段，此干扰对于网络性能的影响是非常大的。

信道管理器将检测集群 AP 所在的频段（b/g 或 a），并使用预先确定的互不干扰的信道集合。对于“b/g”无线电频段，常用的一组非干扰信道为 1、6、11。信道 1、4、8、11 产生的重叠最小。类似的一组非干扰信道用于“a”无线电频段，这包括用于该模式的所有信道，因为它们不会产生重叠。

8.2.3 示例：信道管理前后的网络

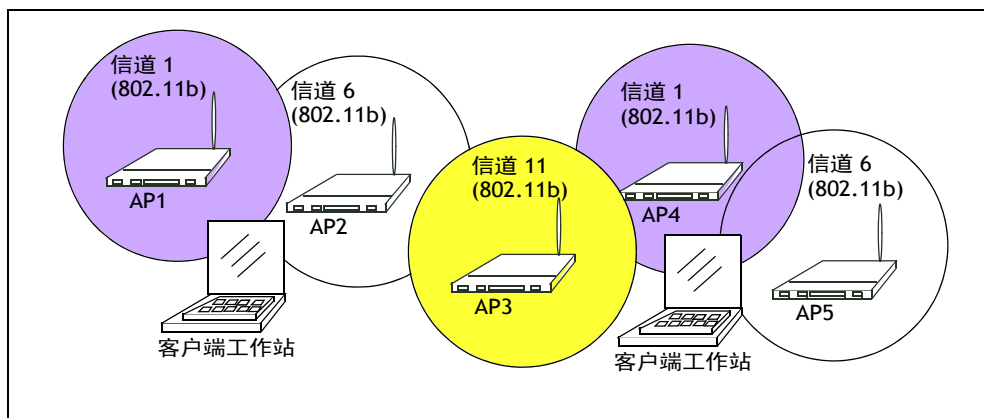
如果不使用自动信道管理功能，则可以在连续信道上向集群 AP 分配信道，而这样将会产生重叠并导致干扰。例如，AP1 可以分配给信道 6，AP2 分配给信道 6，AP3 分配给信道 5，如图 8.2 中所示。

图 8.2 不使用自动信道管理功能



使用自动信道管理功能时，集群中的 AP 会自动重新分配到非干扰信道，如 8.3 中所示。

图 8.3 启用信道管理时



8.3 配置和查看信道管理设置

Channel Management（信道管理）页面显示集群接入点之前、当前和计划的信道分配。默认情况下，禁用自动信道分配功能。您可以启用信道管理，以优化程时间间隔内该集群上信道的使用情况。

在此页面上，您可以查看集群中所有 AP 的信道分配，停止/启用自动信道管理，并手动“更新”当前的信道映射（AP 至信道）。手动更新时，信道管理器将评估信道的使用情况，如有必要，会根据当前的高级设置重新分配 AP 到新的信道，以减少干扰。

使用高级设置，您可以修改触发信道重新分配的干扰抑制电位，更改自动更新的时间表，并重新配置用于分配的信道集。

以下小节介绍了如何在您的网络上配置和使用信道管理：

- 第 76 页的“停止/启动自动信道分配”。
- 第 76 页的“查看当前的信道分配和设置锁定”。
- 第 77 页的“更新当前信道设置（手动）”。
- 第 77 页的“查看上次建议的信道组更改”。
- 第 77 页的“配置高级设置（自定义/安排信道计划）”。
- 第 79 页的“更新高级设置”。

8.3.1 停止/启动自动信道分配

默认情况下，禁用（关闭）自动信道分配功能。

- 单击 **Start**（启动）恢复自动信道分配。启用自动信道分配后，信道管理器会定期映射集群接入点使用的无线电信道，而且在必要时会重新分配集群 AP 上的信道以减少对集群成员或集群外部其他 AP 的干扰。



注释：信道管理器会覆盖默认的集群行为，以同步集群上所有 AP 的无线电信道。启用信道管理后，集群上的无线电信道不同步到其他 AP。请参阅第 55 页的“在集群配置中共享的设置”中“射频设置”下的注释。

- 单击 **Stop**（停止）以停止自动信道分配。（将不会创建信道使用图或进行信道的重新分配。仅手动更新会影响信道分配。）

8.3.2 查看当前的信道分配和设置锁定

当前信道设置按 IP 地址显示集群的所有接入点的列表。显示屏显示各 AP 广播的频段，各个 AP 使用的当前信道，以及“锁定”当前无线电信道上某个 AP 使其无法重新分配至另一个信道的选项。下表提供了当前信道设置的详细信息。

表 8.1 当前信道设置

字段	描述
<i>IP Address</i> (IP 地址)	指定接入点的 IP 地址 。
<i>Radio</i> （射频）	表示接入点的 MAC 地址。
<i>Band</i> （频段）	表示接入点广播的频段（b/g 或 a）。
<i>Channel</i> （信道）	表示此接入点当前正在上面广播的无线电 信道 。
<i>Locked</i> （锁定）	<p>如果您希望此接入点保留在当前信道上，单击 Locked（锁定）。</p> <p>对某个接入点勾选（启用）“Locked”（锁定）复选框后，作为优化策略的一部分，自动信道管理计划不会将该 AP 重新分配至另一个信道。使用锁定信道的 AP 将计入该计划的要求。</p> <p>单击 Update（更新）后，您将看到锁定的 AP 为“Current Channel”（当前信道）和“Proposed Channel”（建议信道）显示相同的信道。锁定的 AP 将保留其当前信道。</p>

8.3.2.1 更新当前信道设置（手动）

您可以通过单击 *Current Channel Settings*（当前信道设置）屏幕下方的 **Update**（更新）来运行手动信道管理更新。

8.3.3 查看上次建议的信道组更改

Last Proposed Set of Channel Changes（上次建议的信道组更改）显示上次的信道计划。该计划按 IP 地址列出了集群的所有接入点，并显示各 AP 当前的信道和建议的信道。锁定的信道无重新分配，AP 之间信道分布的优化将考虑到锁定 AP 必须保留在当前信道上这一事实。未“锁定”的 AP 可分配到先前所使用信道以外的信道，具体取于计划的结果。

表 8.2 AP 的信道计划

字段	描述
<i>IP Address</i> (IP 地址)	指定接入点的 IP 地址 。
<i>Current</i> (当前)	表示此接入点当前正在上面广播的无线电信道。
<i>Proposed</i> (建议)	表示执行信道计划时将此接入点重新分配到的无线电信道。

8.3.4 配置高级设置（自定义/安排信道计划）

如果您按所提供的设置使用 *Channel Management*（信道管理）（在不更新 *Advanced Settings*（高级设置）的情况下），如果干扰减少了 25% 或更多，信道会每小时自动微调一次。即使网络繁忙，也会重新分配信道。将使用相应的信道集（对使用 IEEE 802.11b/g 的 AP，为“b/g”；对于使用 IEEE 802.11a 的 AP，为“a”）。

这些默认设置旨在满足您需要实施信道管理的大多数场景。

您可使用 *高级设置* 修改触发信道重新分配的干扰抑制电位，更改自动更新的时间表，并重新配置用于分配的信道集。

表 8.3 高级设置

字段	描述
<i>Advanced</i> (高级)	单击“Advanced”（高级）切换开关可显示/隐藏修改定时和信道规划算法详情的显示设置。默认情况下，这些设置是 隐藏的 。
<i>Change channels if interference is reduced by at least __ (干扰降低至少 __ 时更改信道)</i>	<p>指定建议的计划为了得到应用而必须实现的最低干扰抑制百分比。默认设置为 25%。</p> <p>使用下拉菜单，选择介于 25% 至 75% 范围内的百分比。</p> <p>此设置允许您设置信道重新分配的控制因素，以便网络不会被持续扰乱，从而实现效率的最小增益。</p> <p>例如，如果信道干扰必须降低 75%，则建议的信道分配只会将干扰降低 30%，且信道不会被重新分配。但是如果您将信道干扰的最小优势重置为 25% 并单击 Update（更新），将实施建议的信道计划并根据需要重新分配信道。</p>
<i>Determine if there is better set of channel settings every __ (每隔 __ 确定是否有更好的一组信道设置)</i>	<p>使用下拉菜单指定自动更新的时间表。</p> <p>提供一系列时间间隔，从“1 分钟”到“6 个月”。默认设置为“1 小时”（每 1 小时重新评估信道的使用情况并应用生成的信道计划）。</p>
<i>Use these channels when applying channel assignments (应用信道分配时使用这些信道)</i>	<p>选择特定频段上的一组非干扰信道（“b/g”或“a”）。选项包括：</p> <ul style="list-style-type: none">• b/g 信道 1-6-11• b/g 信道 1-4-8-11• a <p>IEEE 802.11b/802.11g 模式 (802.11 b/g) 支持使用信道 1 至 11。对于“b/g”无线电频段，常用的一组非干扰信道为 1、6、11。</p> <p>信道 1、4、8、11 产生的重叠最小。</p> <p>IEEE 802.11a 模式支持使用更大范围的非连续信道（36、40、44、48、52、56、60、64、149、153、157、161、165）。所有“a”频段信道均为非干扰信道。</p>
<i>Apply channel modifications even when the network is busy (即使网络繁忙时，仍然应用信道修改)</i>	<p>单击以启用或禁用此设置。</p> <p>勾号表示已启用，且即使网络繁忙时仍然应用信道修改。如果未选中，则不会在繁忙网络上应用信道修改。</p> <p>此设置（和干扰抑制设置）旨在帮助权衡在繁忙时段就可能给客户造成的固有中断情况重新分配信道给网络性能带来的成本/收益影响。</p>

8.3.4.1 更新高级设置

单击 *Advanced Settings*（高级设置）下方的 **Update**（更新），应用这些设置。应用后，高级设置将会生效，并会影响自动信道管理的方式。（自动和手动更新时，将会考虑新的干扰抑制最小值、安排的微调时间间隔、信道集以网络繁忙设置。）

无线邻居

9

9.1 导航至无线邻居	83
9.2 了解无线邻居的信息	84
9.3 查看无线邻居	84
9.4 查看集群成员的详细信息	86

Wireless Neighborhood（无线邻居）屏幕显示该集群任何接入点范围内的接入点。此页面提供相邻接入点的详细视图，包括各个接入点的识别信息（SSID 和 MAC 地址）、集群状态（成员和非成员）以及统计数据信息，例如广播各个 AP 的信道、信号强度等。

9.1 导航至无线邻居

要查看 *Wireless Neighborhood*（无线邻居），请单击 **Cluster**（集群）> **Wireless Neighborhood**（无线邻居）选项卡。

图 9.1 集群和非集群中的相邻 AP

View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ☐ In cluster ☐ Not in cluster ☒ Both

	Cluster	
	10.10.100.245 00:00:04:7F:00:00 (Vicky's Office - lower shelf)	10.10.100.238 00:0C:41:16:A3:12 (Vicky's Office - top shelf)
Neighbors (11)		
Vicky's AP-2 (WIP-bld-48b)		54
Vicky's AP-2 (WIP-bld-48b)	73	
OMEGA_NAS	29	46
TEKLOGIX...	20	
novatec	23	
Pronghorn 2.0.2		11
tsunami	18	
tsunami	70	41
Radio 1 - SSID 1	36	41
BradLabNetwork	5	19
Ray's GW 7001 2.0.3		11

Clustered

2 Access Points

3 User Accounts

Wireless Neighborhood shows those access points within range of any access point in the cluster.

This page provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each AP is broadcasting on, signal strength, and so forth.

[More ...](#)

9.2 了解无线邻居的信息

Wireless Neighborhood（无线邻居）视图显示集群各成员范围内的所有接入点，显示哪些接入点在集群成员范围内，并区分集群成员和非成员。

对于各个相邻接入点，*Wireless Neighborhood*（无线邻居）视图识别信息（**SSID** 或网络名称、**IP 地址**、**MAC** 地址）以及射频统计数据（信号强度、信道、信标间隔）。您可以单击某个 AP，获取当前选择 AP 的射频范围内 AP 的其他统计数据。

Wireless Neighborhood（无线邻居）视图可以帮助您：

- 在无线区域内检测并查找非预期（或非法）接入点，以便能够采取措施来限制相关风险。
- 确认预期覆盖范围 通过接入在其他 AP 的信号强度可见的 AP，您可以确认部署是否符合您的规划目标。
- 检测故障。在以颜色编码的表格内，覆盖范围图形的任何非预期更改一目了然。

9.3 查看无线邻居

下表列出了无线邻居的详细信息。

表 9.1 无线邻居统计数据

字段	描述
<i>Display Neighboring APs</i> （显示相邻 AP）	单击以下任何一个单选按钮来更改视图： <ul style="list-style-type: none">• <i>In cluster</i>（集群成员）— 仅显示作为集群成员的相邻 AP。• <i>Not in cluster</i>（非集群成员）— 仅显示非集群成员的相邻 AP。• <i>Both</i>（两者兼具）— 显示所有相邻 AP（集群成员和非集群成员）。
<i>Cluster</i> （集群）	表格顶部的“Cluster”（集群）列表显示集群中所有接入点的 IP 地址。（它与第 53 页的“导航至接入点管理”中所述的 <i>Cluster</i> （集群）> <i>Access Points</i> （接入点）上显示的集群成员列表相同。） 如果集群中只有一个 AP，则这里只显示一个 IP 地址栏；表示该 AP “与自己形成集群”。 您可以单击一个 IP 地址，查看特定 AP 的更多详情，具体如第 86 页的图 9.2 中所示。

表 9.1 无线邻居统计数据 （续）

字段	描述																																												
Neighbors (邻居)	<p>在左侧栏中由 SSID（网络名称）列出的是一个或多个集群 AP 邻居的接入点。被探测为集群成员邻居的接入点本身也可以是集群成员。列表顶部始终显同样是集群成员的邻居，同时还在上方显示颜色条并包含位置指示器。</p> <p>Neighbors（邻居）列表中各 AP 右侧的彩色条显示每个相邻 AP 的信号强度，此强度是由 IP 地址显示在该列顶部的集群成员检测到的。</p> <p>此 AP（集群成员）对 IP 地址为 10.10.100.246 的 AP 可见（信号强度为 54）...</p> <p>... 但对地址为 10.10.100.223 的 AP 不可见</p> <table><tr><th>Neighbors (88)</th><th>10.10.100.246 (not set)</th><th>10.10.100.223 (not set)</th><th>10.10.100.213 (not set)</th></tr><tr><td>TEKLOGIX... (not set)</td><td></td><td>2</td><td>48</td></tr><tr><td>TEKLOGIX... (not set)</td><td></td><td></td><td></td></tr><tr><td>TEKLOGIX... (not set)</td><td>54</td><td>0</td><td></td></tr><tr><td>TEKLOGIX... (not set)</td><td>34</td><td>5</td><td>26</td></tr><tr><td>TEKLOGIX... (not set)</td><td>22</td><td></td><td>50</td></tr><tr><td>Brad Lab 10S</td><td>20</td><td>18</td><td>27</td></tr><tr><td>wi-fi-a</td><td>46</td><td></td><td>34</td></tr><tr><td>guest</td><td>4</td><td>6</td><td>48</td></tr><tr><td>int</td><td>4</td><td>5</td><td>48</td></tr><tr><td>g10_wgt624_guest</td><td>21</td><td>14</td><td>33</td></tr></table> <ul style="list-style-type: none">• 深蓝条 — 深蓝条和较高的信号强度数字（例如 50）表示 IP 地址显示在该列顶部的 AP 所检测到的邻居的信号强度良好。• 浅蓝条 — 浅蓝条和较低信号强度数字（例如 20 或更低）表示 IP 地址显示在该列顶部的 AP 所检测到的邻居的信号强度一般或较弱。• 白色条 — 白色条和数字 0 表示其中一个集群成员检测到的相邻 AP 无法被 IP 地址显示在该列顶部的 AP 检测到。• 浅灰条 — 浅灰条和无信号强度数字表示由其他集群成员而非 IP 地址显示在该列顶部的 AP 检测到邻居。• 深灰条 — 深灰条和无信号强度数字表示这是 IP 地址显示在该列顶部的 AP（因为它不适用于显示 AP 对自身的检测情况）。	Neighbors (88)	10.10.100.246 (not set)	10.10.100.223 (not set)	10.10.100.213 (not set)	TEKLOGIX... (not set)		2	48	TEKLOGIX... (not set)				TEKLOGIX... (not set)	54	0		TEKLOGIX... (not set)	34	5	26	TEKLOGIX... (not set)	22		50	Brad Lab 10S	20	18	27	wi-fi-a	46		34	guest	4	6	48	int	4	5	48	g10_wgt624_guest	21	14	33
Neighbors (88)	10.10.100.246 (not set)	10.10.100.223 (not set)	10.10.100.213 (not set)																																										
TEKLOGIX... (not set)		2	48																																										
TEKLOGIX... (not set)																																													
TEKLOGIX... (not set)	54	0																																											
TEKLOGIX... (not set)	34	5	26																																										
TEKLOGIX... (not set)	22		50																																										
Brad Lab 10S	20	18	27																																										
wi-fi-a	46		34																																										
guest	4	6	48																																										
int	4	5	48																																										
g10_wgt624_guest	21	14	33																																										

9.4 查看集群成员的详细信息

要查看集群成员 AP 的详细信息，请在页面顶部点击集群成员的 IP address（IP 地址）。

图 9.2 集群成员 AP 的详细信息

View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ☐ In cluster ☐ Not in cluster ☒ Both

Cluster

10.10.100.245
00:00:04:7F:00:00
(Vicky's Office - lower shelf)

10.10.100.238
00:0C:41:16:A3:12
(Vicky's Office - top shelf)

Neighbors (10)

Vicky's Network (WIP-bld-48b)		45
Vicky's Network (WIP-bld-48b)	51	
IOMEGA_NAS	37	49
TEKLOGIX...	22	
novatec		
Pronghorn 2.0.2		20
tsunami	18	10
tsunami	54	42
BradLabNetwork	11	
Ray's GW 7001 2.0.3		17

Neighbor Details

10.10.100.245

SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
IOMEGA_NAS	00:03:2F:27:4E:EE	1	10	37	100	74203
TEKLOGIX...	00:0C:41:0A:30:3E	6	10	22	100	74203
Vicky's Network (WIP-bld-48b)	00:0C:41:16:A3:12	2	10	51	100	74203
novatec	00:0E:81:01:01:1A	6	10	-4	100	74203
tsunami	00:13:5F:56:E8:00	10	10	18	100	74203
tsunami	00:14:A8:36:28:40	4	10	54	100	74203

Clustered

2 Access Points

3 User Accounts

下表说明了所选 AP 的详细信息。

表 9.2 接入点统计数据

字段	描述
SSID	<p>接入点的<i>服务集标识符(SSID)</i>。</p> <p>SSID 是限长 32 个字符的字母数字字符串，唯一地标识无线局域网。它也被称为<i>网络名称</i>。</p> <p>在 Basic Settings（基本设置）(第 5 章：“配置基本设置”)或 Manage（管理）> 802.11 Settings（802.11 设置）(第 13 章：“设置无线接口”)中设置 SSID。</p> <p>在同一接入点上运行的访客网络和内部网络始终必须具有两个不同的网络名称。</p>
MAC Address (MAC 地址)	<p>显示相邻接入点的 MAC 地址。</p> <p>MAC 地址是唯一标识网络各节点的硬件地址。</p>
Channel (信道)	<p>显示接入点当前广播所在的信道。</p> <p>信道定义了用于收发射频的射频频谱部分。</p> <p>在 Manage（管理）> 802.11 Advanced Settings（802.11 高级设置）中设置信道。 (请参阅 第 16 章：“配置 802.11 射频设置”。)</p>
Rate (速率)	<p>显示此接入点当前发射的速率（兆位/秒）。</p> <p>当前速率始终是 Supported Rates（支持速率）中所显示的速率之一。</p>
Signal (信号)	<p>表示此接入点发射的射频信号强度，以分贝 (Db) 为单位进行测量。</p>
Beacon Interval (信标间隔)	<p>显示此接入点使用的 信标间隔。</p> <p>接入点每隔一定时间就会发射信标帧，表示存在无线网络。默认行为是每 100 毫秒发送一个信标帧（或每秒发送 10 个信标帧）。</p> <p>在 Manage（管理）> 802.11 Advanced Settings（802.11 高级设置）上设置信标间隔。（请参阅 第 16 章：“配置 802.11 射频设置”。）</p>
Capability (功能)	<p>当转化为二进制时，十六进制数字表示每个 IEEE 802.11 的特性或功能，以及其在该接入点上是“打开”还是“关闭”。</p>
Beacon Age (信标时间)	<p>显示从接入点发射最近信标的日期和时间。</p>

10.1 了解无线网络的安全问题	91
10.1.1 如何知道使用的是哪一种安全模式?	91
10.1.2 比较安全模式的密钥管理、身份验证及加密算法	92
10.1.2.1 何时使用未加密（无安全性）	92
10.1.2.2 何时使用静态 WEP	93
10.1.2.3 何时使用 IEEE 802.1x	94
10.1.2.4 何时使用 WPA 个人版	95
10.1.2.5 何时使用 WPA 企业版	96
10.1.3 是否禁止了广播 SSID 增强安全性?	97
10.1.4 如何通过站点隔离保护网络?	97
10.2 配置安全设置	98
10.2.1 广播 SSID、站点隔离和安全模式	98
10.2.2 安全模式	100
10.2.2.1 None (Plain-text)（无（纯文本））	100
10.2.2.2 Static WEP（静态 WEP）	101
10.2.2.3 IEEE 802.1x	106
10.2.2.4 WPA Personal（WPA 个人版）	109
10.2.2.5 WPA Enterprise（WPA 企业版）	112
10.3 更新设置	116

以下小节介绍如何在产品名称上配置安全性设置。

10.1 了解无线网络的安全问题

从本质上来说，无线媒介比有线媒介的安全性低些。例如，以太网 **NIC** 通过物理介质如同轴电缆或双绞线传输数据包。无线 **NIC** 以无线方式传播无线通信信号，不必使用物理访问方式或高级设备即可轻松连接无线 LAN。黑客只需一台便携式计算机，配备无线 **NIC**，并具备点知识，就能轻松攻击您的无线网络，他甚至不需要在接入点的常规范围内。黑客在客户端使用一精密天线，就可以从数英里以外的地方连接到该网络。

产品名称提供大量身份验证和加密方法，确保只有预定的用户才能访问您的无线基础设施。以下各节中对各种安全模式进行了详细的介绍。

您还可参阅相关主题：附录 B：“无线客户端/RADIUS 服务器上的安全设置”。

10.1.1 如何知道使用的是哪一种安全模式？

一般来说，我们建议在内部网络上使用在环境下可行的最可靠安全模式。在接入点上配置安全性时，首先必须选择安全模式，然后在某些模式下选择种身份验证算法，以及是否允许客户端不使用指定的安全模式与之关联。

拥有 *远程身份验证拨入用户服务 (RADIUS)* 的 *Wi-Fi 受保护访问 (WPA)* 使用 **CCMP (AES)** 加密算法提供可用的最佳数据保护，如果所有客户端工作站均安装了 **WPA Supplicant**，无疑 **CCMP** 是最佳选择。但是，与客户端或甚至其他入点的向后兼容性或互操作性问题可能会要求您通过使用另一种加密算法的 **RADIUS** 配置 **WPA**，或选择其他安全模式。

但即便如此，在某些类型的网络上，安全性可能并不那么重要。如果仅提供互联网和打印机访问，和在访客网络上一样，将安全模式设为 **无 (纯文本)** 可能是恰当的做法。要防止其他客户端意外发现并连接至您的网络，可以禁用广播 **SSID**，这样就不会公开您的网络名称。如果网络完全隔离于对敏感信息的访问，在某些情况下可能会提供足够的保护。此级别的保护仅适用于访客网络，对于更注重连接是否容易的客户端而言，它也是在安全性和便利性之间做取舍后适当的做法。（请参阅第 97 页的“是否禁止了广播 **SSID** 增强安全性？”）

下文简短介绍了确保模式更为安全的因素、提供了各种模式的说明以及何时使用各种模式。

10.1.2 比较安全模式的密钥管理、身份验证及加密算法

以下三大因素确定了安全协议的有效性：

- 协议管理密钥的方式。
- 协议中是否具有集成用户身份验证。
- 协议用于编码/解码数据的加密算法或公式

下列是产品名称上可用的安全模式，并介绍了各种模式中使用的密钥管理、身份验证及加密算法。我们提供了一些建议，方便您了解何时使用某种模式更为恰当。

- 第 92 页的“何时使用未加密（无安全性）”。
- 第 93 页的“何时使用静态 WEP”。
- 第 94 页的“何时使用 IEEE 802.1x”。
- 第 95 页的“何时使用 WPA 个人版”。
- 第 96 页的“何时使用 WPA 企业版”。

10.1.2.1 何时使用未加密（无安全性）

将安全模式设为 *None (Plain-text)*（无（纯文本））时，按照定义，不提供任何安全性。在此模式下，数据不进行加密，而是在网络上将其作为“纯文本”发送。不使用密钥管理、数据加密或用户身份验证。

建议

不建议在内部网络经常使用未加密模式，即“*None (Plain-text)*（无（纯文本））”，因为它并不安全。这是能够运行访客网络的唯一模式，顾名思义它是不安全的 LAN，总是与内部 LAN 上的任何敏感信息虚拟分离或物理分离。

因此，只能在访客网络上将安全模式设为 *None (Plain-text)*（无（纯文本）），或在内部网络上进行初始设置、测试或解决问题时设置此模式。

另请参阅

有关如何配置未加密安全模式的信息，请参阅第 100 页的“*None (Plain-text)*（无（纯文本））”。

10.1.2.2 何时使用静态 WEP

静态 *有线等效加密 (WEP)* 是适用于 802.11 无线网络的数据加密协议。为网络上的所有无线工作站和接入点配置静态 64 位（40 位密钥 + 24 位初始化向量 (IV)）或 128 位（104 位密钥 + 24 位 IV）共享密钥用于数据加密。

表 10.1 静态 WEP 安全模式

密钥管理	加密算法	用户身份验证
静态 <i>WEP</i> 使用管理员提供的固定密钥。WEP 密钥使用不同的插槽（产品名称上最多 4 个）编入索引。 各客户端工作站必须在同一插槽中将相同的密钥编入索引，才能访问接入点上的数据。	<i>RC4</i> 流密码用于加密帧主体及各个 802.11 帧的循环冗余校验 (CRC)。	如果您将身份验证算法设为 “Shared Key”（共享密钥），此协议提供基本形式的用户身份验证。 而如果将身份验证算法设为 “Open System”（开放式系统），则不进行任何形式的身份验证。 如果将算法设为 “Both”（二者），则仅验证 WEP 客户端的身份。

建议

静态 WEP 提供的安全性相当于通过以太网连接发送解密数据，但它存在重大缺陷，不提供预期的安全级别。

因此，**不建议使用静态 WEP** 作为安全模式。只能在下列情况下使用静态 WEP：由于存在互操作性问题，静态 WEP 是您唯一可用的选项；您不关心泄露您网络上的数据的风险。

另请参阅

有关如何配置静态 WEP 安全模式的信息，请参阅第 101 页的 “Static WEP（静态 WEP）”。

10.1.2.3 何时使用 IEEE 802.1x

IEEE 802.1x 是使用被称为 EAP Encapsulation Over LAN (EAPOL) 的协议，通过 802.11 无线网络传输可扩展的身份验证协议 (EAP) 的标准。该标准比静态 WEP 更新、更安全。

表 10.2 IEEE 801.1x 安全模式

密钥管理	加密算法	用户身份验证
IEEE 802.1x 提供动态生成的密钥，且定期刷新。 各工作站有不同的单播密钥。	RC4 流密码用于加密帧主体及各个 802.11 帧的循环冗余校验 (CRC)。	IEEE 802.1x 模式支持各种身份验证方法，例如证书、Kerberos 和通过 RADIUS 服务器进行的公钥身份验证。 您可以选择使用产品名称嵌入式 RADIUS 服务器或外部 RADIUS 服务器。嵌入式 RADIUS 服务器支持受保护的 EAP (PEAP) 和 MSCHAP V2。

建议

IEEE 802.1x 模式是比静态 WEP 更好的选择，因为密钥是动态生成的，并且定期更改。但是，它使用的加密算法和静态 WEP 相同，因此可靠性低于在 Wi-Fi 受保护访问 (WPA) 或 WPA2 中使用的 TKIP 和 CCMP (AES) 等更为高级的加密方法。

此外，兼容性问题也比较麻烦，这是因为它支持各种身份验证方法，但却缺少标准实施方法。

因此，IEEE 802.1x 模式不是与 Wi-Fi 受保护访问 (WPA) 或 WPA2 同样安全的解决方案。如果由于某些客户端工作站没有 WPA 而无法使用 WPA，则比使用 IEEE 802.1x 模式更好的解决方案是使用 WPA 企业版模式。

如果网络上有外部 RADIUS 服务器，我们建议使用它，这比使用 AP 上的嵌入式 RADIUS 服务器更好。外部 RADIUS 服务器将提供比本地身份验证更高的安全性。

另请参阅

有关如何配置 IEEE 802.1x 安全模式的信息，请参阅第 106 页的 “IEEE 802.1x”。

10.1.2.4 何时使用 WPA 个人版

Wi-Fi 受保护访问个人版预共享密钥(PSK) 实施 Wi-Fi 联盟 IEEE 802.11h 标准，包括高级加密算法(AES)、计数器模式/CBC-MAC 协议(CCMP) 和临时密钥完整性协议(TKIP) 机制。该模式提供的加密算法与配备 RADIUS 的 WPA 2 相同，但无法集成 RADIUS 服务器进行用户身份验证。

此安全模式可向后兼容仅支持原始 WPA 的无线客户端。

表 10.3 WPA 个人版安全模式

密钥管理	加密算法	用户身份验证
WPA 个人版提供动态生成的密钥，且定期刷新。 各工作站有不同的单播密钥。	<ul style="list-style-type: none">临时密钥完整性协议(TKIP)。计数器模式/CBC-MAC 协议(CCMP) 高级加密标准(AES)。	使用预共享(PSK) 密钥，提供类似于 WEP 中的共享密钥的用户身份验证。

建议

当可选用 WPA 企业版时，不建议将 WPA 个人版用于产品名称。

我们建议改用 WPA 企业版，除非存在互操作性问题导致您无法使用此模式。

例如，EAP 与 RADIUS 服务器进行通信时，网络上的某些设备可能不支持 WPA 或 WPA2。嵌入式打印机服务器或实施空间非常有限的其他小型客户端设备可能不支持 RADIUS。在述这些情况下，建议您使用 WPA 个人版。

另请参阅

有关如何配置此安全模式的信息，请参阅第 109 页的“WPA Personal（WPA 个人版）”。

10.1.2.5 何时使用 WPA 企业版

使用 远程身份验证拨入用户服务 (RADIUS) 的 Wi-Fi 受保护访问企业版实施 Wi-Fi 联盟 IEEE 802.11h 标准，包括 高级加密标准 (AES)、计数器模式/CBC-MAC 协议 (CCMP) 和 临时密钥完整性协议 (TKIP) 机制。此模式要求使用 RADIUS 服务器对用户进行身份验证。WPA 企业版提供适用于无线网络的最佳安全性。

此安全模式还向后兼容仅支持原始 WPA 的无线客户端。

表 10.4 WPA 企业版安全模式

密钥管理	加密算法	用户身份验证
WPA 企业版提供动态生成的密钥，且定期刷新。 各工作站有不同的单播密钥。	<ul style="list-style-type: none">临时密钥完整性协议 (TKIP)。计数器模式/CBC-MAC 协议 (CCMP) 高级加密标准 (AES)。	远程身份验证拨入用户服务 (RADIUS) 您可以选择使用产品名称嵌入式 RADIUS 服务器或外部 RADIUS 服务器。嵌入式 RADIUS 服务器支持受保护的 EAP (PEAP) 和 MSCHAP V2。

建议

建议使用 WPA 企业版模式。用于 WPA 模式的 CCMP (AES) 和 TKIP 加密算法远优于静态 WEP 或 IEEE 802.1x 模式使用的 RC4 算法。因此，应尽可能使用 CCMP (AES) 或 TKIP。所有 WPA 模式允许使用这些加密方法，因此当可选用 WPA 时，建议优先使用 WPA 安全模式。此外，在此模式下采用 RADIUS 服务器进行用户身份验证，结果优于 WPA 个人版模式。

如果网络上有外部 RADIUS 服务器，我们建议使用它，这比使用 AP 上的嵌入式 RADIUS 服务器更好。外部 RADIUS 服务器将提供比本地身份验证更高的安全性。

选择 WPA 企业版安全模式中的选项时，使用以下指南：

1. 到目前为止，无线网络上能提供最高安全性的就是使用 CCMP (AES) 加密算法的 WPA 企业版模式。AES 是对称的 128 位块数据加密技术，可在网络的多个层使用。它是当前适用于无线网络的最有效的加密系统。如果网络上的所有客户端或其他 AP 与 WPA/CCMP 兼容，请使用此加密算法。（如果所有客户端与 WPA2 兼容，请选择仅支持 WPA2 客户端。）

2. 第二个最佳选择是将加密算法设为 TKIP 和 CCMP 的 WPA 企业版。这样，WPA 客户端工作站就无需与 CCMP 进行关联，它使用 TKIP 加密**多播**和**广播**帧，并允许客户端选择是否对于**单播**（AP 到单个站点）帧使用 CCMP 或 TKIP。此 WPA 配置实现了更高的互操作性，但却要以牺牲一定的安全性为代价。支持 CCMP 的客户端工作站可将其用于**单播**帧。如果您将加密算法设为“Both”（二者）时遇到 AP 到单个站点互操作性问题，则需要改为选择 TKIP。（请参阅下一选项。）
3. 第三个最佳选择是将加密算法设为 **TKIP** 的 WPA 企业版。某些客户端在同时启用 CCMP 和 TKIP 时会遇到互操作性问题。如果您遇到此问题，则选择 TKIP 作为加密算法。此为标准的 WPA 模式，也具有客户端无线软件安全功能的互操作性最高的模式。TKIP 是唯一一个经过 **Wi-Fi WPA** 认证测试的加密算法。

另请参阅

有关如何配置此安全模式的信息，请参阅第 112 页的“WPA Enterprise（WPA 企业版）”。

10.1.3 是否禁止了广播 SSID 增强安全性？

您可以抑制（禁止）此广播，阻止工作站自动发现您的接入点。抑制该 AP 的广播 SSID 时，客户端工作站上的 List of Available Networks（可用网络列表）中将不显示网络名称。客户端必须在请求方中配置确切的网络名称，才能进行连接。

禁用广播 SSID 足以阻止客户端意外连接到您的网络，但却无法阻止黑客连接网络或监控未加密流量的最简单尝试。

它为那些更注重客户端可简单获得连接且不提供任何敏感信息的公开网络（例如访客网络）提供了最低级别的保护。

（另请参阅第 100 页的“访客网络”。）

10.1.4 如何通过站点隔离保护网络？

启用 *Station Isolation*（站点隔离）时，接入点会阻止无线客户端之间的通信。接入点仍然允许无线客户端与网络上的有线设备之间的数据通信，但却不允许无线客户端之间的数据通信。

通信的阻断还延伸至通过 **WDS** 链路连接至网络的无线客户端；启用 Station Isolation（站点隔离）时，这些客户端彼此之间无法通信。

请参阅第 20 章：“无线分布系统”了解有关 WDS 的更多信息。

10.2 配置安全设置

要设置安全模式，请导航至 *Security* （安全性）选项卡，并如下所述更新字段。

图 10.1 安全设置页面

<div>Basic Settings</div> <div>User Management</div> <div>Cluster</div> <div>Access Points</div> <div>Sessions</div> <div>Channel Management</div> <div>Wireless Neighborhood</div> <div>Security</div> <div>Status</div> <div>Interfaces</div>	<div>Modify Internal Network security settings</div> <div><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</div> <div>Mode: <div>WPA Personal</div></div> <div>WPAVersions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2</div> <div>Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)</div> <div>Key: <div>reoreore</div></div> <div>Update</div>
---	--

以下配置信息说明了如何在接入点上配置安全模式。请记住，每个要与接入点交换数据的无线客户端必须配置为与接入点安全性一致的安全模式和加密钥设置。

在双射频 AP 上，这些安全设置应用于两个无线电通信。



注释：除纯文本外，安全模式仅适用于“内部”网络的配置。在“访客”网络上，只能使用纯文本模式。（有关访客网络的更多信息，请参阅第 14 章：“设置访客接入”。）

10.2.1 广播 SSID、站点隔离和安全模式

要配置接入点的安全性，请选择一种安全模式并如表 10.5 中所述填充相关字段。



注释：您还可以允许或禁止 *Broadcast SSID* （广播 SSID）并启用/禁用 *Station Isolation* （站点隔离）作为额外的预防措施，具体如第 99 页的表 10.5 中所述。

表 10.5 安全设置

字段	描述
<i>Broadcast SSID</i> (广播 SSID)	<p>要启用 Broadcast SSID（广播 SSID），请直接选中旁边的复选框。默认情况下，接入点广播（允许）其信标帧中的<i>服务集标识符(SSID)</i>。</p> <p>您可以抑制（禁止）此广播，阻止工作站自动发现您的接入点。抑制该 AP 的广播 SSID 时，客户端工作站上的 List of Available Networks（可用网络列表）中将不显示网络名称。客户端必须在请求方中配置确切的网络名称，才能进行连接。</p>
<i>Station Isolation</i> (站点隔离)	<p>要启用 Station Isolation（站点隔离），请直接选中旁边的复选框。</p> <ul style="list-style-type: none"> 禁用 Station Isolation（站点隔离）时，无线客户端一般会通过接入点发送流量，从而实现彼此间的通信。 启用 <i>Station Isolation</i>（站点隔离）时，接入点会阻止无线客户端之间的通信。接入点仍然允许无线客户端与网络上的有线设备之间的数据通信，但却不允许无线客户端之间的数据通信。通信的阻断还延伸至通过 WDS 链路连接至网络的无线客户端；启用 Station Isolation（站点隔离）时，这些客户端彼此之间无法通信。请参阅第 20 章：“无线分布系统”了解有关 WDS 的更多信息。
<i>Security Mode</i> (安全模式)	<p>选择 <i>Security Mode</i>（安全模式）。选择下列选项之一：</p> <ul style="list-style-type: none"> 第 100 页的“None (Plain-text)（无（纯文本））”。 第 101 页的“Static WEP（静态 WEP）”。 第 106 页的“IEEE 802.1x”。 第 109 页的“WPA Personal（WPA 个人版）”。 第 112 页的“WPA Enterprise（WPA 企业版）”。 <p>对于访客网络，只能应用“无（纯文本）”安全模式。（有关详细信息，请参阅第 14 章：“设置访客接入”。）</p> <p>除“无（纯文本）”外，安全模式仅适用于“内部”网络的配置。</p>

10.2.2 安全模式

☒ Broadcast SSID ☐ Station Isolation

Mode:

WPA Personal

None (Plain-text)

Static WEP

IEEE802.1x

WPA Personal

WPA Enterprise

WPA Version:

☒ WPA2

☐ CCMP (AES)

Cipher:

Key:

reoreore

10.2.2.1 None (Plain-text)（无（纯文本））

无（或纯文本安全性）意味着传入或传出产品名称的任何数据均未经加密。

如果您选择 *None (Plain-text)*（无（纯文本））作为安全模式，则无法在 AP 上配置其他选项。进行初始网络配置或解决问题时，此安全模式非常有用；如果经常使用内部网络，不建议使用，因为它并不安全。

访客网络

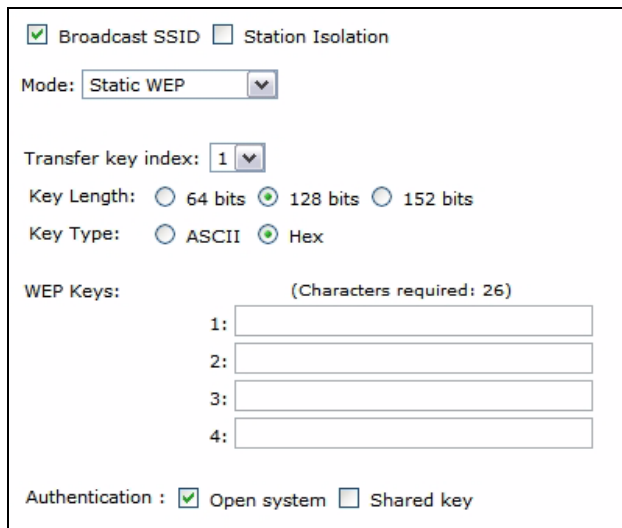
访客网络只能在将安全性设置为“None (Plain-text)”（无（纯文本））的模式下运行，根据定义它可以轻松访问，不安全的 *LAN* 总是与内部 LAN 上的任何敏感信息虚拟或物理隔离。例如，访客网络只能为日常访客提供互联网和打印机访问。

访客 AP 上缺少安全性，旨在帮助访客尽可能轻松地连接网络，且无需在其客户端中进行任何安全性设置。

对于访客网络上的最低保护级别，您可以选择抑制（禁止）此广播，阻止客户端工作站自动发现您的接入点。（另请参阅第 97 页的“是否禁止了广播 SSID 增强安全性？”。）

有关访客网络的更多信息，请参阅第 14 章：“设置访客接入”。

10.2.2.2 Static WEP（静态 WEP）



The image shows a configuration window for Static WEP. At the top, there are two checkboxes: 'Broadcast SSID' (checked) and 'Station Isolation' (unchecked). Below this is a 'Mode:' dropdown menu set to 'Static WEP'. Underneath is a 'Transfer key index:' dropdown menu set to '1'. Then, there are two rows of radio buttons: 'Key Length' with options '64 bits', '128 bits' (selected), and '152 bits'; and 'Key Type' with options 'ASCII' and 'Hex' (selected). Below these is a section for 'WEP Keys' with a note '(Characters required: 26)'. It contains four numbered input fields (1, 2, 3, 4) for keys. At the bottom, there is an 'Authentication:' section with two checkboxes: 'Open system' (checked) and 'Shared key' (unchecked).

有线等效加密 (WEP) 是适用于 802.11 无线网络的数据加密协议。为网络上的所有无线工作站和接入点配置静态 64 位（40 位密钥 + 24 位初始化向量 (IV)）或 128 位（104 位密钥 + 24 位 IV）共享密钥用于数据加密。在接入点及其客户端工作站之间无法混用 64 位和 128 位 WEP 密钥。

Static WEP（静态 WEP）不是最安全的可用模式，但比“None (Plain-text)”（无（纯文本））安全设置提供更高的保护，防止外部人员轻松破解未加密的无线数据通信。（如需了解更安全的模式，请参阅第 106 页的“IEEE 802.1x”页上的小节第 109 页的“WPA Personal（WPA 个人版）”，或第 112 页的“WPA Enterprise（WPA 企业版）”。

WEP 根据静态密钥，对无线网络上移动的数据进行加密。（加密算法是被称为 RC4 的“流”密码。）接入点使用密钥将数据传输至客户端工作站。各个户端工作站必须使用相同的密钥才能对其从接入点接收的数据进行解密。

客户端工作站可以使用不同的密钥将数据传输至接入点。（或者，它们都可以使用相同的密钥，但由于一个工作站可以对另一个工作站发送的数据进解密，因此安全性更低一些。）如果您选择 *Static WEP*（静态 WEP）安全模式，提供有关接入点设置的信息，如下图所示和第 102 页的表 10.6 中所述。

表 10.6 静态 WEP 安全设置

字段	描述
<i>Transfer Key Index</i> (传输密钥索引)	<p>从下拉菜单中选择一个密钥索引。提供 1 至 4 个密钥索引。 默认值为 1。</p> <p>Transfer Key Index （传输密钥索引）表示接入点将使用哪个 WEP 密钥对其传输的数据进行加密。</p>
<i>Key Length</i> (密钥长度)	<p>通过单击以下其中一个单选按钮，指定密钥长度：</p> <ul style="list-style-type: none">• 64 位• 128 位
<i>Key Type</i> (密钥类型)	<p>通过单击以下其中一个单选按钮，选择密钥类型：</p> <ul style="list-style-type: none">• ASCII• 十六进制
<i>Characters Required</i> (所需字符数)	<p>表示 WEP 密钥中所需的字符数量。</p> <p>所需的字符数量会根据您对 Key Length （密钥长度）和 Key Type （密钥类型）的设置自动更新。</p>
<i>WEP Keys</i> (WEP 密钥)	<p>您最多可以指定 4 个 WEP 密钥。在每个文本框内输入各个密钥的字符串。</p> <p>如果选择 “ASCII”，输入整数和字母的组合（0-9、a-z 和 A-Z）。如果选择 “HEX”，输入十六进制数字（0-9 和 a-f 或 A-F 的任何组合）。</p> <p>各个密钥所用的字符数量与 “Characters Required”（所需字符数）字段中指定的相同。这些是 RC4 WEP 密钥，与使用接入点的站点共享。</p> <p>各客户端工作站必须配置为使用与 AP 中指定的相同插槽中的相同 WEP 密钥之一。（请参阅第 103 页的 “使用静态 WEP 时需要谨记的规则”。）</p>

表 10.6 静态 WEP 安全设置（续）

字段	描述
Authentication Algorithm (身份验证算法)	<p>身份验证算法定义用于确定当静态 WEP 作为安全模式时是否允许客户端工作站与接入点关联的方法。从下拉菜单中选择下列任一选项，指定身份验证法：</p> <ul style="list-style-type: none">• Open System（开放式系统）。• Shared Key（共享密钥）。• Both（两者兼具）。 <p>Open System（开放式系统）身份验证允许任何客户端工作站与接入点关联，无论该客户端工作站是否拥有正确的 WEP 密钥。此算法还可用于纯文本、IEEE 802.1x 和 WPA 模式。将身份验证算法设为“Open System”（开放式系统）时，任何客户端都可与该接入点关联。</p> <p>请注意，这里只是允许客户端工作站与接入点关联，但并不保证它可以与接入点之间进行数据通信。站点必须有正确的 WEP 密钥，才能成功访问并解密接入点中的数据，并将可读数据传输至接入点。</p> <p>Shared Key（共享密钥）身份验证要求客户端工作站具有正确的 WEP 密钥，才能与该接入点关联。将身份验证算法设为“Shared Key”（共享密钥）时，WEP 密钥错误的站点无法与该接入点进行关联。</p> <p>默认设置为 Both（两者兼具）。将身份验证算法设为“Both”（两者兼具）时：</p> <ul style="list-style-type: none">• 配置为在共享密钥模式下使用 WEP 的客户端工作站必须有有效的 WEP 密钥，才能与该接入点进行关联。• 配置为使用 WEP 作为开放式系统（共享密钥模式未启用）的客户端工作站将能够与接入点进行关联，即使它们没有正确的 WEP 密钥。

使用静态 WEP 时需要谨记的规则

- 所有客户端工作站必须将无线 LAN (WLAN) 安全性设为 WEP，且所有客户端必须具有在 AP 上指定的 WEP 密钥之一，才能解码 AP 到站点之间的数据传输。
- 该 AP 必须具有在站点到 AP 之间传输数据的客户端使用的所有密钥，才能解码站点传输。
- 相同的密钥必须占用所有节点（AP 和客户端）上的相同插槽。例如，如果 AP 将 abc123 密钥定义为 WEP 密钥 3，则客户端工作站必须将相同的字符串定义为 WEP 密钥 3。
- 在某些无线客户端软件（例如 Funk Odyssey）上，可以配置多个 WEP 密钥，并定义客户端工作站“传输密钥索引”，然后设置站点，使用不同的密钥对其传输的数据进行加密。这样，就确保了相邻 AP 无法解码彼此的传输内容。

使用静态 WEP 的示例

举个简单的例子，假设您在接入点上配置了 3 个 WEP 密钥。在本示例中，AP 的 Transfer Key Index （传输密钥索引）设为 3。这意味着插槽 “3” 中的 WEP 密钥是该接入点用于加密其所发送数据的密钥。

图 10.2 设置接入点上的 AP 传输密钥

☒ Broadcast SSID

☐ Station Isolation

Mode:

Static WEP

Transfer key index:

3

Key Length:

☒ 64 bits

☐ 128 bits

☐ 152 bits

Key Type:

☒ ASCII

☐ Hex

WEK Keys: (Characters required: 5)

1:

abcde

2:

efghij

3:

klmno

4:

Authentication :

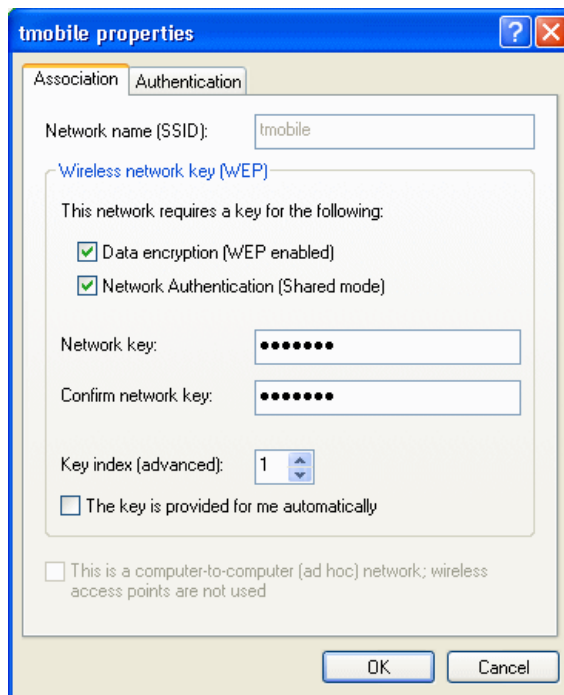
☒ Open system

☐ Shared key

然后，必须将所有客户端工作站设置为使用 WEP，并为各个客户端提供在 AP 上定义的插槽/密钥组合之一。

在本示例中，我们将在 Windows 客户端上设置 WEP 密钥 1。

图 10.3 向无线客户端提供 WEP 密钥



如果您有第二个客户端工作站，则还需要具备在 AP 上定义的其中一个 WEP 密钥。您可以向其提供与第一个客户端工作站相同的 WEP 密钥。更安全的解决方案是，您可以向第二个客户端工作站提供另一个 WEP 密钥（例如密钥 2），这样两个站点就无法解密彼此之间的传输。

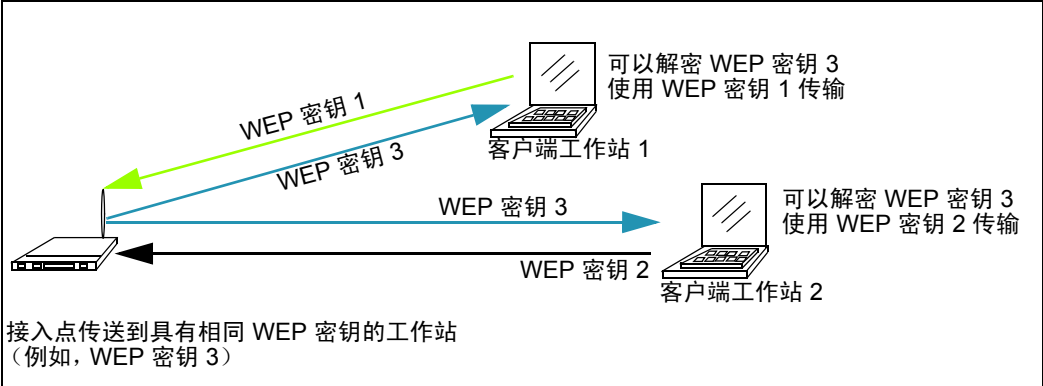
在客户端工作站上设置传输密钥索引的静态 WEP

某些无线客户端软件（例如 Funk Odyssey）允许配置多个 WEP 密钥，并可在客户端工作站设置传输索引，然后可以指定用于站点到 AP 传输的其他密钥。（标准 Windows 无线客户端软件不允许此操作。）

在本示例中，使用 Funk Odyssey 客户端软件，可以向各个客户端提供 WEP 密钥 3，这样各客户端就可以使用该密钥解码 AP 传输；还可向客户端 1 提供 WEP 密钥 1，并将其设为传输密钥。您可以向客户端 2 提供 WEP 密钥 2，并将其设为传输密钥索引。

图 10.2.2.3 显示了 AP 和使用多个 WEP 密钥及传输密钥索引的两个客户端工作站的动态机制。

图 10.4 在客户端工作站上使用多个 WEP 密钥和传输密钥索引的示例



10.2.2.3 IEEE 802.1x

IEEE 802.1x 标准定义了基于端口的身份验证，同时是用于密钥管理的基础设施。通过使用被称为 EAP Encapsulation Over LAN (EAPOL) 协议的 **IEEE 802.11** 无线网络，发送可扩展身份验证协议 (**EAP**) 消息。IEEE 802.1x 提供动态生成的密钥，且定期刷新。RC4 流密码用于加密帧主体及各个 802.11 帧的循环冗余校验 (CRC)。此模式要求使用 **RADIUS** 服务器对用户进行身份验证。如果启用内部 RADIUS 服务器的该选项，则通过 *Cluster (集群) > User Management (用户管理)* 选项卡，在 AP 上配置用户帐户。否则，请在外部 RADIUS 服务器上配置用户帐户。

接入点要求 **RADIUS** 服务器支持 **EAP**，例如 Microsoft Internet 身份验证服务器或产品名称内部身份验证服务器。要用于 Windows 客户端，身份验证服务器必须支持受保护的 EAP (PEAP) 和 **MSCHAP V2**。

配置 IEEE 802.1x 模式时，可以选择是否使用嵌入式 RADIUS 服务器或您提供的外部 RADIUS 服务器。产品名称嵌入式 RADIUS 服务器支持受保护的 **EAP** (PEAP) 和 **MSCHAP V2**。

如果您使用自己的 RADIUS 服务器，则可以选择使用 IEEE 802.1x 模式支持的任何一种身份验证方法，包括证书、Kerbero 以及公钥身份验证。但是请谨记，须配置客户端工作站使用和接入点相同的身份验证方法。

如果选择 *IEEE 802.1x* 安全模式，请提供以下信息：

Security Mode

IEEE 802.1x

Authentication Server

Built-in

Radius IP

127.0.0.1

Radius Key

•••••

☐ Enable radius accounting

☒ Broadcast SSID

☐ Station Isolation

Mode:

IEEE802.1x

☐ Use internal radius server

Radius IP:


10.128.14.14

Radius Key:

••••••••••

☐ Enable radius accounting

表 10.7 IEEE 802.1x 安全设置

字段	描述
<i>Use internal radius server</i> (使用内部 RADIUS 服务器)	<p>从下拉菜单中选择以下选项之一：</p> <ul style="list-style-type: none">要使用产品名称提供的身份验证服务器，确保选中 Use internal radius server（使用内部 RADIUS 服务器）字段旁的复选框。如果选择此选项，则无需提供 Radius IP 和 Radius 密钥，它们是自动提供的。如果启用内部 RADIUS 服务器的选项，则通过 <i>Cluster（集群）</i> > <i>User Management（用户管理）</i> 选项卡，在 AP 上配置用户帐户。有关详细信息，请参阅第 7 章：“管理用户帐户”。要使用外部身份验证服务器，确保取消选中 Use internal radius server（使用内部 RADIUS 服务器）字段旁的复选框。如果您取消选中此复选框，则必须提供要使用的服务器的 Radius IP 和 Radius 密钥。 <p>注： 根据 IP 地址和 UDP 端口号识别 RADIUS 服务器，以使用它提供的不同的服务。在当前版本的产品名称上，该接入点使用的 RADIUS 服务器用户数据报协议 (UDP) 端口不可配置。（对产品名称进行硬编码，以使用 RADIUS 服务器 UDP 端口 1812 进行身份验证，使用端口 1813 进行计费。）</p>
<i>Radius IP</i>	<p>在文本框中输入 Radius IP。</p> <p>Radius IP 是 RADIUS 服务器的 IP 地址。</p> <p>（产品名称内部身份验证服务器为 127.0.0.1。）</p> <p> 如果网络上有外部 RADIUS 服务器，我们建议使用它，这比使用 AP 上的嵌入式 RADIUS 服务器更好。外部 RADIUS 服务器将提供比本地身份验证更高的安全性。有关如何设置用户帐户的信息，请参阅第 7 章：“管理用户帐户”。</p>
<i>Radius Key</i> (Radius 密钥)	<p>在文本框中输入 Radius 密钥。</p> <p>Radius Key（Radius 密钥）是 RADIUS 服务器的共享密钥。您输入的文本将显示为 “*” 字符，以防止其他人在您键入时看到 RADIUS 密钥。</p> <p>（产品名称内部身份验证服务器密钥是秘密的。）</p> <p>此值绝对不会通过网络发送。</p>
<i>Enable radius accounting</i> (启用 Radius 计费)	<p>如果您想要跟踪并测量特定用户已使用的资源，例如系统时间、传送和接收的数据量等，请选中 “Enable radius accounting”（启用 Radius 计费）旁的复选。</p>

10.2.2.4 WPA Personal（WPA 个人版）

Wi-Fi 受保护访问个人版是 Wi-Fi 联盟 IEEE 802.11i 标准，包括计数器模式/CBC-MAC 协议、高级加密标准算法 (CCMP-AES) 和临时密钥完整性协议 (TKIP) 机制。

WPA 个人版采用预共享密钥（取代与企业版 WPA 安全模式中所用相同的 IEEE 802.1x 和 EAP）。PSK 仅可用于凭据的初始检查。此安全模式为仅支持原始 WPA 的无线客户端提供向后兼容性。

如果选择 WPA 个人版安全模式，请如第 110 页的表 10.8 中所述完成设置。

Security Mode

WPAWPA2 Personal (PSK)

Supported Client Stations

Both

Cipher Suites

TKIP

Key

☒ Broadcast SSID

☐ Station Isolation

Mode:

WPA Personal

WPAVersions:

☒ WPA

☒ WPA2

Cipher Suites:

☒ TKIP

☐ CCMP (AES)

Key:

reoreore

表 10.8 WPA 个人版安全设置

字段	描述
<i>WPA Versions</i> (WPA 版本)	<p>选择您想要支持的客户端工作站的类型：</p> <ul style="list-style-type: none">• WPA• WPA2• Both （两者兼具） <p>WPA。如果网络上的所有客户端工作站支持原始 WPA，但均不支持较新的 WPA2，则选择 WPA。</p> <p>WPA2。如果网络上的所有客户端工作站支持 WPA2，建议使用根据 <i>IEEE 802.11i</i> 标准提供最佳安全性的 WPA2。</p> <p>Both （两者兼具）。如果混用客户端，一些客户端支持 WPA2，而另一些客户端仅支持原始 WPA，请选择 Both （两者兼具）。这样，就可以同时关联 WPA 和 WPA2 客户端工作站，并对其进行身份验证，但将更稳固的 WPA2 用于支持它的客户端。此 WPA 置实现了更高的互操作性，但却要以牺牲一定的安全性为代价。</p>

表 10.8 WPA 个人版安全设置 （续）

字段	描述
<i>Cipher Suites</i> (加密套件)	<p>选择您想要使用的加密套件：</p> <ul style="list-style-type: none">• TKIP• CCMP (AES)• Both （两者兼具） <p>默认使用临时密钥完整性协议 (TKIP)。</p> <p>TKIP 提供比 WEP 密钥更安全的加密解决方案。TKIP 流程更频繁地更改所使用的加密密钥，更好地确保不会将同一密钥重新用于加密数据（WEP 的缺陷）。TKIP 使用客户端和接入点共享的 128 位“临时密钥”。临时密钥与客户端的 MAC 地址和 16 个八位字节初始化向量组合使用，以生成用于加密数据的密钥。这样，就确保了各个客户端工作站使用不同的密钥对数据进行加密。TKIP 使用 RC4 进行加密，与 WEP 相同。但 TKIP 每隔 10000 个数据包更改临时密钥，并对其进行分发，因此极大地提高了网络的安全性。</p> <p>计数器模式/CBC-MAC 协议 (CCMP) 是使用高级加密算法 (AES) 的 IEEE 802.11i 的加密方法。它将 CCM 与密码区块链计数器模式 (CBC-CTR) 和密码区块链消息身份验证代码 (CBC-MAC) 组合使用，实现了加密和消息完整性。</p> <p>如果选择 TKIP 和 CCMP(AES)，则成对密码是 AES，成组密码是 TKIP。成对密码用于单播流量，而成组密码用于多播/广播流量。TKIP 和 AES 客户端均可与该接点进行关联。WPA 客户端必须具有以下密钥之一，才能与 AP 进行关联：</p> <ul style="list-style-type: none">• 有效的 TKIP 密钥• 有效的 CCMP (AES) 密钥 <p>未配置使用 WPA 个人版的客户端将无法与 AP 进行关联。</p>
<i>Key</i> （密钥）	<p>预共享密钥是 WPA 个人版的共享密钥。输入至少由 8 个字符组成的字符串，最多不得超过 63 个字符。</p>

10.2.2.5 WPA Enterprise（WPA 企业版）

使用 远程身份验证拨入用户服务 (RADIUS) 的 Wi-Fi 受保护访问企业版实施 Wi-Fi 联盟 IEEE 802.11h 标准，包括高级加密标准 (AES)、计数器模式/CBC-MAC 协议 (CCMP) 和临时密钥完整性协议 (TKIP) 机制。企业版模式要求使用 RADIUS 服务器对用户的身份进行验证，并通过 Cluster（集群）、User Management（用户管理）选项卡配置用户帐户。

此安全模式向后兼容支持原始 WPA 的无线客户端。

配置 WPA 企业版模式时，可以选择是否使用内置 RADIUS 服务器或您所提供的外部 RADIUS 服务器。产品名称内置 RADIUS 服务器支持受保护的 EAP (PEAP) 和 MSCHAP V2。

如果选择 “WPA 企业版” 安全模式，请如第 113 页的表 10.9 中所述完成设置。

Security Mode

WPAWPA2 Enterprise (RADIUS)

Supported Client Stations

WPA

Enable pre-authentication

Cipher Suites

TKIP

Authentication Server

Built-in

Radius IP

127.0.0.1

Radius Key

Autokatalok

Enable radius accounting

Allow non-WPA IEEE 802.1x clients

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☒ WPA ☒ WPA2

☐ Enable pre-authentication

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key: ●●●●●●●●

☐ Enable radius accounting

表 10.9 WPA 企业版安全设置

字段	描述
WPA Versions (WPA 版本)	<p>选择您想要支持的客户端工作站的类型：</p> <ul style="list-style-type: none">• WPA• WPA2• Both （两者兼具） <p>WPA。如果网络上的所有客户端工作站支持原始 WPA，但均不支持较新的 WPA2，则选择 WPA。</p> <p>WPA2。如果网络上的所有客户端工作站支持 WPA2，建议使用根据 IEEE 802.11i 标准提供最佳安全性的 WPA2。</p> <p>Both （两者兼具）。如果混用客户端，一些客户端支持 WPA2，而另一些客户端仅支持原始 WPA，请选择 WPA 和 WPA2。这样，就可以同时关联 WPA 和 WPA2 客户端工作站，并对其进行身份验证，但将更稳固的 WPA2 用于支持它的客户端。此 WPA 配置实了更高的互操作性，但却要以牺牲一定的安全性为代价。</p>

表 10.9 WPA 企业版安全设置 （续）

字段	描述
<i>Enable pre-authentication</i> (启用预身份验证)	<p>对于 WPA 版本，如果只选择 WPA2，或选择 WPA 和 WPA2，您可以为 WPA2 客户端启用预身份验证。</p> <p>如果要 WPA2 客户端发送预身份验证包，请单击 Enable pre-authentication（启用预身份验证）。将从客户端当前使用的接入点将预身份验证信息转发至目标接入点。启用此功能后，可帮助连接至多个接入点的漫游客户端加身份验证。</p> <p>如果选择“WPA”作为 WPA 版本，则不应用此选项，因为可选的 WPA 不支持此功能。</p>
<i>Cipher Suites</i> (加密套件)	<p>选择要使用的加密套件：</p> <ul style="list-style-type: none">• TKIP• CCMP (AES)• Both（两者兼具） <p>默认使用临时密钥完整性协议 (TKIP)。</p> <p>TKIP 提供比 WEP 密钥更安全的加密解决方案。TKIP 流程更频繁地更改所使用的加密密钥，更好地确保不会将同一密钥重新用于加密数据（WEP 的缺陷）。TKIP 使用客户端和接入点共享的 128 位“临时密钥”。临时密钥与客户端的 MAC 地址和 16 个八位字节初始向量组合使用，以生成用于加密数据的密钥。这样，就确保了各个客户端工作站使用不同的密钥对数据进行加密。TKIP 使用 RC4 进行加密，与 WEP 相同。但 TKIP 每隔 10000 个数据包更改临时密钥，并对其进行分发，因此极大地提高了网络的安全性。</p> <p>计数器模式/CBC-MAC 协议 (CCMP) 是使用高级加密算法 (AES) 的 IEEE 802.11i 的加密方法。它将 CCM 与密码区块链计数器模式 (CBC-CTR) 和密码区块链消息身份验证代码 (CBC-MAC) 组合使用，实现了加密和消息完整性。</p> <p>选择 TKIP 和 CCMP 时，TKIP 和 AES 客户端均可以与接入点关联。配置使用配备 RADIUS 的 WPA 的客户端工作站必须具有以下任一信息才能与 AP 关联：</p> <ul style="list-style-type: none">• 有效的 TKIP RADIUS IP 地址和有效的共享密钥。• 有效的 CCMP (AES) IP 地址和有效的共享密钥。 <p>未配置使用配备 RADIUS 的 WPA 的客户端将无法与 AP 进行关联。</p> <p>默认情况下，选择 TKIP 和 CCMP。选择 TKIP 和 CCMP 时，配置为使用配备 RADIUS 的 WPA 的客户端工作站必须具有以下信息：</p> <ul style="list-style-type: none">• 有效的 TKIP RADIUS IP 地址和 RADIUS 密钥。• 有效的 CCMP AES IP 地址和 RADIUS 密钥。

表 10.9 WPA 企业版安全设置 （续）

字段	描述
<i>Use internal radius server</i> (使用内部 RADIUS 服务器)	<p>您可以使用产品名称提供的内置身份验证服务器，或使用外部 RADIUS 服务器。</p> <ul style="list-style-type: none">要使用产品名称提供的身份验证服务器，确保选中 Use internal radius server（使用内部 RADIUS 服务器）字段旁的复选框。如果选择此选项，则无需提供 Radius IP 和 Radius 密钥，它们是自动提供的。如果启用内部 RADIUS 服务器的该选项，则通过 <i>Cluster</i>（集群）> <i>User Management</i>（用户管理）选项卡，在 AP 上配置用户帐户。有关详细信息，请参阅第 7 章：“管理用户帐户”。要使用外部身份验证服务器，确保取消选中 Use internal radius server（使用内部 RADIUS 服务器）字段旁的复选框。如果您取消选中此复选框，则必须提供要使用的服务器的 Radius IP 和 Radius 密钥。 <p>注：根据 IP 地址和 UDP 端口号识别 RADIUS 服务器，以使用它提供的不同的服务。在当前版本的产品名称上，该接入点使用的 RADIUS 服务器用户数据报协议 (UDP) 端口不可配置。（对产品名称进行硬编码，以使用 RADIUS 服务器 UDP 端口 1812 进行身份验证，使用端口 1813 进行计费。）</p>
<i>Radius IP</i>	<p>在文本框中输入 Radius IP。Radius IP 是 RADIUS 服务器的 IP 地址。</p> <p>（产品名称内部身份验证服务器为 127.0.0.1。）</p> <p> 如果网络上有外部 RADIUS 服务器，我们建议使用它，这比使用 AP 上的嵌入式 RADIUS 服务器更好。外部 RADIUS 服务器将提供比本地身份验证更高的安全性。</p> <p>有关如何设置用户帐户的信息，请参阅第 7 章：“管理用户帐户”。</p>
<i>Radius Key</i> (Radius 密钥)	<p>在文本框中输入 Radius 密钥。</p> <p>Radius Key（Radius 密钥）是 RADIUS 服务器的共享密钥。您输入的文本将显示为 “*” 字符，以防止其他人在您键入时看到 RADIUS 密钥。</p> <p>（产品名称内部身份验证服务器密钥是秘密的。）</p> <p>此值绝对不会通过网络发送。</p>
<i>Enable RADIUS accounting</i> (启用 RADIUS 计费)	<p>如果您想要使用 WPA 客户端工作站的用户名和密码对其进行身份验证，请单击 Enable RADIUS Accounting（启用 RADIUS 计费）另请参阅第 7 章：“管理用户帐户”。</p>

10.3 更新设置

要更新安全设置：

1. 导航至 *Security*（安全）选项卡页面。
2. 根据需要配置安全设置。
3. 单击 **Update**（更新）按钮应用更改。

11.1 接口	119
11.1.1 以太网（有线）设置	120
11.1.2 无线设置	120
11.2 事件日志	120
11.2.1 启用或禁用持久性	121
11.2.2 严重程度	121
11.2.3 深度	122
11.2.4 用于内核消息的日志中继主机	122
11.2.4.1 了解远程记录	122
11.2.4.2 设置日志中继主机	123
11.2.4.3 在状态、事件页面上启用/禁用日志中继主机	124
11.2.5 事件日志	124
11.3 发射/接收统计数据	125
11.4 关联的无线客户端	127
11.4.1 链路完整性监控	127
11.5 相邻接入点	128



重要说明： 此处所述的所有维护和监控任务均涉及特定接入点上的查看和修改设置；并非位于多个接入点自动共享的集群配置上。因此，请务必确保您访问的是用于要配置的特定接入点的管理 Web 页面。有关信息，请参阅第 59 页的“特定 AP 和管理独立 AP 的配置信息”。

11.1 接口

要监控有线 LAN 和无线 LAN (WLAN) 设置，请导航至要监控的接入点的 *Status* (状态) > *Interfaces* (接口)。



注释： 在双射频接入点上，显示了射频一和射频二的当前无线设置。在单射频接入点上，显示单射频的设置。下图显示了双射频 AP 界面的页面。

图 11.1 网络接口页面

View settings for network interfaces

Wired Settings [\(Edit \)](#)

LAN or Internal Interface
MAC Address 00:08:A2:01:10:AC
VLAN ID
IP Address 10.128.75.98
Subnet Mask 255.255.0.0


Guest Interface
MAC Address 00:00:00:00:00:00
VLAN ID
Subnet

Wireless Settings [\(Edit \)](#)

Radio
Mode IEEE 802.11g
Channel 5 (2432 MHz)

Internal Interface
MAC Address 00:08:A2:01:10:B0
Network Name (SSID) SFGWPA /

Guest Interface
MAC Address n/a
Network Name (SSID) TEKLOGIX GUEST /



This page displays current Ethernet (Wired) and Wireless settings on the access point.

To configure Ethernet Settings, go to the [Ethernet \(Wired\) Settings](#) tab.

To configure Wireless Settings, go to the [Wireless Settings](#) tab.

[More ...](#)

本页显示了产品名称的当前设置。它显示 *Ethernet (Wired) Settings* (以太网 (有线) 设置) 和 *Wireless Settings* (无线设置)。

11.1.1 以太网（有线）设置

内部接口包括以太网 *MAC 地址*、*IP 地址*、*子网掩码* 和关联的网络无线名称 (*SSID*)。

访客接口包括 *MAC 地址*、*VLAN ID* 和关联的网络无线名称 (*SSID*)。

如果您想要更改任何设置，请单击 **Edit**（编辑）链接。

11.1.2 无线设置

Radio（射频）接口包括射频 *Mode*（模式）和 *信道*。此处还显示显示内部接口和访客接口的 *MAC 地址*（只读）和网络名称。（有关详细信息，请参阅第 13 章：“设置无线接口”和第 16 章：“配置 802.11 射频设置”。）

如果您想要更改任何设置，请单击 **Edit**（编辑）链接。

11.2 事件日志

要查看特定接入点的系统事件和内核日志，在要监控的接入点管理 Web 页面上，导航至 *Status*（状态）> *Events*（事件）。

图 11.2 接入点事件

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

View events generated by this access point

Options

Persistence ☐ Enabled ☒ Disabled

Severity

7

Depth

128

Update

☐ Relay Log

Relay Host

Relay Port

514

Update

Events

Clear All

Time	Type	Service	Description
Jun 4 19:14:29	info	dropbear [3074]	exit after auth (admin): Exited normally
Jun 4 19:14:29	err	dropbear [3074]	chown /dev/tty0 0 0 failed: Read-only file system
Jun 4 18:25:30	info	hostapd	wlan0: STA 00:10:c6:36:6f:1f WPA: group key poll timed out (no reply was received)
Jun 4 18:24:00	info	hostapd	wlan0: STA 00:10:c6:36:6f:1f WPA: group key exchange completed

Events（事件）选项卡页面允许启用或禁用 *Persistence*（持久性）。该页面同时提供了启用远程“日志中继主机”的选项，让您能够在内核日志中捕获所有系统事件和错误。（这需要首先设置一台远程中主机。请参阅第 122 页的“用于内核消息的日志中继主机”）。*Events*（事件）选项卡还列出了该接入点生成的最新事件（请参阅第 124 页的“事件日志”）。



注释：9160 G2 无线网关使用网络时间协议 (NTP) 获取其日期和时间信息。该数据以 UTC 格式（也称为格林威治标准时间）报告。你需要将报告的时间转换为当地时间。有关设置网络时间协议的信息，请参阅第 25 章：“网络时间协议服务器”。

11.2.1 启用或禁用持久性

可在 *Events*（事件）选项卡中可以启用或禁用 *Persistence*（持久性）。持久性日志保存在 NVRAM 中。即使重新启动后，所有持久性日志仍然保留在 NVRAM 中。非持久性日志仅在运行期间保存。如果重新启动 9160 G2，所有非持久性日志将丢失。

在 *Events*（事件）选项卡中启用 *Persistence*（持久性），以确保所有的日志均已写入 NVRAM，即使在重新启动后，这些日志仍可恢复。



注释：需要记住的是，启用持久性将导致连续的写入操作。存在用完 AP 的闪存元素的风险——鉴于此风险性较高，您应当根据需要进行确定是否启用持久性。

表 11.1 持久性配置设置

字段	描述
<i>Relay Log</i> (中继日志)	选择启用或禁用 <i>Persistence</i> （持久性）。
<i>Relay Host</i> (中继主机)	您可选择介于 0 和 7 之间的严重性级别。 <i>Severity</i> （严重程度）7 是最不严重的程度， <i>Severity</i> （严重程度）0 是最严重的程度。 有关严重程度的更多详情，请参阅第 121 页的“严重程度”。
<i>Relay Port</i> (中继端口)	您可输入介于 1 和 128 之间的值。 有关深度的更多信息，请参阅第 122 页的“深度”。

11.2.2 严重程度

配置严重程度旨在过滤或限制事件日志中显示的安全性消息。您可能不太想要看到所有消息的列表。可使用 *严重程度* 配置功能过滤那些不太严重或重要的消息。

如果您将 *Severity*（*严重程度*）设为 7，则事件日志中将显示严重程度介于 0 和 7 之间的所有消息。另外，如果您想要过滤消息，可将 *Severity*（*严重程度*）设为 4。在此情况下，事件日志中将出现严重程度介于 4 和 0 之间的所有消息。因此，不太严重的消息和通知将被忽略。

表 11.2 严重程度配置设置

严重程度	描述
0	紧急报警：系统不可用
1	提示：必须立即采取行动
2	临界：临界情况
3	错误：错误情况
4	警告：警告情况
5	通知：正常但重大的情况
6	信息：信息消息
7	调试：调试级消息

11.2.3 深度

Depth（深度）字段中指定的值确定了可保存至 NVRAM 的日志条目的数量。您最多可以保存 128 个条目。如果依靠日志消息来监控 AP 的性能，应将 *Depth*（深度）值设定为最大值 **128**。

11.2.4 用于内核消息的日志中继主机

- 第 122 页的 “了解远程记录”。
- 第 123 页的 “设置日志中继主机”。
- 第 124 页的 “在状态、事件页面上启用/禁用日志中继主机”。

11.2.4.1 了解远程记录

内核日志是系统事件（显示在系统日志中）和内核消息的综合列表，例如丢弃帧等错误条件。

您无法直接从接入点的管理 Web UI 查看内核日志消息。您必须首先设置一个运行系统日志程序的远程服务器，并在您的网络上作为系统日志的 “日志中继主机”。然后，您可以配置产品名称，将其系统日志消息发送给远程服务器。

使用远程服务器来收集接入点系统日志消息，有诸多好处。您可以：

- 从多个接入点聚集系统日志消息。
- 与单个接入点相比，消息保存的时间更长。
- 触发脚本管理操作和提示。

11.2.4.2 设置日志中继主机

要使用内核日志中继，您必须配置一台远程服务器来接收系统日志消息。根据您用作远程日志主机的机器类型的不同，该程序将有所不同。以下是如使用系统日志后台程序配置一台远程 Linux 服务器的示例。

使用 Linux 系统日志的示例

下列步骤可激活 Linux 服务器上的系统日志后台程序。确保您具有完成这些任务所需的根用户身份标识。

1. 以根用户的身份登录到要用作系统日志中继主机的机器。

下列操作要求具有根用户权限。如果您还未以根用户登录，在命令行提示中键入 su，提示即成为根用户（“super user”（超级用户））。

2. 编辑文件顶部的 /etc/init.d/syslogd，并为变量 SYSLOGD 添加 “-r”。您编辑的行将显示为：

SYSLOGD=“-r”

查阅说明页，获得有关系统日志命令选项的更多信息。（在命令行键入 man syslogd。）

3. 如果您想要将所有消息发送至一个文件，请编辑 /etc/syslog.conf。

例如，您可添加此行来将所有消息发送至名为 “AP_syslog” 的日志文件。

```
* *    -/tmp/AP_syslog
```

查阅说明页，获得有关 syslog.conf 命令选项的更多信息。（在命令行键入 man syslog.conf。）

4. 通过在命令行提示中键入下列内容，重新启动系统日志服务器：

```
/etc/init.d/syslogd restart
```



注释：系统日志程序将默认使用端口 514。我们建议保留此默认端口。然而，如果您选择重新配置日志端口，确保您为系统日志指定的端口号未被其他进程使用。

11.2.4.3 在状态、事件页面上启用/禁用日志中继主机

要在 *Status*（状态）> *Events*（事件）页面上启用和配置日志中继，按如下所述设定 *日志中继* 选项，然后单击 **Update**（更新）。

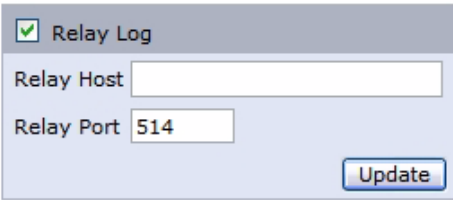


表 11.3 日志中继主机设置

字段	描述
<i>Relay Log</i> (中继日志)	选择启用或禁用日志中继主机： 如果选中 Relay Log （中继日志）复选框，将启用日志中继主机， <i>Relay Host</i> （中继主机）和 <i>Relay Port</i> （中继端口）字段将可编辑。
<i>Relay Host</i> (中继主机)	指定中继主机的 IP 地址 或 DNS 名称。 注： 如果您使用的是 <i>Devicescape Wireless Operations Center</i> ，存储库服务器应接收来自所有接入点的系统日志消息。在这种情况下，使用操作中心存储库服务器作中继主机。
<i>Relay Port</i> (中继端口)	指定中继主机上系统日志程序的端口号。 默认端口为 514 。

更新设置

要应用更改，请单击 **Update**（更新）。

如果 *启用了* 日志中继主机，单击 **Update**（更新）将启用远程记录。接入点将把其用于实时显示的内核消息发送至远程日志服务器监视器、指定的内核日志文件或其他存储器，具体取决于配日志中继主机的方式。

如果 *禁用了* 日志中继主机，单击 **Update**（更新）将禁用远程记录。

11.2.5 事件日志

事件日志显示了接入点上的系统事件，例如站点关联、身份验证和其他事件。实时事件日志总是在正在监控的接入点的 *Status*（状态）> *Events*（事件）管理 Web UI 页面上显示。

11.3 发射/接收统计数据

要查看特定接入点的发射/接收统计数据，在要监控的接入点的管理 Web 页面上，导航至 *Status*（状态）> *Transmit/Receive*（发射/接收）。



注释：图 11.3 显示双射频 AP 的发射/接收页面。单射频 AP 的管理 Web 页面外观略有不同。

图 11.3 发射和接收统计数据页面

Basic Settings	View transmit and receive statistics for this access point			
User Management				
Cluster				
Access Points	IP Address 10.128.75.4			
Sessions	MAC Address 00:08:A2:01:4B:52 00:00:00:00:00:00 00:08:A2:01:4B:56 n/a			
Channel Management	VLAN ID			
Wireless Neighborhood	Name (SSID)		SFG	TEKLOGIX GUEST
Security				
Status				
Interfaces				
Events				
Transmit/Receive				
Client Associations				
Neighboring Access Points				
Manage				
Ethernet Settings				
802.11 Settings				
802.11 Advanced Settings				
VWN				

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
Total packets	11329	0	4622	0
Total bytes	3482589	0	649463	0
Errors	0	0	2	0

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
Total packets	833047	0	37	0
Total bytes	89628621	0	3190	0
Errors	0	0	0	0

该页面提供了有关当前接入点的一些基本信息，并实时显示此接入点的发射和接收统计数据，具体如第 126 页的表 11.4 中所述。显示的所有发射和接收统计数据为自接入点上次启动后的汇总值。如果重新启动 AP，这些数字显示自重新启动后的发射/接收汇总值。

表 11.4 发射/接收统计数据

字段	描述
<i>IP Address</i> (IP 地址)	接入点的 IP 地址 。
<i>MAC Address</i> (MAC 地址)	<p>指定接口的媒体访问控制 (MAC) 地址。</p> <p>MAC 地址是代表网络接口的任何设备的永久性、唯一的硬件地址。MAC 地址由制造商分配。</p> <p>产品名称的每个接口具有唯一的 MAC 地址。对于双射频接入点，这两个射频的每个接口具有不同的 MAC 地址。</p>
<i>VLAN ID</i>	<p>虚拟 LAN (VLAN) ID。</p> <p>VLAN 是对网络上的设备进行基于软件的逻辑分段，允许这些设备就像连接至一个物理网络那样运行，尽管实际上它们并未连接网络。</p> <p>VLAN 可用于在同一接入点上建立内部和访客网络。</p>
<i>Name (SSID)</i> (名称 (SSID))	<p>无线网络名称。也称为 SSID，该字母数字密钥是无线局域网的唯一标识。</p> <p>在 Basic Settings （基本设置）选项卡上设置 SSID。（请参阅第 47 页的“提供网络设置”。）</p>
发射和接收信息	
<i>Total Packets</i> (数据包总数)	表示此接入点发射 （在发射表中）或接收 （在接收表中）的数据包总数。
<i>Total Bytes</i> (字节总数)	表示此接入点发射 （在发射表中）或接收 （在接收表中）的字节总数。
<i>Errors</i> (错误数)	表示与此接入点发送和接收数据有关的错误总数。

11.4 关联的无线客户端

要查看与特定接入点关联的客户端工作站，请在要监控的接入点的管理 Web 页面上，导航至 *Status*（状态） > *Client Associations*（客户端关联）。

显示了关联的工作站，以及有关每个工作发射和接收的数据包流量的信息（请参阅第 127 页的图 11.4）。

图 11.4 关联的客户端工作站

Basic Settings	View list of currently associated client stations							
User Management								
Cluster								
Access Points								
Sessions								
Channel Management								
Wireless Neighborhood								
Security								
Status								
Interfaces								
Events								
Transmit/Receive								
Client Associations								
Neighboring Access Points								

Network	Station	Status		From Station		To Station	
		Authenticated	Associated	Packets	Bytes	Packets	Bytes
wlan0	00:0c:f1:3e:99:ae	Yes	Yes	1732	261063	1517	510274
wlan0	00:90:4b:93:f4:35	Yes	Yes	687	123005	572	155409

11.4.1 链路完整性监控

产品名称提供链路完整性监控，从而不断验证其与每个关联客户端的连接（甚至在发生数据交换时）。要执行此操作，AP 可在没有其他流量通过时将数据包发送给客户端。当客户端超出范围，即使在没有正常流量交换期间，可允许接入点进行检测。客户端连接会在客户端消失后 300 秒内丢弃关联客户端的列表，即使并未取消关联（但超出范围）。

11.5 相邻接入点

“相邻接入点”的状态页面提供您查看其管理 Web 页面的接入点范围内所有接入点的实时统计数据。要查看无线网络上其他接入点的信息，请导航至 *Status*（状态）> *Neighboring Access Points*（相邻接入点）（请参阅第 128 页的图 11.5）。

图 11.5 相邻接入点的状态

View neighboring access points													
AP Detection <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="button" value="Update"/>													
MAC	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates	
00:08:a2:01:13:20	100	AP		On	Off	2.4	11	1		2	Fri Jan 2 06:33:01 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:22:34	100	AP		On	On	2.4	3	1		3	Fri Jan 2 06:31:23 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:12:fc	100	AP		On	Off	2.4	6	1		1	Fri Jan 2 06:26:45 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:22:30	100	AP		On	On	2.4	6	1		1	Fri Jan 2 06:26:07 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:02:73:e4	100	AP	steve	On	On	2.4	6	1		6616	Fri Jan 2 06:34:40 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	

相邻接入点的信息如表 11.5中所述。

表 11.5 相邻接入点统计数据

字段	描述
MAC	显示相邻接入点的 MAC 地址。 MAC 地址是唯一标识网络各节点的硬件地址。
Radio (射频)	双射频 AP 如果对相邻 AP “探测”的接入点为双射频接入点，则显示 Radio（射频）字段。 Radio（射频）字段显示在哪个射频上检测到相邻 AP。 <ul style="list-style-type: none">wlan 0（射频一）wlan 1（射频二） 单射频 AP 单射频接入点的 <i>Neighboring Access Points</i> （相邻接入点）页面上不显示此字段。
Beacon Int. (信标间隔)	显示此接入点使用的 信标 间隔。 接入点每隔一定时间就会发射信标帧，表示存在无线网络。默认行为是每 100 毫秒发送一个信标帧（或每秒发送 10 个信标帧）。 可在 <i>Manage</i> （管理）> <i>802.11 Advanced Settings</i> （高级设置）选项卡页面上设置信标间隔。（请参阅第 16 章：“配置 802.11 射频设置”。）
Capability (功能)	当转化为二进制时，十六进制数字表示每个 <i>IEEE 802.11</i> 的特性或功能，以及其在该接入点上 是“打开”还是“关闭”。

表 11.5 相邻接入点统计数据 （续）

字段	描述
<i>Type</i> (类型)	<p>表示设备类型：</p> <ul style="list-style-type: none">• AP 表示相邻设备是在 基础架构模式下支持 IEEE 802.11 无线网络框架的接入点。• 点对点表示在点对点模式下运行的相邻工作站。设定为点对点模式的工作站可彼此直接通信，无需使用传统的接入点。点对点模式是 IEEE 802.11 无线网络框架，也被称为 “对等” 模式或独立基本服务集 (IBSS)。
<i>SSID</i>	<p>接入点的服务集标识符 (SSID)。</p> <p>SSID 是限长 32 个字符的字母数字字符串，唯一地标识无线局域网。它也被称为 “网络名称”。</p> <p>SSID 在 Basic Settings（基本设置）（请参阅第 5 章：“配置基本设置”）或 <i>Manage</i>（管理）> <i>Wireless Settings</i>（无线设置）（请参阅第 13 章：“设置无线接口”）中进行设置。</p> <p>在同一接入点上运行的访客网络和内部网络始终必须具有两个不同的网络名称。</p>
<i>Privacy</i> (加密)	<p>表示相邻设备是否存在安全性。</p> <ul style="list-style-type: none">• Off（关）表示相邻设备的安全模式设定为 “无” 模式（无安全性）。• On（开）表示相邻设备具有一些安全性。 <p>可在 <i>Security</i>（安全性）选项卡页面上配置 AP 的安全性。有关安全性设置的详细信息，请参阅第 10 章：“配置安全性”。</p>
<i>WPA</i>	<p>表示此接入点的 WPA 安全性是 On（开）还是 Off（关）。</p>
<i>Band</i> (频段)	<p>表示此接入点当前使用的 IEEE 802.11 模式。（例如，IEEE 802.11a、IEEE 802.11b、IEEE 802.11g。）</p> <p>显示的数字表示根据下图所示的模式。</p> <ul style="list-style-type: none">• 2.4 表示 IEEE 802.11b 模式或 IEEE 802.11g 模式。• 5 表示 IEEE 802.11a 模式。

表 11.5 相邻接入点统计数据 （续）

字段	描述
<i>PHY</i>	<p>表示此接入点当前使用的 IEEE 802.11 模式。（例如，IEEE 802.11a、IEEE 802.11b、IEEE 802.11g。）</p> <p>显示的数字表示根据下图所示的模式。</p> <ul style="list-style-type: none">• 4 表示 IEEE 802.11b 模式• 7 表示 IEEE 802.11g 模式• 8 表示 IEEE 802.11a 模式• 256 表示 Atheros Turbo 模式
<i>Channel</i> (信道)	<p>显示接入点当前广播所在的信道。</p> <p>信道定义了用于收发射频的射频频谱部分。</p> <p>在 <i>Radio Settings</i>（射频设置）中设置信道。（请参阅第 16 章：“配置 802.11 射频设置”。）</p>
<i>Rate</i> (速率)	<p>显示此接入点当前发射的速率（兆位/秒）。</p> <p>当前速率将始终为 <i>Rates</i>（速率）中所示的支持速率之一。</p>
<i>Signal</i> (信号)	<p>表示此接入点发射的射频信号强度，以分贝 (Db) 为单位进行测量。</p>

表 11.5 相邻接入点统计数据 （续）

字段	描述
<i>ERP</i>	<p><i>扩展速率协议(ERP)</i> 指 <i>IEEE 802.11g</i> 工作站使用的协议。</p> <p>此字段指示使用此接入点的 <i>IEEE 802.11g</i> 客户端工作站应在和 <i>IEEE 802.11g (ERP)</i> 工作站相同的信道上存在 <i>IEEE 802.11b</i> （非 ERP）工作站或接入点时，发送数据。</p> <p>如果 <i>IEEE 802.11g</i> 工作站确定使用相同信道的网络上存在一个或多个 <i>IEEE 802.11b</i> 节点，将启用 <i>request-to-send</i> （请求发送） (<i>RTS</i>) 和 <i>clear-to-send</i> （可以发送） (<i>CTS</i>)保护。</p> <p>当前 UI 上显示的数字为十六进制数字，当其转化为二进制时，可显示如何设置 ERP 标记。</p> <p>使用下图确定用于此 AP 的当前 ERP 设置。</p> <ul style="list-style-type: none">• 0x0 表示 “无”。不存在 <i>IEEE 802.11b</i> （非 ERP）工作站。• 0x1 表示存在一台 <i>IEEE 802.11b</i> （非 ERP）设备。此 AP 仅有一个 <i>IEEE 802.11b</i> 工作站。（该标记永远不得单独使用。）• 0x2 表示 <i>IEEE 802.11g</i> 工作站应使用 <i>RTS/CTS</i> 保护。同一信道上存在另一个仅有 <i>IEEE 802.11b</i> 客户端工作站的 AP。• 0x3 表示存在一台非 ERP 设备，且 <i>IEEE 802.11g</i> 工作站应使用 <i>RTS/CTS</i> 保护。• 0x4 表示 <i>IEEE 802.11g</i> 工作站应使用 Barker 前导码。• 0x5 表示 <i>IEEE 802.11g</i> 应使用与 0x1 相同的协议，但拥有 Barker 前导码。• 0x6 表示 <i>IEEE 802.11g</i> 应使用与 0x2 相同的协议，但拥有 Barker 前导码。• 0x7 表示 <i>IEEE 802.11g</i> 应使用与 0x3 相同的协议，但拥有 Barker 前导码。
<i>Beacons</i> (信标)	表示自上次启动后，该接入点发射的信标总数。
<i>Last Beacon</i> (最近信标)	指从接入点最近发射信标的日期和时间。
<i>Rates</i> (速率)	<p>表示为相邻接入点设置的支持速率和基本（标称）速率。所示速率以兆位/秒（Mbp）为单位。</p> <p>所有支持的速率均已列出，基本速率以粗体显示。</p> <p>在 <i>Radio Settings</i>（射频设置）上配置速率设置。（请参阅第 16 章：“配置 802.11 射频设置”。）接入点显示的速率将始终为 AP 的 <i>Radio Settings</i>（射频设置）中指定的当前速率。</p>

以太网（有线）接口

12

12.1 导航至以太网（有线）设置	135
12.1.1 DNS 主机名	136
12.1.2 访客接入	136
12.1.2.1 配置内部 LAN 和访客网络	136
12.1.2.2 启用或禁用访客接入	137
12.1.2.3 指定虚拟访客网络	137
12.1.3 虚拟无线网络	138
12.1.4 内部接口设置	138
12.1.5 访客接口设置	141
12.1.6 更新设置	141

以太网（有线）设置介绍了您的以太网局域网 (LAN) 的配置。



注释：以太网设置在集群中不共享。这些设置必须在管理页面上针对各个接入点单独配置。要访问组成当前集群的某个接入点的管理页面，请在当前 AP 的 Cluster（集群）> Access Points（接入点）页面上，单击 **IP Address**（IP 地址）链接。有关集群共享哪些设置的更多信息，请参阅第 54 页的“哪些设置可以/不可以作为集群配置的组成部分进行共享？”。

12.1 导航至以太网（有线）设置

要在产品名称上配置“有线”地址和相关设置，导航至 *Manage*（管理）> *Ethernet Settings*（以太网设置）选项卡，然后按照以下小节所述更新字段。

图 12.1 以太网设置概览

<div>Basic Settings</div> <div>User Management</div> <div>Cluster</div> <div>Access Points</div> <div>Sessions</div> <div>Channel Management</div> <div>Wireless Neighborhood</div> <div>Security</div> <div>Status</div> <div>Interfaces</div> <div>Events</div> <div>Transmit/Receive</div> <div>Client Associations</div> <div>Neighboring Access Points</div> <div>Manage</div> <div>Ethernet Settings</div> <div>802.11 Settings</div> <div>802.11 Advanced Settings</div> <div>VWN</div> <div>WDS</div> <div>Guest Login</div> <div>MAC Filtering</div> <div>Load Balancing</div> <div>Services</div> <div>QoS</div>	<div>Modify Ethernet (Wired) settings</div> <div>DNS Hostname<div>PTX9160-Wireless-AP</div></div> <div>Guest Access<div><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</div></div> <div>For Guest Access<div>VLAN on Ethernet Port</div></div> <div>Virtual Wireless Networks (Using VLANs on Ethernet Port 1)<div><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</div></div> <div>Internal Interface Settings</div> <div>MAC Address<div>00:08:A2:01:4B:52</div></div> <div>VLAN ID<div>2</div></div> <div>Management VLAN ID<div>2</div></div> <div>Untagged VLAN<div><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</div></div> <div>Untagged VLAN ID<div>1</div></div> <div>Connection Type<div>DHCP</div></div> <div>Static IP Address<div>192 . 168 . 1 . 10</div></div> <div>Subnet Mask<div>255 . 255 . 255 . 0</div></div> <div>Default Gateway<div>192 . 168 . 1 . 254</div></div> <div>DNS Settings via DHCP<div><input checked="" type="radio"/> On <input type="radio"/> Off</div></div> <div>DNS Nameservers<div><div></div> . <div></div> . <div></div> . <div></div></div><div></div> . <div></div> . <div></div> . <div></div></div>
--	--

DNS Domain

example.com

Guest Interface Settings

MAC Address

00:00:00:00:00:00

VLAN IDSubnet

n/a

Update

12.1.1 DNS 主机名

表 12.1 设置 DNS 名称

字段	描述
<i>DNS Hostname</i> (DNS 主机名)	<p>在文本框中输入接入点的 DNS 名称。</p> <p>这是主机名。它由您的 ISP 或网络管理员提供，也可以由您自己提供。</p> <p>系统名称的规则为：</p> <ul style="list-style-type: none">• 此名称最长 20 个字符。• 仅允许使用字母、数字和短划线。• 名称必须以字母开头，以字母或数字结束。

12.1.2 访客接入

您可以在同一台 产品名称上，通过隔离的网络和安全的内部 *LAN* 提供受控的访客接入。

12.1.2.1 配置内部 LAN 和访客网络

局域网 (LAN) 是覆盖区域有限的通信网络，例如建筑物楼层。LAN 连接多台计算机和其他网络设备（例如存储设备和打印机）。

*以太网*是实施 LAN 的最常用技术。 *Wi-Fi (IEEE)* 是另一种非常流行的 LAN 技术。产品名称 允许您在同一个接入点上配置两个不同的 LAN：一个用于安全的 *内部* LAN，另一个用于不安全及安全性低或无内部资源访问权限的公共 *访客网络*。要配置上述网络，您需要提供无线和以太网（有线）设置。

以下小节提供了有关如何配置以太网（有线）设置的信息。

（有关如何配置无线设置的信息，请参阅第 13 章：“设置无线接口”。有关如何设置访客接口的概述，请参阅第 14 章：“设置访客接入”。）

12.1.2.2 启用或禁用访客接入

默认情况下，产品名称的访客接入功能为**禁用**状态。如果您想要在您的 AP 上提供访客接入，请在 *Ethernet (Wired) Settings*（以太网（有线）设置）选项卡上启用访客接入。

表 12.2 启用/禁用访客接入

字段	描述
<i>Guest Access</i> (访客接入)	<p>默认情况下，产品名称的访客接入功能为禁用状态。</p> <ul style="list-style-type: none">要启用访客接入，单击 Enabled（启用）。要禁用访客接入，单击 Disabled（禁用）。

12.1.2.3 指定虚拟访客网络

如果您启用访客接入，必须在此接入点上**虚拟**创建“内部”和“访客网络”，方法是将接入点的 LAN 端口连接至支持 **VLAN** 的交换机的标记端口，然后在此管理页面上定义两个不同的虚拟 LAN。（有关更多信息，请参阅第 14 章：“设置访客接入”。）如表 12.3 中所述创建实际上分开的内部和访客 LAN。

表 12.3 指定虚拟访客网络

字段	描述
<i>Guest Access</i> (访客接入)	<ul style="list-style-type: none">选择 Enabled（启用），启用访客接入。（如果您选择此选项，必须在下一个设置 <i>For Guest access use</i>（用于访客接入）上选择 VLAN，然后在页面的其余部分提供访客网络 VLAN 的详细信息。）选择 Disabled（禁用），禁用访客接入。
<i>For Guest Access</i> (用于访客接入)	<p>在此接入点上指定事实上独立的访客网络：</p> <ul style="list-style-type: none">由于接入点仅使用与内部 LAN 的一个物理连接，因此请从下拉菜单中选择 VLAN on Ethernet Port 1（以太网端口 1 上的 VLAN）。这将启用您必须提供 VLAN ID 的“VLAN”设置。请参阅第 141 页的“访客接口设置”。 <p>重要说明：如果您重新配置访客和内部接口以使用 VLAN，可能丢失与接入点的连接。第一，确保您所使用的交换机和 DHCP 服务器支持 VLAN，符合 IEEE 802.1Q 标准。在 Manage（管理）> Ethernet Settings（以太网设置）页面上配置 VLAN 后，将交换机上的以太网电缆重新连接至标记的包 (VLAN) 端口。然后，通过管理 Web 页面，重新连接至新的 IP 地址。（必要时，请向基础设施支持管理员核实 VLAN 和 DHCP 配置。）</p>

12.1.3 虚拟无线网络

如果您想要将内部网络配置为 VLAN（无论您是否配置了访客网络），可以在接入点上启用虚拟无线网络。

如果您想要按照第 160 页的“配置 VLAN”中所述，在 *Manage（管理）* > *VWN* 选项卡上配置 VLAN 上的附加虚拟网络，必须启用此功能。

表 12.4 启用虚拟无线网络

字段	描述
<i>Virtual Wireless Networks (Using VLANs on Ethernet Port 1)（虚拟无线网络（使用以太网端口 1 上的 VLAN））</i>	<ul style="list-style-type: none">选择 <i>Enabled（启用）</i> 为内部网络和附加网络启用 VLAN。（如果您选择此选项，无论您是否配置了 Guest Access（访客接入），均可以在 VLAN 上运行内部网络，并且可按照第 160 页的“配置 VLAN”中所述，使用 <i>Manage（管理）</i> > <i>VWN</i> 选项卡设置 VLAN 上的附加网络。）选择 <i>Disabled（禁用）</i> 将为内部网络以及此接入点上的所有其他虚拟网络禁用 VLAN。

12.1.4 内部接口设置

要配置内部 LAN 的以太网（有线）设置，请按照表 12.5 中所述填写字段。

表 12.5 内部 LAN 的以太网设置

字段	描述
<i>MAC Address (MAC 地址)</i>	显示此接入点上以太网端口的内部接口的 MAC 地址。此为只读字段，无法更改。
<i>VLAN ID</i>	<p>如果您选择按“VLAN”配置内部和访客网络，则此字段将会启用。</p> <p>对于内部 VLAN，提供 1 到 4094 之间的一个数字。</p> <p>这样导致接入点发送带有 VLAN 标记的 DHCP 请求。交换机和 DHCP 服务器必须支持 VLAN IEEE 802.1p 框架。接入点必须能够连接 DHCP 服务器。</p> <p>请咨询管理员，了解 VLAN 和 DHCP 配置。</p>

表 12.5 内部 LAN 的以太网设置（续）

字段	描述
<i>Management VLAN ID</i> （管理 VLAN ID）	<p>如果您已通过 VLAN 启用 VWN 或访客接入，将启用此字段。</p> <p>输入 Management VLAN ID（管理 VLAN ID）的值。此 ID 可以是 1 到 4094 之间的任何值。</p> <p>Management VLAN ID（管理 VLAN ID）使您能够指定用于管理 AP 的 VLAN。然后，您可以通过 Web 用户界面、命令行界面以及使用此 VLAN 的 SNMP，管理 AP。</p> <p>如果将连接类型设为 DHCP，将导致接入点发送带有 VLAN 标记的 DHCP 请求。交换机和 DHCP 服务器必须支持 VLAN IEEE 802.1Q 帧。接入点必须能够连接 DHCP 服务器。</p> <p>对于您指定的 Management VLAN ID（管理 VLAN ID）没有任何限制。Management VLAN ID（管理 VLAN ID）可以与 Internal VLAN ID（内部 VLAN ID）、Guest VLAN ID（访客 VLAN ID）、VWN VLAN ID 或 Untagged VLAN ID（未标记 VLAN ID）相同。</p>
<i>Untagged VLAN</i> （未标记 VLAN）	<p>如果您已通过 VLAN 启用 VWN 或访客接入，可以启用或禁用未标记 VLAN。</p> <p>选择 Enabled（启用）以启用 <i>Untagged VLAN</i>（未标记 VLAN）。</p> <p>选择 Disabled（禁用）以禁用 <i>Untagged VLAN</i>（未标记 VLAN）。</p> <p>如果启用 <i>Untagged VLAN</i>（未标记 VLAN），则收到的任何不带 VLAN 标记的包将被作为带指定未标记 VLAN ID 的包处理。</p> <p>如果禁用 <i>Untagged VLAN</i>（未标记 VLAN），则收到的任何不带 VLAN 标记的包将桥接至 WDS 链路，但不用于 AP。</p>
<i>Untagged VLAN ID</i> （未标记 VLAN ID）	<p>如果您已启用 <i>Untagged VLAN</i>（未标记 VLAN），将启用此字段。</p> <p>输入 <i>Untagged VLAN ID</i>（未标记 VLAN ID）的值。此 ID 可以是 1 到 4094 之间的任何值。</p> <p>对于您指定的 Untagged VLAN ID（未标记 VLAN ID）没有任何限制。Untagged VLAN ID（未标记 VLAN ID）可以与 Internal VLAN ID（内部 VLAN ID）、Guest VLAN ID（访客 VLAN ID）、VWN VLAN ID 或 Management VLAN ID（管理 VLAN ID）相同。</p>

表 12.5 内部 LAN 的以太网设置（续）

字段	描述
<i>Connection Type</i> (连接类型)	<p>您可以选择 DHCP 或 Static IP（静态 IP）。</p> <p>动态主机配置协议 (DHCP) 是指定中央服务器如何为网络上的设备提供网络配置信息的协议。DHCP 服务器向客户端系统提供“租赁”。提供的信息包括 IP 地址和网络掩码，以其 DNS 服务器和网关的地址。</p> <p>Static IP（静态 IP）表示手动提供所有网络设置。您必须提供产品名称的 IP 地址、子网掩码、默认网关的 IP 地址，以及至少一个 DNS 名称服务器的 IP 地址。</p> <p>如果您选择 DHCP，产品名称将从 DHCP 服务器获取其 IP 地址、子网掩码、DNS 以及网关信息。</p> <p>否则，如果您选择 Static IP（静态 IP），请填入 <i>静态 IP 设置</i> 中所述的项目。</p> <p>重要说明：如果您的内部网络上没有 DHCP 服务器且打算使用，则连接接入点后第一件要做的事就是将 Connection Type（连接类型）从“DHCP”更改为“Static IP”（静态 IP）。将 Connection Type（连接类型）更改为“Static IP”（静态 IP）后，您可以为 AP 分配新的静态 IP 地址，或继续使用默认地址。我们建议分配新的地址，以便稍后您在同一网络上连接另一个产品名称时，两个 AP 的 IP 地址是唯一的。</p> <p>如果您需要恢复默认的静态 IP 地址，可以按第 308 页的“重置出厂默认配置”中所述将 AP 重置为出厂默认值。</p>
<i>Static IP Address</i> (静态 IP 地址)	<p>如果您选择 Static IP（静态 IP）作为连接类型，将启用这些字段。</p> <p>在文本框中输入静态 IP 地址。</p>
<i>Subnet Mask</i> (子网掩码)	<p>在文本框中输入子网掩码。您必须从您的 ISP 或网络管理员那里获取此信息。</p>
<i>Default Gateway</i> (默认网关)	<p>在文本框中输入默认网关。</p>
<i>通过 DHCP 的 DNS 设置</i>	<p>域名服务 (DNS) 是将网络资源的描述性名称解析为数字 IP 地址的系统。您可以选择以启用此选项，将通过 DHCP 自动分配 DNS 服务器的 IP 地址。（只有当您指定 DHCP 为连接类型时，才会显示此选项。）</p> <p>如果您选择 Off（关闭），应手动分配静态 IP 地址。</p>

表 12.5 内部 LAN 的以太网设置（续）

字段	描述
<i>DNS Nameservers</i> (DNS 名称服务器)	域名服务(DNS) 是将网络资源的描述性名称（ 域名 ，例如 <i>www.psionteklogix.com</i> ）解析为数字 IP 地址（例如 66.93.138.219）的系统。DNS 服务器称为 <i>Nameserver</i> （名称服务器）。 通常有两台名称服务器：主名称服务器和辅助名称服务器。
<i>DNS Domain</i> (DNS 域)	识别 DNS 服务器的域。

12.1.5 访客接口设置

要配置“访客”接口的以太网（有线）设置，如下所述填写字段。

表 12.6 配置访客接口以太网设置

字段	描述
<i>MAC Address</i> (MAC 地址)	显示此接入点上以太网端口的访客接口的 MAC 地址。此为只读字段，无法更改。
<i>VLAN ID</i>	如果您选择按“VLAN”配置内部和访客网络，则此字段将会 启用 。 对于访客 VLAN，提供 1 到 4094 之间的一个数字。
<i>Subnet</i> (子网)	显示访客接口的子网地址。例如， 192.168.1.0。

12.1.6 更新设置

要更新以太网设置，请执行以下操作：

1. 导航至 *Ethernet Settings*（以太网设置）页面。
2. 根据需要配置以太网设置。
3. 单击 **Update**（更新）按钮应用更改。

设置无线接口

13

13.1 导航至无线设置	145
13.2 配置 802.11d 监管域支持	146
13.3 802.11h 监管域控制	146
13.4 配置射频接口	147
13.5 配置 “内部” 无线 LAN 设置	149
13.6 配置 “访客” 网络无线设置	149
13.7 更新无线设置	150

无线设置描述了与接入点中的射频设备特别相关的局域网 (*LAN*) 特性 (*802.11* 模式和信道) 以及与接入点的网络接口特别相关的特性 (接入点的 *MAC* 地址和无线网络名称, 也被称为 *SSID*)。

以下小节介绍了如何在产品名称上配置 “无线” 地址以及相关的设置, 包括 802.IQv1。

13.1 导航至无线设置

要设置接入点的无线地址, 请导航至 *Manage* (管理) > *802.11 Settings* (802.11 设置) 选项卡, 将打开 *Wireless Settings* (无线设置) 页面, 并如下所述更新字段。



注释: 图 13.1 显示了双射频 AP 的 *Wireless Settings* (无线设置) 页面。单射频 AP 的管理 Web 页面外观略有不同。

图 13.1 无线设置配置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

Modify wireless settings

802.11d Regulatory Domain Support ☒ Enabled ☐ Disabled
IEEE802.11h support present.

Radio Interface

Mode

IEEE 802.11g

Channel

6

Internal Settings

MAC Address 00:08:A2:01:4B:56

SSID

SFG

Guest Settings

MAC Address

SSID

TEKLOGIX GUEST

Update

13.2 配置 802.11d 监管域支持

您可以启用或禁用 IEEE 802.11d 监管域支持，按如下所述广播接入点的国家/地区代码信息。

表 13.1 启用 802.11d 支持

字段	描述
802.11d Regulatory Domain Support (802.11d 监管域支持)	<p>在接入点上启用对 IEEE 802.11d 支持后，作为 AP 信标的组成部分，AP 会广播其运行时所在的国家/地区：</p> <ul style="list-style-type: none">要启用 802.11d 监管域支持，单击 Enabled（启用）。要禁用 802.11d 监管域支持，单击 Disabled（禁用）。对于双射频 AP，会显示两个 MAC 地址：内部接口上每个射频一个 MAC 地址。 <p>注：IEEE 802.11d 定义在任何国家/地区运行 IEEE 802.11 无线 LAN 的标准规则，无需重新配置。IEEE 802.11d 允许客户端工作站在任何国家/地区运行，无需重新配置。Devicescape 参考 AP 必须由制造商通过命令行接口 (CLI) 国家/地区代码进行配置，以便在特定国家/地区运行。</p>

13.3 802.11h 监管域控制

表 13.2 IEEE 802.11h 标准

字段	描述
IEEE 802.11h	<p>管理 UI 将显示 IEEE 802.11h 监管域控制对 AP 是否生效。最终用户管理员无法禁用 IEEE 802.11h。以下详细信息仅供参考。</p> <p>IEEE 802.11h 是提供满足 5GHz 频段的特定监管域所需的两项服务的标准。这两项服务分别是传输功率控制 (TPC) 和动态频率选择 (DFS)。</p> <ul style="list-style-type: none">TPC 要求在 5 GHz 频段中运行的射频局域网 (RLAN) 使用发射功率控制。这就需要遵守规定的最大发射输出功率以及各个允许信道的缓解要求。这样就可减少了对卫星服务的干扰。DFS 要求在 5 GHz 频段中运行的 RLAN 实施一种机制，以避免与雷达系统共用信道，确保统一利用任何可用的信道。 <p>注：如果将 AP 配置成在 802.11h 作为最低标准的任何国家/地区工作，802.11h 会自动启用。目前，只有划入欧洲电信标准协会 (ETSI) 类别的国家/地区要求达到此标准。802.11h 也适用于日本。</p>

AP 开发人员需要谨记与 IEEE **802.11h** 标准相关的以下关键点：

- 802.11h 仅可用于 802.11a 频段。对于 802.11b 或 802.11g 不需要。
- 如果您在支持 802.11h 的域中运行，则 BBS 信道选择始终为 “Auto”（自动）。即使已配置其他信道，也会忽略并自动选择信道。
- 启用 802.11h 后，初始启动时间最少增加 60 秒。这是扫描选定信道的雷达干扰所需的最短时间。
- 802.11h 运行时，可能很难设置 WDS 链路。这是因为 WDS 链路上两个 AP 的工作信道会不断改变，具体取决于信道使用情况和雷达干扰。只有 AP 在相同信道上运行时，WDS 才会工作。有关 WDS 详细信息，请参阅第 20 章：“无线分布系统”。

13.4 配置射频接口

射频接口允许您按表 13.3 中所述设置无线电信道和 802.11 模式。



注释：在双射频 AP 上，您必须为射频接口 1 和射频接口 2 配置射频接口设置。

表 13.3 射频接口设置

字段	描述
MAC Addresses (MAC 地址) (仅显示在双射频 AP 上)	<p>表示接口的媒体访问控制 (MAC) 地址。</p> <p>射频接口 1（内部/访客）和射频接口 2（内部/访客）的 MAC 地址仅在双射频 AP 上显示。</p> <p>MAC 地址是代表网络接口的任何设备的永久性、唯一的硬件地址。MAC 地址由制造商分配。您无法更改 MAC 地址。作为接口的唯一标识符，在此仅出于信息目的提供。</p>

表 13.3 射频接口设置 （续）

字段	描述
<i>Mode</i> （模式）	<p><i>Mode</i>（模式）定义该射频使用的 <i>物理层(PHY)</i> 标准。</p> <p>产品名称可用作具有一个或两个射频的单频段或双频段接入点。<i>Mode</i>（模式）的配置选项取决于您使用的产品。</p> <p>单频段 AP： 对于单频段 AP，选择以下模式之一：</p> <ul style="list-style-type: none">• IEEE <i>802.11b</i>• IEEE <i>802.11g</i> <p>双频段 AP： 对于双频段 AP，选择以下模式之一：每个射频接口一种模式。</p> <ul style="list-style-type: none">• IEEE <i>802.11b</i>• IEEE <i>802.11g</i>• <i>IEEE 802.11a</i> <p>单射频或双射频 AP： 如果您使用的是双射频 AP，为两个射频接口选择 IEEE 802.11 模式。（对于单射频 AP，只有一个射频接口。）</p>
<i>Channel</i> （信道）	<p>选择 <i>信道</i>。信道范围和默认值由射频接口的 <i>模式</i> 确定。</p> <p><i>信道</i>定义射频用来收发无线电信号的射频频谱部分。各种模式提供大量信道，具体取决于国家和跨国机构，例如联邦通信委员会 (FCC) 或国际电信联盟 (ITU-R) 许可频谱的方式。</p> <p>默认值为 Auto（自动），启动时挑选最不繁忙的信道。</p>

13.5 配置 “内部” 无线 LAN 设置

内部设置描述内部无线 LAN (WLAN) 的 *MAC* 地址（只读）和网络名称（也称为 *SSID*），如表 13.4 中所述。

表 13.4 无线 LAN 设置

字段	描述
<i>MAC Address</i> (<i>MAC 地址</i>)	显示此接入点内部接口的 <i>MAC</i> 地址。此为只读字段，无法更改。 尽管此接入点实际上是一台设备，它在网络上可表现为两个或更多节点，每个节点都有一个唯一的 <i>MAC</i> 地址。对单个接入点使用多个 <i>基本服务集标识符 (BSSID)</i> 即可实现。 “内部” 接入点显示的 <i>MAC</i> 地址是 “内部” 接口的 <i>BSSID</i> 。 对于双射频 AP，显示两个 <i>MAC</i> 地址：内部接口上的每个射频各显示一个。
<i>Wireless Network Name (SSID)</i> (<i>无线网络名称 (SSID)</i>)	输入内部 WLAN 的 <i>SSID</i> 。 <i>服务集标识符 (SSID)</i> 是最长 32 个字符的字母数字字符串，唯一地标识无线局域网。它也被称为 <i>网络名称</i> 。对于在 <i>SSID</i> 中使用的字符没有任何限制。

13.6 配置 “访客” 网络无线设置

访客设置描述 *访客网络* 的 *MAC* 地址（只读）和无线网络名称 (*SSID*)，如表 13.5 中所述。配置有两个不同的网络名称 (*SSID*) 的接入点，允许您在产品名称上使用访客接口功能。有关详细信息，请参阅第 14 章：“设置访客接入”。

表 13.5 访客网络无线设置

字段	描述
<i>MAC Address</i> (<i>MAC 地址</i>)	显示此接入点访客接口的 <i>MAC</i> 地址。此为只读字段，无法更改。 尽管此接入点实际上是一台设备，它在网络上可表现为两个或更多节点，每个节点都有一个唯一的 <i>MAC</i> 地址。对单个接入点使用多个 <i>基本服务集标识符 (BSSID)</i> 即可实现。 “访客” 接入点显示的 <i>MAC</i> 地址是 “访客” 接口的 <i>BSSID</i> 。 对于双射频 AP，显示两个 <i>MAC</i> 地址：访客接口上的每个射频各显示一个。
<i>Wireless Network Name (SSID)</i> (<i>无线网络名称 (SSID)</i>)	输入 <i>访客网络</i> 的 <i>SSID</i> 。 <i>服务集标识符 (SSID)</i> 是最长 32 个字符的字母数字字符串，唯一地标识无线局域网。它也被称为 <i>网络名称</i> 。对于在 <i>SSID</i> 中使用的字符没有任何限制。 对于访客网络，提供不同于内部 <i>SSID</i> 且可轻松识别为 “访客” 网络的 <i>SSID</i> 。

13.7 更新无线设置

要更新无线设置，请执行以下操作：

1. 导航至 *802.11 Settings*（802.11 设置）页面。
2. 根据需要配置无线设置。
3. 单击 **Update**（更新）按钮应用更改。

设置访客接入

14

14.1 了解访客接口	153
14.2 配置访客接口	153
14.2.1 在虚拟 LAN 上配置访客网络	154
14.2.2 配置欢迎屏幕（强制网络门户）	154
14.3 将访客网络用作客户端	155
14.4 部署示例	156

开箱即用的 **访客接口** 功能允许配置产品名称，以控制访客对独立网络的访问。同一个接入点可以配置为两个不同的无线网络进行广播和工作：分别是安全的“内部” LAN 和公共“访客”网络。访客客户端无需提供用户名或密码便可访问访客网络。访客登录后，会看到访客欢迎屏幕（也被称为“强制网络门户”）。

14.1 了解访客接口

您可以定义访客连接的独特参数，并将访客客户端与该网络其他更敏感的区域隔离。



重要说明： 访客网络不提供任何安全性；只允许纯文本安全模式。

同时，您可以配置安全的 **内部网络**（使用与访客接口相同的接入点），提供对防火墙后受保护信息的完整访问权限，并要求提供安全登录信息或证书才能进行访问。

您可以对用于访客接口的产品名称进行配置，方法是使用具有 VLAN 的单个网络，并在产品名称的管理 Web 页面上设置访客接口配置选项。（有关如何设置此类型访客接口的详细信息，请参阅第 154 页的“在虚拟 LAN 上配置访客网络”。



注释： 此方法利用 9160 G2 无线网关内置的多种 **BSSID** 和虚拟 LAN (VLAN) 技术。内部网络和访客网络作为同一个接入点上的多个 BSSID 实施，每一个都在无线接口上具有不同的网络名称 (SSID)，并在有线接口上具有不同的 VLAN ID。

在双射频接入点上，访客管理和登录设置同时应用于射频一和射频二。

14.2 配置访客接口

要配置产品名称上的访客接口，请执行以下步骤：

1. 如以下小节，“在虚拟 LAN 上配置访客网络”中所述，将接入点配置为代表两个虚拟的独立网络。
2. 如第 154 页的“配置欢迎屏幕（强制网络门户）”小节中所述，设置访客强制网络门户的访客欢迎屏幕。



注释： 集群上的接入点不共享访客接口设置。这些设置必须在管理页面上针对各个接入点单独配置。要转至当前集群成员接入点的管理页面，请在当前 AP 的 Cluster（集群）> Access Points（接入点）页面上，单击 **IP Address**（IP 地址）链接。有关集群共享和不共享的设置的更多信息，请参阅第 54 页的“哪些设置可以/不可以作为集群配置的组成部分进行共享？”。

14.2.1 在虚拟 LAN 上配置访客网络



注释： 如果要配置虚拟 LAN (VLAN) 上的访客网络和内部网络，则使用的交换机和 DHCP 服务器必须支持 VLAN。

作为前提步骤，请按照 IEEE 802.1Q 标准中所述配置交换机上用于处理带有 VLAN 标记的数据包的端口。

集群上的接入点不共享访客欢迎屏幕设置。更新某个接入点的设置时，集群中的其他接入点将共享该配置。有关集群共享和不共享的设置的更多信息请参阅第 54 页的“哪些设置可以/不可以作为集群配置的组成部分进行共享？”。

要配置虚拟 LAN 上的内部网络和访客网络，请执行以下操作：

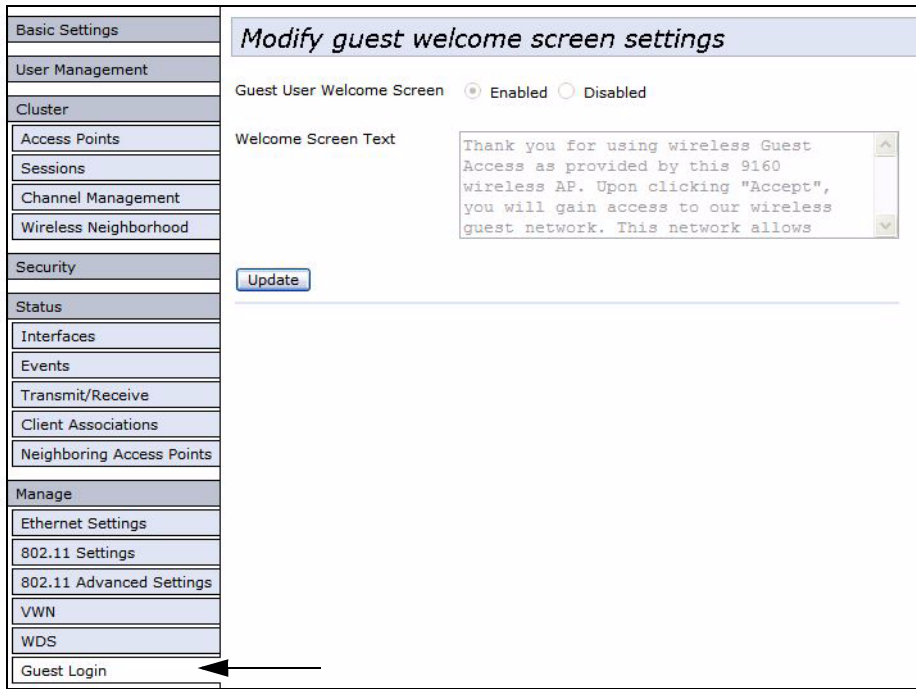
1. 仅在接入点上的网络端口与 LAN 之间使用一个有线连接。（确保将此端口配置为处理带有 VLAN 标记的数据包）。
2. 如第 12 章：“以太网（有线）接口”中的小节所述，在 VLAN 上配置内部网络和访客网络的以太网（有线）设置。
（先启用访客接入，然后选择对于内部访问和访客访问，使用两个 VLAN，如第 137 页的“指定虚拟访客网络”中所述。）
3. 提供内部网络和访客网络的射频接口设置和网络名称 (SSID)，如第 13 章：“设置无线接口”中所述。
4. 如第 154 页的“配置欢迎屏幕（强制网络门户）”中所述配置访客初始屏幕。

14.2.2 配置欢迎屏幕（强制网络门户）

您可以设置或修改访客客户端打开 Web 页面或尝试浏览 Web 时看到的欢迎屏幕。要设置强制网络门户，请执行以下操作：

1. 导航至 *Manage*（管理）> *Guest Login*（访客登录）选项卡。

图 14.1 访客登录屏幕设置



- 2. 选择 **Enabled** （启用）以启用欢迎屏幕。
- 3. 在 *Welcome Screen Text* （欢迎屏幕文本）字段中，输入您希望访客客户端在强制网络门户上看到的文本消息。
- 4. 单击 **Update** （更新）应用更改。

14.3 将访客网络用作客户端

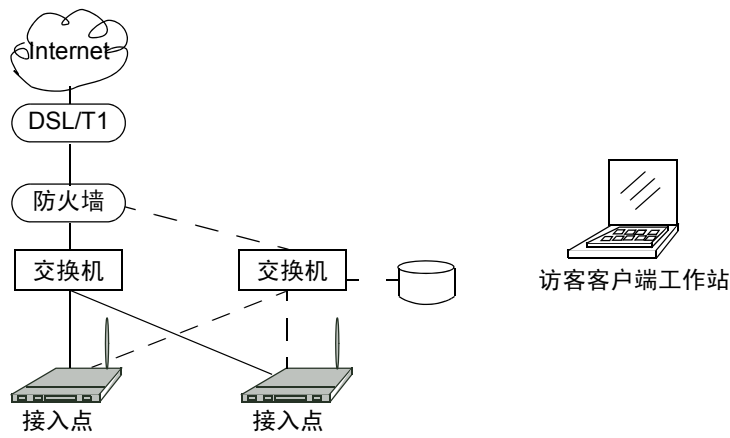
配置访客网络后，客户端便可以如下所示访问访客网络：

- 1. 访客客户端进入覆盖区域并扫描无线网络。
- 2. 访客网络通过访客 SSID 或类似的名称推广自己，具体取决于在访客接口的管理 Web 页面中指定访客 SSID 的方式。
- 3. 访客客户端选择访客 SSID。
- 4. 访客客户端启动 Web 浏览器并看到访客欢迎屏幕。
- 5. 单击访客欢迎屏幕上的一个按钮即可继续。
- 6. 访客客户端现可使用“访客”网络。

14.4 部署示例

在图 14.2 中，虚线表示专用的访客连接。从相同的产品名称管理 Web 页面管理所有接入点和所有连接（包括访客）。

图 14.2 专用的访客连接



15.1 导航至虚拟无线网络设置.	159
15.2 配置 VLAN.	160
15.3 更新设置	161

以下小节介绍如何在虚拟 LAN (VLAN) 上配置多个无线网络。

15.1 导航至虚拟无线网络设置

要在 VLAN 上设置多个网络，请导航至 *Manage*（管理）> *VWN* 选项卡，然后如下所述更新字段。

图 15.1 VWN 设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Modify Virtual Wireless Network settings

Virtual Wireless Networks : Disabled

VWN	Enabled	VLAN ID	SSID	Broadcast SSID	Security
1	<input type="checkbox"/>		Virtual Wireless Network 1	<input checked="" type="checkbox"/>	None
2	<input type="checkbox"/>		Virtual Wireless Network 2	<input checked="" type="checkbox"/>	None

Update

15.2 配置 VLAN



注释：要在 VLAN 上配置其他网络，必须首先在 Ethernet Settings（以太网设置）页面上启用 Virtual Wireless Networks（虚拟无线网络）。请参阅第 138 页的“虚拟无线网络”。



重要说明：如果您配置 VLAN，可能会丢失与接入点的连接。首先，确保根据 IEEE 802.1Q 标准验证您使用的交换机和 DHCP 服务器支持 VLAN。配置 VLAN 后，将交换机上的以太网电缆重新连接至标记的数据包 (VLAN) 端口。然后，通过管理 Web 页面，重新连接至新的 IP 地址。（如有必要，请咨询基础设施支持管理员，了解 VLAN 和 DHCP 配置。）

表 15.1 虚拟无线网络设置

字段	描述
Virtual Wireless Network（虚拟无线网络）	最多可以配置 6 个 VWN。
Enabled（启用）	您可以启用或禁用配置的网络。 <ul style="list-style-type: none">要启用指定的网络，请选中相应的 VWN 旁的 Enabled（启用）复选框。要禁用指定的网络，请取消选中相应的 VWN 旁的 Enabled（启用）复选框。 禁用指定的网络后，将会丢失您输入的 VLAN ID。
VLAN ID	对于内部 VLAN，提供 1 到 4094 之间的一个数字。 这样导致接入点发送带有 VLAN 标记的 DHCP 请求。交换机和 DHCP 服务器必须支持 VLAN IEEE 802.1Q 帧。接入点必须能够连接 DHCP 服务器。 请咨询管理员，了解 VLAN 和 DHCP 配置。
SSID	以字符串的形式输入无线网络的名称。该名称将应用到此网络上的所有接入点。添加更多接入点时，它们将共享此 SSID。 服务集标识符 (SSID) 是一个限长 32 个字符的字母数字字符串。 注： 如果您作为无线客户端连接到管理的相同 AP，则重置 SSID 会导致您丢失与 AP 的连接。保存新设置后，您需要重新连接至新的 SSID。

表 15.1 虚拟无线网络设置 （续）

字段	描述
<i>Broadcast SSID</i> (广播 SSID)	<p>选中 Broadcast SSID（广播 SSID）复选框，选择 <i>Broadcast SSID</i>（广播 SSID）设置。</p> <p>默认情况下，接入点广播（允许）其信标帧中的 <i>服务集标识符</i>(SSID)。</p> <p>您可以抑制（禁止）此广播，阻止工作站自动发现您的接入点。抑制该 AP 的广播 SSID 时，客户端工作站上的 <i>List of Available Networks</i>（可用网络列表）中将不显示网络名称。客户端必须在请求方中配置确切的网络名称，才能进行连接。</p> <p>注： 您在这里设置的广播 SSID 专用于此虚拟网络（一或二）。其他网络继续使用已配置的安全模式：</p> <ul style="list-style-type: none">• 您的原始内部网络（在 <i>Ethernet Settings</i>（以太网设置）页面上配置）使用在 <i>Security</i>（安全）上设置的广播 SSID。• 如果配置访客网络，则始终允许广播 SSID。
<i>Security</i> （安全）	<p>选择此 VLAN 的 <i>Security Mode</i>（安全模式）。选择下列选项之一：</p> <ul style="list-style-type: none">• None (Plain-text)（无（纯文本））• Static WEP（静态 WEP）• WPA Personal（WPA 个人版） <p>注： 您在此处设置的安全模式专用于该虚拟网络。其他网络继续使用已配置的安全模式：</p> <ul style="list-style-type: none">• 您的原始内部网络（在 <i>Ethernet Settings</i>（以太网设置）页面上配置）使用在 <i>Security</i>（安全）上设置的安全模式。• 如果配置访客网络，始终将安全模式设为“None”（无）。

15.3 更新设置

要更新 VLAN 设置，请执行以下操作：

1. 导航至 *VWN* 选项卡页面。
2. 根据需要配置 VLAN 设置。
3. 单击 **Update**（更新）按钮应用更改。

配置 802.11 射频设置

16

16.1 了解无线通信设置	165
16.2 导航至无线通信设置	165
16.3 配置无线通信设置	167
16.4 更新设置	171

以下各节阐述了如何在产品名称上配置 802.11 无线通信设置：

16.1 了解无线通信设置

无线通信设置直接控制接入点中的无线通信设备的行为，及其与物理介质之间的交互；即，AP 发射电磁波的方式/类型。您可以指定打开或关闭无线通信、射频 (RF) 广播信道、信标间隔（AP 信标传输之间的时间量）、发射功率、无线通信运行的 IEEE 802.11 模式等。

产品名称配置为具有一个射频的双频段接入点。

接入点能够在下列模式下进行广播：

- IEEE 802.11b 模式。
- IEEE 802.11g 模式。
- IEEE 802.11a 模式。
- Atheros Turbo 5 GHz。
- Atheros Dynamic Turbo 5 GHz。
- Atheros Turbo 2.4 GHz。
- Atheros Dynamic Turbo 2.4 GHz。
- 扩展范围。



重要说明： Psion Teklogix 移动数据终端不支持 Atheros Turbo 模式，并且为了防止不必要的无线通信开销，不建议使用 Turbo 模式。

如第 165 页的“导航至无线通信设置”和第 167 页的“配置无线通信设置”中所述，配置 IEEE 模式及其他无线通信设置。

16.2 导航至无线通信设置

要指定无线通信设置，请导航至 *Manage*（管理）> *802.11 Advanced Settings*（高级设置）选项卡，该操作将打开 *Radio Settings*（无线通信设置）页面，并如第 167 页的表 16.1 中所述更新字段。

图 16.1 无线通信设置配置概述

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Modify radio settings

Status ☒ On ☐ Off

Mode IEEE 802.11g

Super AG ☐ Enabled ☒ Disabled

Extended Range ☐ Enabled ☒ Disabled

Channel 6

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, Even Numbers)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 2007 (Range: 0-2007)

Transmit Power 100 Percent

Rate Supported Basic

54 Mbps ☒ ☐

48 Mbps ☒ ☐

36 Mbps ☒ ☐

24 Mbps ☒ ☐

18 Mbps ☒ ☐

12 Mbps ☒ ☐

11 Mbps ☒ ☒

9 Mbps ☒ ☐

6 Mbps ☒ ☐

5.5 Mbps ☒ ☒

2 Mbps ☒ ☒

1 Mbps ☒ ☒

Rate Sets

☐ Broadcast/Multicast Rate Limiting

Rate Limit 50 (packets per second)

Rate Limit Burst 75 (packets per second)

166 Psion Teklogix 9160 G2 无线网关用户手册

16.3 配置无线通信设置

表 16.1 射频设置

字段	描述
<i>Radio</i> (射频)	<p>产品名称可用作单射频或双射频接入点。</p> <p>单射频 AP: 如果您使用的是单射频版本的产品名称，则 Radio（射频）选项卡中不包含此字段。</p> <p>双射频 AP: 如果您使用的是双射频版本的产品名称，请指定射频一或射频二。在双射频 AP 上，此选项卡的其他设置应用于此字段中选择的射频。确保配置两个射频的设置。</p>
<i>Status (On/Off)</i> (状态 (开/关))	<p>指定是否通过单击 On（开）或 Off（关）来打开或关闭射频。</p>
<i>Mode</i> (模式)	<p><i>Mode</i>（模式）定义该射频使用的物理层(PHY)标准。</p> <p>产品名称可用作单频段或双频段接入点。</p> <p>单频段 AP: 对于单频段 AP，选择以下其中一种模式：</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g <p>双频段 AP: 对于双频段 AP，选择以下其中一种模式：</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g• IEEE 802.11a <p>注：如果您使用的是双射频 AP，根据在上述的 Radio（射频）字段中选择 Radio One（射频一）或 Radio Two（射频二），将提供不同的模式。</p> <p>选择射频模式后，会自动为该模式选择相应的基本和支持速率集。（请参阅 第 170 页此表靠下位置的速率设置描述。）</p>
<i>Super AG</i>	<p>启用 Super AG 后，通过增加无线通信模式（IEEE 802.11b、g、a 等）的无效通信吞吐量，提供更好的性能。请记住，启用 Super AG 后，接入点传输将会消耗多带宽。</p> <ul style="list-style-type: none">• 要启用 Super AG，单击 Enabled（启用）。• 要禁用 Super AG，单击 Disabled（禁用）。

表 16.1 射频设置 （续）

字段	描述
<i>Extended Range</i> (扩展范围)	<p>Atheros 扩展范围 (XR) 是在较长距离内实施低速率流量的专有方法。它对启用 XR 的客户端和接入点是透明的，并可与 802.11g 和 802.11a 模式下的 802.11 标准实现互操作性。不支持 802.11b 模式下的 Atheros XR、Atheros Turbo 5 GHz 或 Atheros Dynamic Turbo 5 GHz。</p> <p>启用 Atheros XR 后，将扩展客户端及接入点运行的范围。</p> <ul style="list-style-type: none">• 要启用扩展范围，单击 Enabled（启用）。• 要禁用扩展范围，单击 Disabled（禁用）。 <p>如果您选择硬件模式 IEEE 802.11b、Atheros Turbo 5 GHz 或 Atheros Dynamic Turbo 5 GHz，此选项将不可用。上述硬件模式不支持 Atheros XR。</p>
<i>Channel</i> (信道)	<p>信道定义了用于收发射频的射频频谱部分。信道范围和默认信道由射频接口的模式确定。</p> <p>对于大多数模式而言，默认值为 Auto（自动）。建议使用自动模式，因为使用该模式后系统会根据信号强度、流量负载等自动检测最佳信道选项。但是，您还可以在 1 到 11 之间选择一个信道。</p>
<i>Beacon Interval</i> (信标间隔)	<p>接入点每隔一段时间就会传输 信标帧，表示存在无线网络。默认行为是每 100 毫秒发送一个信标帧（或每秒发送 10 个信标帧）。</p> <p>以毫秒为单位设置 <i>Beacon Interval</i>（信标间隔）值。输入 20 到 2000 之间的一个值。</p>
<i>DTIM Period</i> (DTIM 周期)	<p>传输流量信息图 (DTIM) 消息是某些 信标帧中包含的元素。它指示当前哪些客户端工作站在低功率睡眠模式下接入点上有缓冲数据等待提取。</p> <p>在此处规定的 DTIM 周期表示此接入点服务的客户端应多长时间检查一次在 AP 上等待提取的缓冲数据。</p> <p>在给定的范围 (1 - 255) 内指定 DTIM 周期。</p> <p>测量单位为信标。例如，如果将其设为 1，客户端将在每一个信标检查一次 AP 上缓冲的数据。如果将其设为 2，客户端应每隔一个信标进行一次检查。如果将其设为 10，客户端应每 10 个信标进行一次检查。</p>

表 16.1 射频设置 （续）

字段	描述
<i>Fragmentation Threshold</i> (分段阈值)	<p>指定 256 和 2346 之间的一个数字，设置为帧的大小（以字节为单位）。</p> <p>分段阈值限制通过网络传输的数据包（帧）的大小。如果数据包超过这里设置的分段阈值，将会启用分段功能，且该数据包将作为多个 802.11 帧发送。</p> <p>如果正在传输的数据包等于或小于该阈值，将不使用分段。</p> <p>将阈值设为最大值（2,346 字节），会有效禁用分段。</p> <p>分段涉及更多开销，这是因为不仅需要进行帧的分割及重组的额外工作，还会增加网络上的消息流量。但是，分段可帮助改进网络性能和可靠性（如果配置正确）。</p> <p>使用更低的分段阈值发送较小的帧可以帮助解决一些干扰问题（例如，微波炉）。</p> <p>默认情况下，分段关闭。我们不建议使用分段，除非怀疑存在射电干扰。应用到各分段的额外标头增加了网络上的开销，并会大大减少吞吐量。</p>
<i>RTS Threshold</i> (RTS 阈值)	<p>指定 0 和 2347 之间的一个 RTS 阈值 值。</p> <p>RTS 阈值指定了发送 (RTS) 传输请求的数据包大小。这有助于控制通过接入点的流量，尤其是有大量客户端的接入点。</p> <p>如果指定较低的阈值，RTS 数据包的发送频率将会更频繁。这会消耗更多带宽，并降低数据包的吞吐量。</p> <p>另一方面，发送更多 RTS 数据包可帮助网络从忙碌网络或有电磁干扰的网络上可能发生的干扰或冲突恢复。</p>
<i>Maximum Stations</i> (最大站点数)	<p>指定允许在任何时间访问此 AP 的站点的最大数量。</p> <p>可以输入 0 和 2007 之间的一个值。</p>
<i>Transmit Power</i> (发射功率)	<p>提供一个百分比值，设置此接入点的发射功率。</p> <p>默认值是使用 100% 的功率进行接入点传输。</p> <div> 建议：</div> <ul style="list-style-type: none">在大多数情况下，我们建议使用默认值，并将发射功率设为 100%。这种方法是最有效的，因为它向接入点提供了最大的广播范围，并减少了所需的 AP 数量。如需增加网络容量，请将 AP 放得近一些，并减少发射功率值。这将有助于减少 AP 之间的重叠和干扰。较低的发射功率设置还可提高您网络的安全性这是因为无线信号越弱，就越不可能在网络的物理位置范围之外进行传播。

表 16.1 射频设置 （续）

字段	描述
<i>Rate Sets</i> (速率设置)	<p>查看您希望接入点支持的传输速率设置，以及您希望接入点使用的基本速率设置。</p> <p>以兆位/秒为单位表示速率。</p> <ul style="list-style-type: none">• 支持的速率设置表示接入点支持的速率。您可以查看多个速率（单击复选框选中或取消选中速率）。AP 将会根据错误率以及客户端与 AP 的距离等因素，自动选择最有效的速率。• 基本速率设置表示接入点出于设置与网络上其他 AP 和客户端工作站之间的通信目的，应用到网络的速率。通过 AP 广播其支持速率设置子集的方式通常更为有效。 <p>要支持“b”和“g”客户端，请将射频模式更改为 IEEE 802.11g。Web UI 将会自动选择允许“b”和“g”客户端进行连接的默认速率设置。</p> <p>要仅支持“g”客户端，请将射频模式更改为 IEEE 802.11g。Web UI 将会自动选择默认速率设置。现在，添加 24、12 和 6 作为基本速率。这样，会阻止“b”客户端进行连接，这是因为它们不支持这些速率；但允许“g”客户端连接，因为标准要求它们支持这些速率。</p> <p>有关更多信息，请参阅第 167 页 页上此表靠上部分的 <i>Mode</i>（模式）描述。</p>
<i>Enable Broadcast/Multicast Rate Limiting</i> (启用广播/多播速率限制)	<p>启用广播/多播速率限制后，可通过限制网络上传输的数据包数量来改进整体网络性能。</p> <p>对于网络上的大多数节点不感兴趣的流量，某些协议使用多播和广播数据包。例如，ARP 请求其他机器、DHCP 或 BOOTP 消息。对于某些协议，如果设置速率限制控制，实际上是限制网络上传输的冗余数据包的数量。通常情况下，任何过滤流量将会于稍后重新传输，且不会造成困难。</p> <ul style="list-style-type: none">• 要启用多播/广播速率限制，单击 Enabled（启用）。• 要禁用多播/广播速率限制，单击 Disabled（禁用）。 <p>默认情况下禁用 <i>Multicast/Broadcast Rate Limiting</i>（多播/广播速率限制）选项。在启用 <i>Multicast/Broadcast Rate Limiting</i>（多播/广播速率限制）之前，禁用以下字段。</p>
<i>Broadcast/Multicast Rate Limit</i> (广播/多播速率限值)	<p>输入您想要为多播和广播流量设置的速率限值。该限值应大于每秒 1 个数据包，小于每秒 50 个数据包。低于此速率限值的任何流量将符合相应目的地的要求，并传输至目的地。</p> <p>默认和最大速率限值设置为每秒 50 个数据包。</p>
<i>Broadcast/Multicast Rate Limit Burst</i> (广播/多播速率突破最大值)	<p>设置速率突破最大值，确定所有流量超出速率限值前突发多少流量。此突发限值允许网络上间断突发的流量超出设置速率限值。</p> <p>默认和最大速率突破最大值设置为每秒 75 个数据包。</p>

16.4 更新设置

要更新射频设置：

1. 导航至 *802.11 Advanced Settings*（802.11 高级设置）选项卡页面。
2. 根据需要配置射频设置。
3. 单击 **Update**（更新）按钮应用更改。



注释：如果您使用双射频版本的 9160 G2 无线网关，请谨记在此选项卡上配置射频一和射频二。显示的设置应用于射频一或射频二，这取决于您在 **Radio**（射频）字段（选项卡上的第一个字段）中选择哪个射频。配置其中一个射频设置后，单击 **Update**（更新），然后选择并配置另一个射频。确保单击 **Update**（更新），应用另一个射频的第二个配置设置集。

MAC 地址过滤

17

17.1 导航至 MAC 过滤设置	175
17.2 使用 MAC 过滤	176
17.3 更新设置	176

媒体访问控制(MAC)地址是唯一标识网络各个节点的硬件地址。所有 IEEE 802 网络设备均共享一个通用的 48 位 MAC 地址格式，通常显示为使用分号分隔的 12 个十六进制数字的字符串，例如 FE:DC:BA:09:87:65。无线客户端使用的每个无线网络接口卡 (NIC) 都有一个唯一的 MAC 地址。

您可以通过打开 *MAC Filtering* (MAC 过滤) 并指定批准的 MAC 地址列表，来控制客户端对无线网络的访问。打开 AC 过滤 时，仅具有列出的 MAC 地址的客户端可以访问网络。

以下小节介绍了如何在产品名称上使用 MAC 地址过滤。

17.1 导航至 MAC 过滤设置

要启用按 MAC 地址过滤，请导航至 *Manage* (管理) > *MAC Filtering* (MAC 过滤) 选项卡，并如下所述更新字段。

图 17.1 MAC 过滤设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Configure MAC Filtering of client stations

Filter

☐ Allow only stations in list

☒ Block all stations in list

Stations List

10:10:10:10:14:44

Remove

: : : : : Add

Update

17.2 使用 MAC 过滤

此页面允许您基于 *媒体访问控制* (MAC) 地址控制对产品名称的访问。根据您的设置过滤器的情况，您可以仅 *允许* 具有列出的 MAC 地址的客户端工作站，或 *阻止* 访问所列的工作站。

对于访客接口，**MAC** 过滤设置同时应用到两个 **BSS**。

在双射频的 AP 上，MAC 过滤设置应用于两个射频

表 17.1 MAC 过滤设置

字段	描述
<i>Filter</i> (过滤器)	要设置 MAC 地址 <i>过滤器</i> ，单击以下单选按钮之一： <ul style="list-style-type: none">Allow only stations in the list （仅允许列表中的工作站）Block all stations in list （阻止列表中的工作站）
<i>Stations List</i> (工作站列表)	要在 Stations List （工作站列表）中添加 MAC 地址，在下面的文本框内输入 48 位 MAC 地址，然后单击 Add （添加）。 MAC 地址将添加到 Stations List （工作站列表）中。 要从 Stations List （工作站列表）中删除 MAC 地址，请选择它的 48 位 MAC 地址，然后单击 Remove （删除）。 根据您的设置过滤器的方式，将允许或阻止列表中的工作站访问 AP。

17.3 更新设置

要更新 MAC 设置，请执行以下操作：

1. 导航至 *MAC Filtering* （MAC 过滤）选项卡页面。
2. 根据需要配置 MAC 设置。
3. 单击 **Update** （更新）按钮应用更改。

18.1 了解负载均衡	179
18.1.1 识别不平衡：使用过度或使用过少的接入点	179
18.1.2 指定利用率和客户端关联的限值	179
18.1.3 负载均衡和 QoS	179
18.2 导航至负载均衡设置	179
18.3 配置负载均衡	180
18.4 更新设置	181

产品名称允许您平衡多个接入点上无线客户端连接的分布。使用负载均衡，您可以防止网络中的单个接入点出现性能降级的情况，这是因为它会处理无线流量分配不均的情况。

以下小节介绍如何在无线网络上配置负载均衡。

18.1 了解负载均衡

和产品名称上的大多数配置设置一样，在集群接入点之间共享负载均衡设置。



注释：在某些情况下，您可能仅想要对持续使用过度的一个接入点设置限制。特定接入点在独立模式下运行时，您可向其应用独特的设置。（请参阅第 53 页的“了解集群”和第 53 页的“导航至接入点管理”。）

18.1.1 识别不平衡：使用过度或使用过少的接入点

典型的场景是将多个接入点的客户端关联数据与发射/接收数据进行比较，从而找出持续处理的无线流量比例过大的接入点。当位置放置或其他因素导致一个接入点将最强的信号发射至网络上的大多数客户端时，会发生这种情况。默认情况下，该接入点将接收大多数客户端请求，而其他接入点大多时间是空闲的。

接入点上的无线流量分布不平衡，在客户端关联数据和发射/接收统计数据中非常明显，该统计数据显示使用过度的 AP “利用率”较高，而使用过少的 AP “空闲”时间较多。处理流量超过其公平分配流量的 AP 还由于过载而显示出较慢的数据速率或较低的发射/接收率。

18.1.2 指定利用率和客户端关联的限值

您可以通过启用负载均衡并设置利用率的限值以及每个接入点允许的客户端关联数量，来纠正网络 AP 利用率的不平衡现象。

18.1.3 负载均衡和 QoS

负载均衡还扮演了另一个重要的角色，那就是确保 *IP 语音 (VoIP)* 及其他争用带宽且对时间敏感的应用程序的 *服务质量*，及时接入无线网络的无线电波。有关配置网络 QoS 的更多信息，请参阅第 19 章：“服务质量 (QoS)”。

18.2 导航至负载均衡设置

在管理 UI 上，导航至 *Manage*（管理）> *Load Balancing*（负载均衡）选项卡，并如下一节所述更新字段。

图 18.1 负载平衡设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Modify load balancing settings

Load Balancing

Enabled

Disabled

Utilization for No New Associations

0

(Percent, 0 disables)

Utilization for Disassociation

0

(Percent, 0 disables)

Station Threshold for Disassociation


0

Range 1 - 2007, 0 disables.

Update

18.3 配置负载平衡

要配置负载平衡，请启用**Load Balancing**（负载平衡）并设置接入点的指定利用率触发的限值和行为。



注释： 即使取消客户端与 AP 的关联，如果另一个接入点在范围内，则网络仍会向客户端站点提供持续的服务，以便客户端能够重新连接到网络。客户端应自动重试其最初连接的 AP 以及子网上的其他 AP。取消与 AP 关联的客户端可无缝过渡到同一子网上的另一个 AP。

负载平衡设置作为整体应用到 AP 负载。启用访客接入时，设置同时应用到内部和访客网络。

在双射频 AP 上，负载平衡设置应用到两个射频，但独立计算各个射频的负载，且负载包括内部网络和访客网络（启用访客接入时）的负载。

表 18.1 负载均衡设置

字段	描述
<i>Load Balancing</i> (负载均衡)	要在此接入点上启用负载均衡，单击 Enable （启用）。 要在此接入点上禁用负载均衡，单击 Disable （禁用）。
<i>Utilization for No New Associations</i> (无新关联的利用率)	利用率限值与无线带宽利用率相关。 提供此接入点的带宽利用率百分比限值，表明何时停止接受新的客户端关联。 当此接入点的利用率超过指定限值时，此接入点上不允许进行任何新的客户端关联。 如果您在此字段中指定 0 ，则允许所有新关联，无论利用率是多少。
<i>Utilization for Disassociation</i> (取消关联的利用率)	利用率限值与无线带宽利用率相关。 为此接入点提供带宽利用率百分比限值，表明何时取消与当前客户端的关联。 利用率超过指定限值时，当前与此接入点关联的客户端将会断开连接。 如果您在此字段中指定 0 ，则绝不会断开与当前客户端的连接，无论利用率是多少。
<i>Stations Threshold for Disassociation</i> (取消关联的站点阈值)	指定您希望用作取消关联的“站点阈值”的客户端工作站数量。在任何时间，如果与 AP 关联的客户端站点的数量等于或小于您在此指定的数量，则不会取消与任何站点的关联，无论取消关联的站点阈值是多少。 从理论上来说，允许的客户端站点的最大数量为 2007 。  我们建议将最大值设为 30 到 50 个客户端工作站。考虑到在 AP 客户端之间共享带宽，这样就确保了接入点上的负载是有效的。

18.4 更新设置

要风险负载均衡设置：

- 1. 导航至 *Load Balancing*（负载均衡）选项卡页面。
- 2. 根据需要配置负载均衡设置。
- 3. 单击 **Update**（更新）按钮应用更改。

19.1 了解 QoS	185
19.1.1 QoS 和负载均衡	185
19.1.2 802.11e 和 WMM 标准支持	185
19.1.3 QoS 队列和协调流量的参数	186
19.1.3.1 QoS 队列和数据包上的服务类型 (ToS)	186
19.1.3.2 数据帧的 EDCF 控制和仲裁帧间间隔	187
19.1.3.3 随机退避和最小/最大竞争窗口	188
19.1.3.4 更佳性能的数据包突发	189
19.1.3.5 客户端工作站的传输机会 (TXOP) 间隔	189
19.1.4 802.1p 和 DSCP 标记	189
19.1.4.1 VLAN 优先级	191
19.1.4.2 DSCP 优先级	192
19.2 配置 QoS 队列	192
19.2.1 配置 AP EDCA 参数	194
19.2.2 启用/禁用 Wi-Fi 多媒体	196
19.2.3 配置工作站 EDCA 参数	196
19.3 更新设置	197

服务质量 (**QoS**) 可为您提供指定多个队列上的参数的能力, 从而增加吞吐量并提高差异化无线流量 (例如 *IP 语音* (VoIP)、其他类型的音频、视频和流媒体以及通过产品名称传输的传统 IP 数据) 的性能。

以下各节阐述了如何在产品名称上配置服务质量队列。

19.1 了解 QoS

影响 QoS 的首要因素是网络拥塞, 而这是由于试图访问无线电波的客户段数量不断增加以及在一天中的繁忙时段争用带宽的流量越来越多而造成的。繁忙、超载的网络中, 最明显的性能降级表现在时间敏感的应用程序中, 例如视频、*IP 语音* (VoIP) 和流媒体。

典型的数据文件受 QoS 变化影响较小, 而与此不同的是, 视频、VoIP 和流媒体必须按照指定的顺序, 以一致的速率进行传输, 且**数据包**传输之间的延迟最小。如果服务质量受到影响, 音频或视频将会发生扭曲。

19.1.1 QoS 和负载平衡

组合使用负载平衡 (请参阅第 18 章: “负载平衡”) 和 QoS 技术, 您可在繁忙网络上为时间敏感应用程序提供高质量的服务。负载平衡是在接入点之间更好地分配流量的一种方式。QoS 根据单个接入点不同类型的无线流量的传输优先级, 对带宽和网络访问进行分配。

19.1.2 802.11e 和 WMM 标准支持

QoS 描述了用于控制共享网络连接的数据流的一系列技术。**IEEE 802.11e** 任务组正在定义针对无线网络上的传输质量和服务可用性的 QoS 标准。QoS 旨在通过最大程度减少网络拥塞, 限制**抖动**、**延迟**和**包丢失**, 支持时间敏感或任务关键型应用程序的专用带宽以及优先分配用于信道访问的无线流量, 来提供更好的网络服务。

采用所有 **IEEE 802.11** 工作组标准, 目标是提供实施 QoS 功能的标准方法, 使得来自不同公司的组件能够共同操作。

产品名称提供的 QoS 基于**无线多媒体 (WMM)** 规格和**无线多媒体 (WMM)** 标准, 而这些标准是 **802.11e** 功能子集的实施。

接入点和无线客户端 (便携式计算机、消费类电子产品) 均支持 WMM。

19.1.3 QoS 队列和协调流量的参数

要在产品名称上配置 QoS 选项，需要设置用于不同类型的无线流量的现有队列的参数。您可根据正在发送的媒体的要求对每个队列中的数据包的传输的不同最短和最等待时间进行配置。队列会自动提供音频、视频、多媒体和任务关键型应用的最小传输延迟，并信赖为传统 IP 数据尽力配置的参数。

例如，有效地向时间敏感型音频、视频和多媒体提供更高的传输优先级（信道访问的等待时间更短），而其他应用程序和传统 IP 数据对时间较不敏感，但通常需要更密集的数据以容忍较长的等待时间。

产品名称根据 IEEE 无线多媒体 (WMM) 标准实施 QoS。基于 Linux 的队列类别用于标记数据包并建立多个队列。所提供的队列根据传输的数据类型提供内置的优先级和路由。

管理 UI 可为您提供一种配置队列上的参数的方式。

19.1.3.1 QoS 队列和数据包上的服务类型 (ToS)

产品名称上的 QoS 利用 *WMM* 与服务类型 (*IP*) 相关的数据包标头中的 *ToS* 信息。通过网络发送的每个 IP 数据包在标头中显示 ToS 字段，指示优先分配并通过网络传输数据的方式。ToS 字段由 3 至 7 位值组成，每位代表该数据以及其他元信息的不同方面或优先程度（低延迟、高吞吐量、高可靠性、低成本等等）。

例如，FTP 数据包的 ToS 很可能为实现最大吞吐量而设置，这是因为 FTP 的关键考虑因素在于一次传输相对大量的数据的能力。在这种情况下，最好具交互反馈，但这一点并不是最重要的。VoIP 数据包为实现最小延迟而设置，因为这是该类型数据的质量和性能的重要因素。

接入点检查通过 AP 的所有数据包的标头中的 ToS 字段。根据数据包 ToS 字段中的值，AP 将要传输的数据包分配至其中一个队列，来实现其优先级。此过程自动进行，无论是否专门配置了 QoS。

不同类型的数据域每个队列相关联。队列、相关优先级和传输参数如下所示：

- 数据 0（音频）。最高优先级的队列，最小延迟。时间敏感型数据，如 IP 语音 (VoIP) 会自动发送至该队列。
- 数据 1（视频）。高优先级的队列，最小延迟。时间敏感型数据，例如视频和其他流媒体，会自动发送至该队列。
- 数据 2（尽力配置）中等优先级的队列，中等吞吐量和延迟。大多数传统的 IP 数据会发送至该队列。
- 数据 3（后台）。最低优先级的队列，高吞吐量 需要最大吞吐量且并非为时间敏感型的批量数据会发送至该队列（例如 FTP 数据）。

优先级较高的队列中的数据包将会先于优先级较低的队列中的数据包传输。首先发送队列中标记为“数据 0”和“数据 1”的交互式数据，然后发送“数据 2”中的尽力配置数据，最后发送“数据 3”中的后台（批量）数据。每一个优先级较低的队列（流量等级）会获得较高等级流量发送后剩余的带宽。极端情况下，如果您具有足够的交互式数据，能够始终保持接入点繁忙，则绝不会发送优先级较低的流量。

使用管理 UI 上的 QoS 设置，您可配置 *增强型分布式信道访问 (EDCA)* 参数，该参数可确定当该队列通过接入点发送至客户端或通过客户端发送至接入点时，如何处理每个队列。



注释：无线流量：

- 从接入点向下游传输至客户端工作站。
- 从客户端工作站向上游传输至接入点。
- 从接入点向上游传输至网络。
- 从网络向下游传输至接入点。

启用 WMM 后，9160 G2 无线网关上的 QoS 设置会影响前两项，从接入点向下游传输至客户端工作站（AP EDCA 参数）的流量和从工作站向上游传输至接入点工作站 EDCA 参数）的流量。

禁用 WMM 后，您仍可对从 AP 向下游传输至客户端工作站的流量进行参数的设置（AP EDCA 参数）。

流量（传输至网络或从网络传输）的其他阶段不受 AP 上 QoS 设置的控制。

19.1.3.2 数据帧的 EDCF 控制和仲裁帧间间隔

数据通过帧中的 802.11 无线网络进行传输。**帧**由离散部分的数据以及一些为在无线网络上传输而打包的描述性元信息组成。



注释：帧与数据包的概念类似，不同之处在于数据包在网络层（OSI 模型中的第 3 层）运行，而帧在数据链路层（OSI 模型中的第 2 层）运行。

每个帧包括一个来源 MAC 地址和目标 MAC 地址、显示协议版本的控制字段、帧类别、帧序号、帧主体（和要传输的实际信息）以及用于检测错误的帧检验序列。

802.11 标准规定了用于无线基础设施的管理和控制以及数据传输的各种帧类型。

802.11 帧类型为：(1) 管理帧、(2) 控制帧和(3) 数据帧。管理帧和控制帧（用于管理和控制无线基础设施的可用性）自动具有较高的传输优先级。

802.11e 使用 *帧间间隔*规定哪些帧能够访问可用的信道，并协调不同类别的数据的传输等待时间。

管理帧和控制帧等待传输的时间最短，它们等待一个 **短帧间隔 (SIF)**。这些等待时间内置于 802.11 中作为基础设施支持，且不可配置。

产品名称支持 **802.11e** 标准定义的 **增强型分布式协调功能 (EDCF)**。EDCF 是 **DCF** 标准的增强功能，以 **CSMA/CA** 协议为基础，定义了 **数据帧** 之间的帧间间隔 (IFS)。传输前，数据帧等待 **仲裁帧间间隔 (AIFS)** 所规定的时间。

此参数可配置。



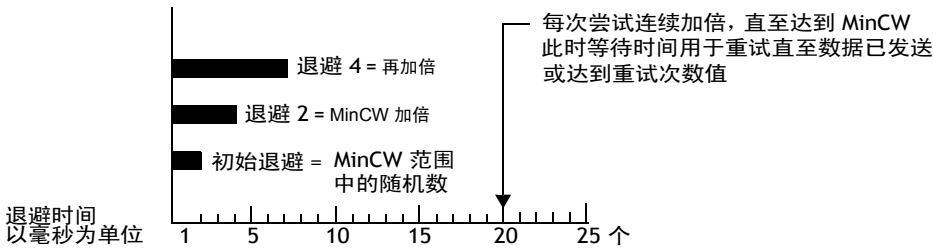
注释：在 **AIFS** 中发送数据帧，可允许首先在 **SIF** 中发送具有较高优先级的管理帧和控制帧。

AIF 可确保多个接入点不会尝试同时发送数据，而是等待，直到有一条信道空闲。

19.1.3.3 随机退避和最小/最大竞争窗口

如果一个接入点检测到媒体使用中（繁忙），会使用 **DCF 随机退避** 定时器确定尝试再次访问一个指定信道之前需要等待的时间。每个接入点在再次尝试之前需要等待一段随机的时间。等待时间（最初为 **最小竞争窗口** 指定的范围内的随机值）会以指数方式增加，达到指定限制（**最大竞争窗口**）。如果多个 **AP** 同时访问媒体并尝试同时传输数据，随机延迟可避免大多数可能发生的冲突。您在网络上的活跃用户越多，退避计时器在减少冲突和重新传输次数中的性能提升就越重要。

图 19.1 DCF 随机退避计时器



接入点使用的随机退避为可配置参数。要描述随机延迟，应定义“最小竞争窗口” (MinCW) 和“最大竞争窗口” (MaxCW)。

- 为 **最小竞争窗口** 指定的值是初始随机退避等待时间的上限。随机退避中使用的数字最初为介于 0 和最小竞争窗口规定的数字之间的随机数字。
- 如果首个随机退避时间在数据帧成功传输之前结束，接入点会增加重试计数器，并加倍随机退避窗口的值。**最大竞争窗口** 中指定的值是随机退避加倍的上限。该加倍会继续进行，直至数据帧已发送，或达到最大竞争窗口大小。

19.1.3.4 更佳性能的数据包突发

产品名称包括基于数据包突发技术的 802.11e, 该技术可增加数据吞吐量并提高通过无线网络进行的传输速度。数据包突发可实现多个数据包的传输, 而无需额外的标头信息开销。这样做的结果是提高了网络速度和数据吞吐量。允许的数据包突发的尺寸 (最大突发长度) 是一个可配置参数。

19.1.3.5 客户端工作站的传输机会 (TXOP) 间隔

传输机会 (TXOP) 是当 Wi-Fi 多媒体 (WMM) 客户端工作站有权在无线媒体 (WM) 上启动传输时的时间间隔。

19.1.4 802.1p 和 DSCP 标记

IEEE 802.1p 是 IEEE 802 标准的扩展, 负责 QoS 的配置。802.1p 的主要用途是优先分配数据链路/MAC 层的网络流量。802.1p 具有过滤多播流量的功能, 确保它不会在第 2 层交换网络增加。它使用标签帧实施优先分配计划。要符合此标准, 第 2 层交换机必须能够将传入的 LAN 数据包分组为不同的流量级别。

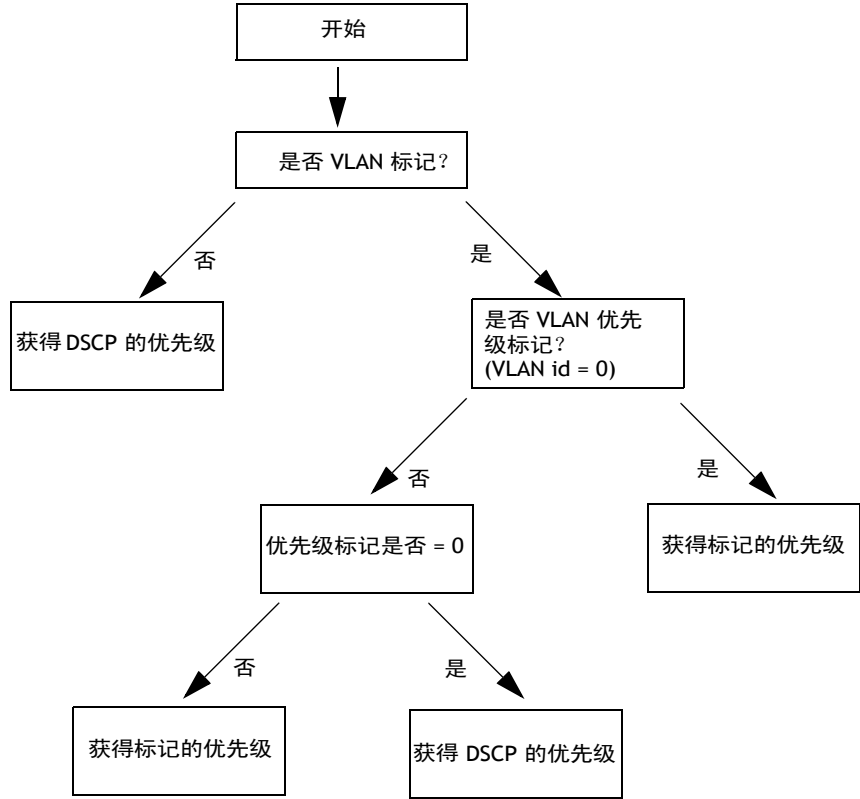
802.1p 标头包括一个用于优先级分配的三位字段, 允许将数据包分组为各种流量类型。规定八个优先级。最高的优先级为七, 即网络关键流量 (音频)。通常会首先传输具有较高优先级的数据包。如果优先级较高的数据包仍在传输中, 则不会传输优先级较低的数据包, 这些数据包将进入队列, 直到优先级较高的数据包成功传输。最低优先级为零, 这是尽力配置的默认值, 当未设置其他值时会自动调用。



注释: 请注意, 除非启用 QoS 和 WMM, 否则 802.1p 将不工作。WMM 必须在 AP 和连接至 AP 的客户端上启用。

图 19.2 中的流程图概述了检索标记和分配网络上的流量的方式。

图 19.2 网络流量的优先级



19.1.4.1 VLAN 优先级

表 19.1 列出了从 VLAN 标记中获得的优先级标记及其关联值。

表 19.1 VLAN 标记优先级

VLAN ID 标记	优先级
0 - 默认 DHCP 值	尽力配置
1	后台
2	后台
3	尽力配置
4	视频
5	视频
6	语音
7	语音

19.1.4.2 DSCP 优先级

表 19.2 列出了 DSCP 值、关联 ID 和优先级。

表 19.2 DSCP 标记优先级

ID 标签	优先级	DSCP 价值
0 - 默认 DHCP 值	尽力配置	0
1	后台	16
2	后台	8
3	尽力配置	24
4	视频	32
5	视频	40
6	语音	48
7	语音	56

19.2 配置 QoS 队列

要设置 QoS 的队列，导航至*Services*（服务）> *QoS*（服务质量）选项卡，并按如下所述配置设置。

图 19.3 服务质量 (QoS) 设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Modify QoS queue parameters

Queue

AIFS

cwMin

cwMax

Max. Burst

Data 0 (Voice)

1

3

7

1.5

Data 1 (Video)

1

7

15

3.0

Data 2 (Best Effort)

3

15

63

0

Data 3 (Background)

7

15

1023

0

AP EDCA parameters

Wi-Fi Multimedia (WMM)
☒ Enabled ☐ Disabled

Queue

AIFS

cwMin

cwMax

TXOP Limit

Data 0 (Voice)

2

3

7

47

Data 1 (Video)

2

7

15

94

Data 2 (Best Effort)

3

15

1023

0

Data 3 (Background)

7

15

1023

0

Station EDCA parameters

Update

要在 **QoS** 上配置服务质量 (产品名称)，需要设置用于不同类型的无线流量的现有队列的参数，并有效指定传输的最短和最长等待时间（通过 **竞争窗口**）。这里所述的设置仅适于接入点上的数据传输行为，不适于客户端工作站上的数据传输行为。



注释：对于访客接口，**QoS** 队列设置适于作为整体的接入点负载（同时使用两个 **BSS**）。

在双射频接入点上，这些设置适用于两个射频，但每个射频的流量单独列入队列。（例外情况是如下所述的访客流量。）

内部和访客网络流量在每个射频中通常一起列入队列。在单射频和双射频 **AP** 上都是如此。

接入点上的 QoS 利用与服务类型 (*ToS*) 相关的 IP 数据包标头中的现有信息。接入点检查通过 AP 的所有数据包的标头中的 ToS 字段。根据数据包 ToS 字段中的值，AP 将要传输的数据包分配至其中一个列，来实现其优先级。不同类型的数据域每个队列相关联。当通过接入点发送队列时，可配置如何处理每个队列的参数。

服务质量的配置包括：

- 第 194 页的“配置 AP EDCA 参数”。
- 第 196 页的“启用/禁用 Wi-Fi 多媒体”。
- 第 197 页的“更新设置”。

19.2.1 配置 AP EDCA 参数

AP 增强型分布式信道访问 (*EDCA*) 参数可影响从接入点传输至客户端工作站的流量。

表 19.3 AP EDCA 参数

字段	描述
<i>Queue</i> (队列)	<p>定义了从 AP 传输至工作站的不同类型数据的队列：</p> <p>数据 0（音频）</p> <p>高优先级的队列，最小延迟。时间敏感型数据，如 VoIP 和流媒体，会自动发送至该队列。</p> <p>数据 1（视频）</p> <p>高优先级的队列，最小延迟。时间敏感型视频数据会自动发送至该队列。</p> <p>数据 2（尽力配置）</p> <p>中等优先级的队列，中等吞吐量和延迟。大多数传统的 IP 数据会发送至该队列。</p> <p>数据 3（后台）</p> <p>最低优先级的队列，高吞吐量 需要最大吞吐量且并非为时间敏感型的批量数据会发送至该队列（例如 FTP 数据）。</p> <p>有关详细信息，请参阅第 186 页的“QoS 队列和协调流量的参数”。</p>

表 19.3 AP EDCA 参数 （续）

字段	描述
<i>AIFS</i> (帧间间隔)	<p>仲裁帧间间隔(AIFS) 指定了 数据帧的等待时间 （以毫秒为单位）。</p> <p>AIFS 的有效值为 1 至 255。</p> <p>有关详细信息，请参阅数据帧的 DCF 控制和帧间间隔。</p> <p>有关详细信息，请参阅第 187 页的 “数据帧的 EDCF 控制和仲裁帧间间隔”。</p>
<i>cwMin</i> (最小竞争窗口)	<p>将该参数输入确定用于传输重新尝试的初始随机退避等待时间 （“窗口”）的算法中。</p> <p>在最小竞争窗口中指定的值是确定初始随机退避等待时间范围的上限 （以毫秒为单位）。</p> <p>所产生的首个随机数字将介于 0 和此处指定的数字之间。</p> <p>如果首个随机退避等待时间在发送数据帧之前到期，重试计数器将递增，且随机退避值 （窗口）加倍。在随机退避值的大小达到最大竞争窗口中定义数字之前，该加倍会继续。</p> <p>“cwmin” 的有效值为 1、3、7、15、31、63、127、255、511 或 1023。</p> <p>有关详细信息，请参阅第 188 页的 “随机退避和最小/最大竞争窗口”。</p>
<i>CWmax</i> (最大竞争窗口)	<p>在最大竞争窗口中指定的值是随机退避值加倍的上限 （以毫秒为单位）。该加倍会继续进行，直至数据帧已发送，或达到最大竞争窗口大小。</p> <p>达到最大竞争窗口大小后将继续重试，直至达到允许的最大重试次数。</p> <p>“cwmin” 的有效值为 1、3、7、15、31、63、127、255、511 或 1023。</p> <p>有关详细信息，请参阅第 188 页的 “随机退避和最小/最大竞争窗口”。</p>
最大 突发长度	<p>仅为 AP EDCA 参数 （最大 突发长度仅适于从接入点传输至客户端工作站的流量。）</p> <p>该值规定了无线网络上数据包突发允许的最大突发长度 （以毫秒为单位）。数据包突发是在无标头信息的情况下所传输的多个帧的集合。开销减少后，能够提高吞吐量并实现更佳的性能。</p> <p>最大突发长度的有效值为 0.0 至 999.9。</p> <p>有关详细信息，请参阅第 189 页的 “更佳性能的数据包突发”。</p>

19.2.2 启用/禁用 Wi-Fi 多媒体

默认情况下，Wi-Fi 多媒体 (WMM) 在接入点上启用。启用 WMM 后，QoS 优先级和无线媒体访问的协调为开启状态。启用 WMM 后，产品名称上的 QoS 设置会控制从接入点向下游传输至客户端工作站（AP EDCA 参数）的流量和从工作站向上游传输至接入点（工作站 EDCA 参数）的流量。

禁用 WMM 将禁用对从工作站向上游传输至接入点的流量上工作站 EDCA 参数的 QoS 控制。在 WMM 禁用的情况下，您仍然可以对从接入点上下游传输至客户端工作站（AP EDCA 参数）进行参数设置。

- 要禁用 WMM 扩展，请单击 **Disabled**（禁用）。
- 要启用 WMM 扩展，请单击 **Enabled**（启用）。

19.2.3 配置工作站 EDCA 参数

工作站增强型分布式信道访问 (EDCA) 参数会影响从客户端工作站传输至接入点的流量。

表 19.4 工作站 EDCA 参数

字段	描述
<i>Queue</i> （队列）	<p>定义了从工作站传输至 AP 的不同类型数据的队列：</p> <p>数据 0（音频）</p> <p>最高优先级的队列，最小延迟。时间敏感型数据，如 VoIP 和流媒体，会自动发送至该队列。</p> <p>数据 1（视频）</p> <p>最高优先级的队列，最小延迟。时间敏感型视频数据会自动发送至该队列。</p> <p>数据 2（尽力配置）</p> <p>中等优先级的队列，中等吞吐量和延迟。大多数传统的 IP 数据会发送至该队列。</p> <p>数据 3（后台）</p> <p>最低优先级的队列，高吞吐量 需要最大吞吐量且并非为时间敏感型的批量数据会发送至该队列（例如 FTP 数据）。</p> <p>有关详细信息，请参阅第 186 页的“QoS 队列和协调流量的参数”。</p>

表 19.4 工作站 EDCA 参数 （续）

字段	描述
<i>AIFS</i> (帧间间隔)	<p>仲裁帧间间隔 (AIFS) 指定了数据帧的等待时间（以毫秒为单位）。</p> <p>有关详细信息，请参阅数据帧的 DCF 控制和帧间间隔。</p> <p>有关详细信息，请参阅第 187 页的“数据帧的 EDCF 控制和仲裁帧间间隔”。</p>
<i>cwMin</i> (最小竞争窗口)	<p>将该参数输入确定用于传输重新尝试的初始随机退避等待时间（“窗口”）的算法中。</p> <p>在最小竞争窗口中指定的值是确定初始随机退避等待时间范围的上限（以毫秒为单位）。</p> <p>所产生的首个随机数字将介于 0 和此处指定的数字之间。</p> <p>如果首个随机退避等待时间在发送数据帧之前到期，重试计数器将递增，且随机退避值（窗口）加倍。在随机退避值的大小达到最大竞争窗口中定义数字之前，该加倍会继续。</p> <p>有关详细信息，请参阅第 188 页的“随机退避和最小最大竞争窗口”。</p>
<i>CWmax</i> (最大竞争窗口)	<p>在最大竞争窗口中指定的值是随机退避值加倍的上限（以毫秒为单位）。该加倍会继续进行，直至数据帧已发送，或达到最大竞争窗口大小。</p> <p>达到最大竞争窗口大小后将继续重试，直至达到允许的最大重试次数。</p> <p>有关详细信息，请参阅第 188 页的“随机退避和最小最大竞争窗口”。</p>
<i>TXOP 限制</i>	<p>仅工作站 EDCA 参数（TXOP 限制仅适于从客户端工作站传输至接入点的流量。）</p> <p>传输机会 (TXOP) 是当 WME 客户端工作站有权在无线媒体 (WM) 上启动传输时的时间间隔。</p> <p>该值定义了客户端工作站的传输机会 (TXOP)，也就是，当 WMM 客户端工作站有权在无线媒体上启动传输时的时间间隔。</p>

19.3 更新设置

要更新 QoS 设置：

- 1. 导航至 *Qos* 选项卡页面。
- 2. 根据需要配置 Qos 设置。
- 3. 单击 **Update**（更新）按钮应用更改。

20.1 了解无线分布系统	201
20.1.1 使用 WDS 桥接远距离有线 LAN.	201
20.1.2 使用 WDS 将网络扩展到有线覆盖区域之外	202
20.1.3 使用 WDS 创建备份链路	202
20.2 与 WDS 链路相关的安全考虑事项.	203
20.2.1 了解静态 WEP 数据加密	203
20.2.2 了解 WPA (PSK) 数据加密	203
20.3 配置 WDS 设置	204
20.3.1 配置 WDS 链路的示例	206
20.4 更新设置	207

产品名称允许您使用无线分布系统 (**WDS**) 连接多个接入点。WDS 允许接入点以无线方式进行彼此之间的通信。在提供无缝的客户端漫游体验和管理多个无线网络方面，此功能至关重要。它还通过减少所需的布线数量，简化网络基础设施。

以下小节介绍如何在产品名称上配置 WDS。

20.1 了解无线分布系统

无线分布系统 (**WDS**) 技术能够以无线方式连接称为基本服务集 (**BSS**) 的接入点，以形成所谓的扩展服务集 (**ESS**)。

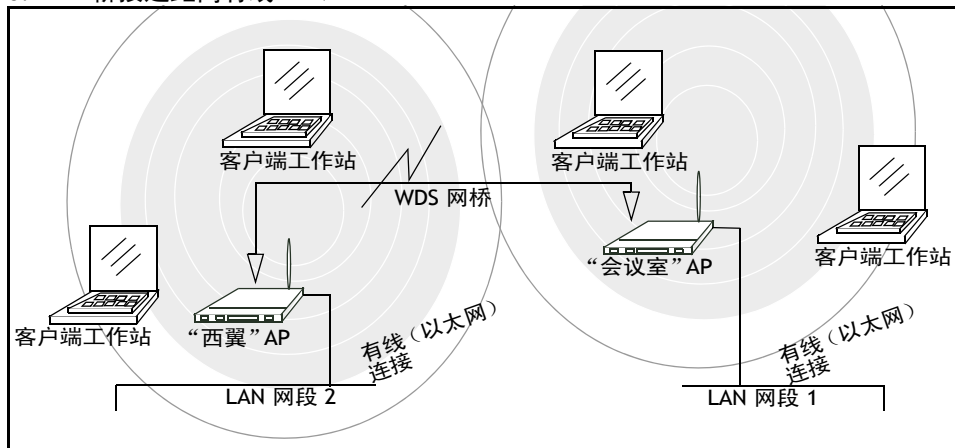


注释：通常情况下，一个 BSS 相当于一个接入点（部署为由单个 AP 组成的无线“网络”），但多 BSSID 功能使单个接入点看起来像网络的两个或多个接入点的情况除外。在这种情况下，接入点有多个唯一的 BSSID。

20.1.1 使用 WDS 桥接远距离有线 LAN

在由多个接入点组成的网络 **ESS** 中，每个接入点只为单个接入点无法覆盖的较大区域的一部分提供服务。您可以使用 WDS 桥接远距离以太网以创建单个 **LAN**。例如，假设您有一个接入点通过以太网连接到网络并服务于会议室（LAN 网段 1）中的多个客户端工作站，另一个以太网有线接入点服务于西翼办公（LAN 网段 2）中的工作站。您可以通过 WDS 链路桥接会议室和西翼接入点，为这两个区域中的客户端创建单个网络（参阅第 201 页的图 20.1）。

图 20.1 桥接远距离有线 LAN

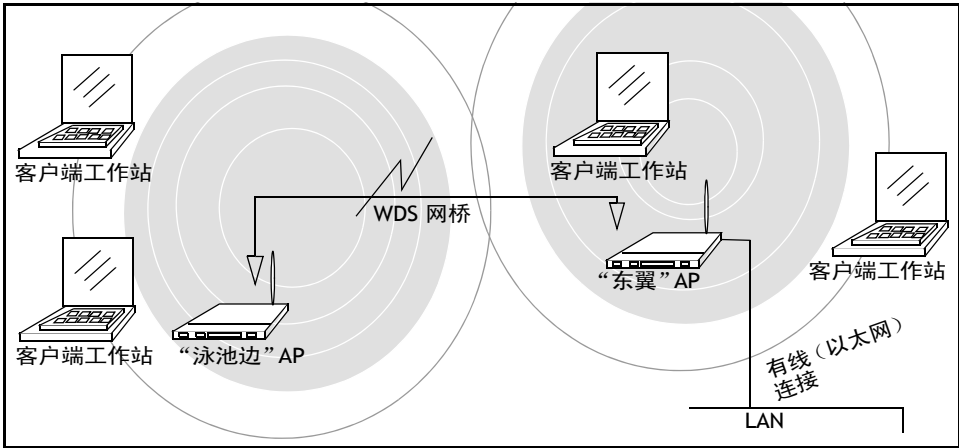


20.1.2 使用 WDS 将网络扩展到有线覆盖区域之外

ESS 可以将网络的覆盖范围扩展到布线难度过大、成本过高或低效的区域。

例如，假设您有一个接入点通过以太网连接到网络并服务于一个区域（以“东翼”为例）中的多个客户端工作站，但无法覆盖范围之外的其他区域。假设通过以太网电缆连线远距离区域的难度过大或者成本过高。要解决此问题，您可以将第二个接入点放置在靠近第二组工作站（在第 202 页的图 20.1.3 中以“泳池边”为例）的位置，并使用一个 WDS 链路桥接两个 AP。这样，便可通过提供一个额外的跃点，以无线方式扩展您的网络，以到达远距离工作站（参见第 202 页的图 20.1.3）。

图 20.2 将网络扩展到有线覆盖区域之外



20.1.3 使用 WDS 创建备份链路

WDS 桥接的另一个用途是创建备份链路。在产品名称上自动启用生成树协议 (STP) 后，WDS 可用于配置网络上的接入点之间的备份路径。例如，在两个接入点之间有两个路径，分别是通过以太网的主路径，和通过 WDS 链路的次级（备份）无线路径。如果以太网连接出现故障，STP 会重新配置其网络映射，并通过启用备份无线路径有效修复出现故障的网络段。

20.2 与 WDS 链路相关的安全考虑事项

在 WDS 链路上设置某种类型的安全性，这一点非常重要。您可以在 WDS 链路上设置任何类型的安全性，这与链路上的 AP 所应用的安全设置无关。例如您可以将 AP1 上的安全性设为 **None**（无），将 AP2 上的安全性设为 **WEP**。即使这两项设置是不同的，您可以选择将 WDS 链路上的安全性设为 **None**（无）或 **WEP**。此规则的唯一例外就是在使用 **WPA (PSK)** 时。如果您将 AP1 和 AP2 的安全性设为 **WPA Personal**（WPA 个人）或 **WPA Enterprise**（WPA 企业），则仅可在 WDS 链路上设置 **WPA (PSK)** 安全设置。

20.2.1 了解静态 WEP 数据加密

静态 *有线等效加密 (WEP)* 是适用于 802.11 无线网络的数据加密协议。必须为指定 WDS 链路中的两个接入点配置相同的安全设置。对于静态 **WEP**，为数据加密指定一个静态 64 位 40 位密钥 + 24 位初始化向量 (IV) 或 128 位（104 位密钥 + 24 位 IV）共享密钥。

您可以在 WDS 链路（网桥）上启用静态 **WEP**。启用 **WEP** 后，使用您提供的固定 **WEP** 密钥，对在 WDS 链路中的两个接入点之间通信的所有数据进行加密。

静态 **WEP** 不能为客户端工作站提供其他可用于服务的安全模式所能达到有效数据保护级别。如果您在用于安全无线通信的 **LAN** 上使用静态 **WEP**，就是将您的网络暴露在危险之中。因此，我们建议在内部网络上的任何 WDS 链路上使用 **WPA (PSK)** 加密。请勿使用基于静态 **WEP** 的 WDS 桥接内部网络上的接入点，除非您并不关心该网络上数据通信的安全风险。有关 **WPA (PSK)** 的更多信息，请参阅下文中的“了解 **WPA (PSK)** 数据加密”。

有关不同安全模式的有效性的更多信息，请参阅第 10 章：“配置安全性”。此主题还涵盖将未加密安全模式用于访客网络上 AP 与工作站之间的通信，而访客网络是用于敏感性较低的数据通信。

20.2.2 了解 WPA (PSK) 数据加密

Wi-Fi 受保护访问（预共享密钥）或 **WPA (PSK)** 是比静态 **WEP** 更强大的安全形式。**WPA (PSK)** 之前被称为“**WPA-Home**”，它工作时所使用的预共享密钥实际上是桥接链路上两个 AP 之间的共享密码。**WPA (PSK)** 提供增强的 802.11 无线安全性，无需实施起来复杂且昂贵的 **RADIUS** 身份验证基础设施。

由于 **WPA (PSK)** 加密依赖于共享密钥，因此必须使用相同的密钥设置 WDS 链路上的两个 AP，否则这两个 AP 将无法通信和共享信息。



注释：出于安全原因，建议您定期更改 WDS 网桥上的共享密钥。

有关不同安全模式的有效性的更多信息，请参阅第 10 章：“配置安全性”。

20.3 配置 WDS 设置

要指定从此接入点到其他接入点之间的流量交换详情，请导航至 *Manage*（管理）> *WDS* 选项卡，并更新如下所述的字段。

 注释：图 20.3 显示了双射频 AP 的 WDS 设置页面。单射频 AP 的管理 Web 页面外观略有不同。

图 20.3 无线分布系统设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Configure WDS bridges to other access points

Local Address00:08:A2:01:4B:56

Remote Address

EncryptionNone (Plain-text)

Remote Address

EncryptionNone (Plain-text)

Remote Address


EncryptionNone (Plain-text)

Remote Address

EncryptionNone (Plain-text)

Update

以下注释总结了有关 **WDS** 配置的一些重要指导准则。请先阅读所有注释，然后再继续进行 WDS 配置。

 注释：使用 WDS 时，确保在参与 WDS 链路的两个接入点上配置 WDS 设置。任何一对接入点之间只能有一个 WDS 链路。也就是说，在特定接入点的 WDS 页面上，远程 MAC 地址仅显示一次。

参与 WDS 链路的两个接入点必须处在同一个无线电信道上，并使用相同的 IEEE 802.11 模式。（参阅第 16 章：“配置 802.11 射频设置”了解有关配置无线通信模式和信道的信息。）

802.11h 工作时，设置 WDS 链路可能有点儿困难。请参阅第 146 页的“802.11h 监管域控制”。

要在此接入点上配置 WDS，请描述用于接收发包的各个 AP，并将信息发送至此 AP。各个目的地 AP 需要以下描述，如表 20.1 中所示。

表 20.1 目的地接入点设置

字段	描述
<i>Local Address</i> (本地地址)	<p>表示此接入点的媒体访问控制 (MAC) 地址。</p> <p>MAC 地址是代表网络接口的任何设备的永久性、唯一的硬件地址。MAC 地址由制造商分配。您无法更改 MAC 地址。此处仅为信息目的而提供，作为接入点或接口的唯一标识符。</p> <p>单射频 AP:</p> <p>在单射频接入点上，单个 MAC 地址显示在 WDS 设置页面的顶部。单射频 AP 显示的地址是该 AP 的 MAC 地址。通过此地址，其他网络便可在外部知道该接入点。</p> <p>双射频 AP:</p> <p>对于双射频 AP 上的 WDS 链路，<i>Local Address</i>（本地地址）反映了所选射频（WLAN0 上的射频 1 或 WLAN1 上的射频 2）的内部接口的 MAC 地址。</p>
<i>Remote Address</i> (远程地址)	<p>指定目的地接入点的 MAC 地址；即数据发送或“转发”到的接入点或从中接收数据的接入点，换句话说，就是您创建 WDS 网桥时所桥接的 AP。</p> <p>单击 <i>Remote Address</i>（远程地址）字段右侧的箭头后，您会看到所有可用 MAC 地址及其在网络上的相关 SSID 的列表。从列表中选择相应的 MAC 地址。</p> <p>注： 下拉列表中显示的 SSID 能够帮助您识别目的地接入点的正确 MAC 地址。此 SSID 是您为 WDS 链路设置的单独 SSID。这两个不是相同的值或名称，而且也不该相同。</p>

表 20.1 目的地接入点设置 （续）

字段	描述
Encryption (加密)	<p>如果您并不关心 WDS 链路上的安全问题，您可能决定不设置任何加密类型。此外，如果您有安全方面的担忧，可以在 “静态 WEP” 和 “WPA (PSK)” 之间进行选择。</p> <p>注： 此处可用的加密类型选项取决于您在 Security （安全）选项卡页面上指定的设置。只有当您在 Security （安全）选项卡页面上将 Mode （模式）设置为 WPA Personal （WPA 个人）或 WPA Enterprise （WPA 企业）， WPA (PSK) 选项才在 WDS 页面上显示。</p> <p>None (Plain Text) （无 （纯文本））：</p> <p>如果您将加密设置为 None （无），则在 WDS 网桥上的 AP 之间发送的数据将不会加密，而是作为纯文本发送。</p> <p>WEP:</p> <p>指定您是否想要为 WDS 链路启用有线等效加密 (WEP)。有线等效加密 (WEP) 是适用于 802.11 无线网络的数据加密协议。必须为 WDS 链路中的两个接入点配置相同的安全设置。对于静态 WEP，为数据加密指定一个静态 64 位 （40 位密钥 + 24 位初始化向量 (IV)）或 128 位 （104 位密钥 + 24 位 IV）共享密。有关 WEP 安全性的更多信息，请参阅第 101 页的 “Static WEP （静态 WEP）”。</p> <p>WPA (PSK):</p> <p>指定您是否想要为 WDS 链路启用 WPA (PSK) 加密。Wi-Fi 受保护访问预共享密钥 WPA (PSK) 是比 WEP 更安全的安全形式。使用 WPA (PSK) 加密时，必须为网络上的各个 AP 设置相同的唯一密钥，否则 AP 将无法彼此通信。</p> <p>只有当您在 Security （安全）选项卡页面上将 Mode （模式）设置为 WPA Personal （WPA 个人）或 WPA Enterprise （WPA 企业）时， WPA (PSK) 选项才在 WDS 页面上显示。有关安全性的更多信息，请参阅第 91 页的 “了解无线网络的安全问题”。</p> <p>有关 WPA (PSK) 安全性的更多信息，请参阅第 109 页的 “WPA Personal （WPA 个人版）”。</p>

20.3.1 配置 WDS 链路的示例

使用 WDS 时，确保在 WDS 链路的*两个*接入点上配置 *WDS* 设置。例如，要在一对接入点 “**MyAP1**” 和 “**MyAP2**” 之间创建 WDS 链路，请执行以下操作：

1. 以下列形式在 Web 浏览器地址栏中输入 MyAP1 的 IP 地址作为 URL，以打开 MyAP1 的管理 Web 页面：
<http://IPAddressOfAccessPoint>
其中， *IPAddressOfAccessPoint* 是 MyAP1 的地址。

2. 导航至 MyAP1 管理 Web 页面上的 WDS 选项卡。

MyAP1（您当前正在查看的接入点）的 MAC 地址将在页面顶部显示为“Local Address”（本地地址）。

3. 配置与 MyAP2 进行数据交换的 WDS 接口

首先输入 MyAP2 的 MAC 地址作为“Remote Address”（远程地址），并填充剩余字段以指定网络（访客或内部）、安全等。保存设置（单击 **Update**（更新））。

4. 导航至管理 Web 页面上的射频设置（*Manage（管理） > 802.11 Advanced Settings（802.11 高级设置）*），验证或设置您想要广播 MyAP1 的模式及无线电信道。

请记住，必须将参与链路的两个接入点 MyAP1 和 MyAP2 设置为相同的模式，并在同一信道上进行传输。

在本示例中，我们使用 IEEE 802.11b 模式并在信道 6 上进行广播。（从“Radio”（射频）选项卡上的下拉菜单中选择模式和信道。）

5. 现在，对 MyAP2 重复相同的步骤：
 - 在 URL 中使用 MyAP2 的 IP 地址，打开 MyAP2 的管理 Web 页面。
 - 导航至 MyAP2 管理 Web 页面上的 WDS 选项卡。（MyAP2 的 MAC 地址将显示为“Local Address”（本地地址）。）
 - 配置与 MyAP1 进行数据交换的 WDS 接口，首选从 MyAP1 的 MAC 地址开始。
 - 导航至 MyAP2 的射频设置，验证其使用的模式及用于广播的信道是否与 MyAP1 相同。（在本示例中，模式为 802.11b，信道为 6。）
 - 单击 **Update**（更新），确保保存设置。

20.4 更新设置

要更新 WDS 设置，请执行以下操作：

1. 导航至 WDS 选项卡页面。
2. 根据需要配置 WDS 设置。
3. 单击 **Update**（更新）按钮应用更改。

配置 SNMP

21

21.1 了解 SNMP 设置	211
21.2 导航至 SNMP 设置	213
21.3 配置 SNMP 设置	214
21.3.1 配置 SNMP 陷阱	216
21.3.2 更新 SNMP 设置	216

以下小节介绍如何在 9160 G2 无线网关企业管理器 API 上配置 SNMP 和相关设置：

21.1 了解 SNMP 设置

简单网络管理协议 (SNMP) 定义了记录、存储和共享网络设备相关信息的标准。SNMP 使得网络管理、故障排除和维护变得更容易。

任何受 SNMP 管理的网络的关键组件包括托管设备、SNMP 代理和管理系统。代理将其设备相关数据存储在管理信息库 (MIB) 中，并在请求时将这些数据返回至 SNMP 管理器。托管设备可以是网络节点，例如接入点基站、路由器、交换机、网桥、集线器、服务器和打印机。

9160 G2 无线网关可以用作 SNMP 托管设备，以无缝集成到网络管理系统，例如 HP OpenView 或 Devicescape Wireless Operations Center。

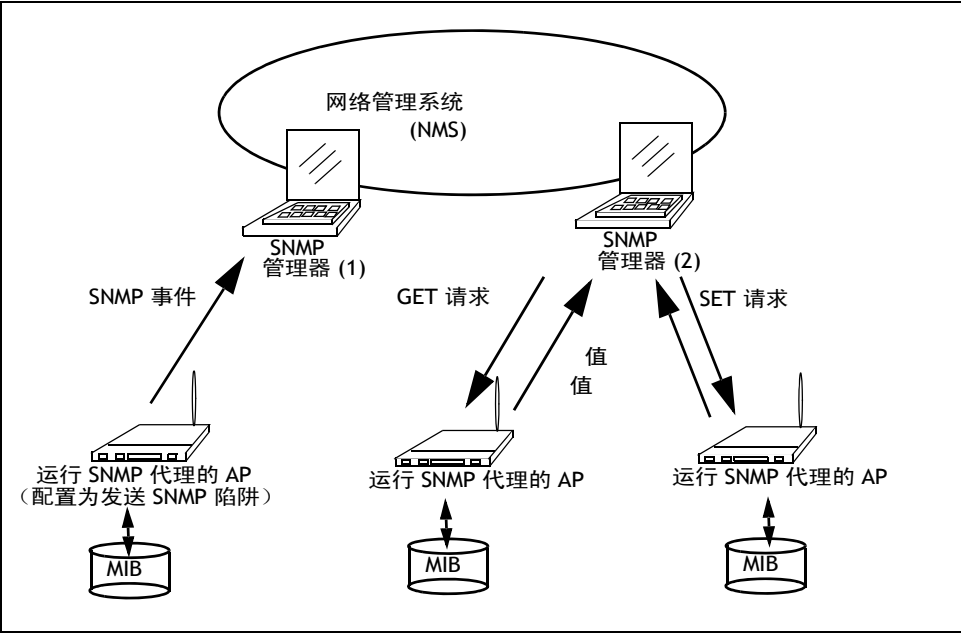
MIB 是网络上虚拟数据库中的对象或文件的集合。SNMP 使用特定的一组命令和查询，从 MIB 获取信息。

9160 G2 无线网关支持以下标准 SNMP MIB：

- 桥接 MIB 802.1d (RFC 1493)。
- SNMPv2 MIB (RFC 3418)。
- IEEE 标准 802.11 MIB （基础）。
- 接口组 MIB (RFC 2233)。
- 基于即将推出的 IEEE 802.11k MIB 的两个专有 MIB （无线 MIB 和系统 MIB）。它们分别提供 9160 G2 无线网关客户端关联列表和 AP 检测表的相关信息。专有系 MIB 提供维护功能，例如系统重启或固件升级。

9160 G2 无线网关还支持 SNMP 陷阱。图 21.1 显示 SNMP 如何在网络上工作。

图 21.1 在网络上运行的 SNMP



21.2 导航至 SNMP 设置

要配置 SNMP 设置，导航至 *Services*（服务） > *SNMP*，并如下所述更新字段。

图 21.2 SNMP 设置概述

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Modify SNMP Settings

SNMP ☒ Enabled ☐ Disabled

Read-only community name (for permitted GETs)

Port number the SNMP agent will listen to

Allow SNMP SET requests ☒ Enabled ☐ Disabled

Read-write community name (for permitted SETs)

Restrict the source of SNMP requests to only the designated hosts or subnets ☐ Enabled ☒ Disabled

Hostname or subnet of Network Management System

Trap Destinations

Community name for traps

Enabled

Hostname

☒

☒

☐

Update

21.3 配置 SNMP 设置

通过 9160 G2 无线网关提供 SNMP 代理的启动/停止控制、社区密码配置、MIB 访问以及 SNMP 陷阱目的地的配置，具体如下所述。

表 21.1 SNMP 设置

字段	描述
<i>SNMP Enabled/Disabled</i> (启用/禁用 SNMP)	<p>您可以选择是否想要在网络上启用 SNMP。默认情况下，禁用 SNMP。</p> <ul style="list-style-type: none">要启用 SNMP，单击 Enabled（启用）。要禁用 SNMP，单击 Disabled（禁用）。 <p>注：如果您未启用 SNMP，将禁用 SNMP 页面上的所有剩余字段。</p>
<i>Read-only community name for permitted GETs</i> (允许 GET 的只读社区名称)	<p>输入只读社区名称。</p> <p>在 SNMPv2c 中定义的社区名称用作简单的身份验证机制，以限制网络上向 SNMP 代理请求数据的机器。名称用作密码，且请求被认为是真实的（如果发送知道密码）。</p> <p>社区名称可以是任何字母数字格式。</p>
<i>Port number the SNMP agent will listen to</i> (SNMP 代理监听的端口号)	<p>默认情况下，SNMP 代理只监听端口 161 的请求。但您可以对此进行配置，以便代理监听另一端口上的请求。</p> <p>输入您希望 SNMP 代理监听请求的端口号。</p>
<i>Allow SNMP SET Requests</i> (允许 SNMP SET 请求)	<p>您可以选择是否允许 SNMP SET 请求。</p> <p>启用 SET 请求后，意味着网络上的机器可以对 AP 上配置的代理执行 SET 请求。</p> <p>注：SET 请求仅限于专有系统 MIB。</p> <ul style="list-style-type: none">要启用 SNMP SET 请求，单击 Enabled（启用）。要禁用 SNMP SET 请求，单击 Disabled（禁用）。
<i>Read-write community name for permitted SETs</i> (允许 GET 的读写社区名称)	<p>启用 SNMP SET 请求后，可以设置读写社区名称。</p> <p>设置社区名称与设置密码类似。仅接受通过此社区识别自己的机器发送的请求。</p> <p>社区名称可以是任何字母数字格式。</p>

表 21.1 SNMP 设置（续）

字段	描述
<i>Restrict the source of SNMP requests to only the designated hosts or subnets（将 SNMP 请求的来源限制为指定的主机或子网）</i>	<p>您可以限制允许的 SNMP 请求的来源。</p> <ul style="list-style-type: none">• 要限制允许的 SNMP 请求的来源，单击 Enabled（启用）。• 要允许任何来源提交 SNMP 请求，单击 Disabled（禁用）。
<i>Hostname or subnet of Network Management System（网络管理系统的主机名或子网）</i>	<p>指定可以对托管设备执行 GET 和 SET 请求的机器的 DNS 主机名或子网。</p> <p>同社区名称一样，它提供 SNMP 设置的安全级别。SNMP 代理仅接受此处指定的主机名或子网发送的请求。</p> <p>要指定子网，以 <i>AddressRange/MaskLength</i> 形式输入一个或多个子网地址范围，其中 <i>AddressRange</i> 是 IP 地址，<i>MaskLength</i> 是掩码位数。支持“NetAddress/NetMask”和“NetAddress/MaskLength”这两种格式。可为此提供单独主机，即 IP 地址或主机名。例如，如果您输入的范围是 192.168.1.0/24，则指定了地址为 192.168.1.0 的子网和子网掩码 255.255.255.0。</p> <p>地址范围用于指定特定 NMS 的子网。仅允许 IP 地址在此范围内的机器在托管设备上执行 GET 和 SET 请求。在上述示例中，地址在 192.168.1.1 到 192.168.1.254 范围内的机器可以在设备上执行 SNMP 命令。（子网范围内带有后缀 .0 的地址始终保留为子网地址，而范围中带有后缀 .255 的地址始终保留为广播地址）。</p> <p>又例如，若您输入的范围是 10.10.1.128/25，则 IP 地址为 10.10.1.129 到 10.10.1.254 的机器可以在托管设备上执行 SNMP 请求。在本示例中，10.10.1.128 是网络地址，10.10.1.255 是广播地址。将指定 126 个地址。</p>

21.3.1 配置 SNMP 陷阱

SNMP 陷阱使得 SNMP 托管设备（例如 9160 G2 无线网关）与指定主机之间的异步消息通信变得容易。如果网络管理系统 (NMS) 负责监控网络上的大量设备，那么定期查询网络上的每台设备是不实际的。在 AP 上启用 SNMP 事件陷阱后，各个设备便可以直接向 SNMP 管理器或 NMS 上的其他指定主机发送有关网络件的消息，例如网络接口正常或发生故障，客户端未能与接入点关联或对其进行身份验证，系统启动或关闭，以及网络拓扑结构更改。

SNMP 陷阱通过消除冗余 SNMP 请求节约了网络资源。此外，它还使得 SNMP 管理器能够更轻松地将网络故障排除。例如，如果 SNMP 管理器负责支持多台设备大型网络，且各台设备有大量对象，则向每台设备上的每个对象请求信息是不实际的。对于托管设备上的各个代理而言，最佳解决方案是通知管理器任何异常事件。通过发送事件陷阱进行通知。收到事件信息后，管理器可以选择采取什么操作（如有）。

表 21.2 SNMP 陷阱设置

字段	描述
<i>Community name for traps</i> （陷阱的社区名称）	输入与 SNMP 陷阱关联的全球社区字符串。 设备发送的陷阱将提供此字符串作为社区名称。
<i>Hostname</i> （主机名）	输入您想要向其发送 SNMP 陷阱的计算机的 DNS 主机名。 DNS 主机名示例：snmptraps.teklogix.com 由于 SNMP 陷阱是 SNMP 代理随机发送的，因此需要指定陷阱的确切发送位置。 确保您已选择相应的主机名旁边的 Enabled （启用）复选框。

21.3.2 更新 SNMP 设置

要更新 SNMP 设置，请执行以下操作：

- 1. 导航至 *SNMP* 选项卡页面。
- 2. 根据需要配置 SNMP 设置。
- 3. 单击 **Update**（更新）按钮应用更改。

22.1 概述	219
22.2 无线电协议	220
22.2.1 自适应轮询/争用协议	220
22.3 窄带菜单	220
22.3.1 窄带射频配置设置	220
22.3.1.1 RA1001A 射频参数	222
22.3.2 Connectivity Options (连接选项)	223
22.3.3 Connectivity Options (连接选项): Base Station (基站) 模式	223
22.3.3.1 Polling Protocol Parameters (轮询协议参数)	225
22.3.3.2 Radio Parameters (射频参数)	227
22.3.4 Connectivity Options (连接选项): RRM 模式	228
22.4 Connectivity (连接) 菜单	228
22.4.1 基站配置设置	230
22.4.2 RRM 组配置设置	231
22.4.2.1 RRM Groups (RRM 组)	233
22.4.2.2 Polling Protocol Parameters (轮询协议参数)	234
22.4.2.3 Radio Parameters (射频参数)	235
22.4.2.4 Group Parameters (组参数)	236
22.4.2.5 Remote Radio Modules (远程无线电模块)	237
22.4.3 无线链路功能配置设置	237
22.4.3.1 Radio Link Features (无线链路功能)	239
22.4.3.2 Automatic Radio Address (自动射频地址)	240
22.4.3.3 Automatic Terminal Number (自动终端号)	241
22.4.4 Hosts (主机) 菜单	242
22.4.4.1 9010 Configuration (9010 配置)	245

22.1 概述

9160 G2 无线网关可用作有线或无线基站，或用作远程无线电模块 (RRM)，利用无线电链路和 Psion Teklogix 专有协议，方便与移动数据终端之间的通信（请参阅第 220 页的“无线电协议”）。

作为有线基站，9160 G2 可以使用自适应轮询/争用协议 (第 220 页) 与无线移动数据终端进行通信，并通过网络连接到网络控制器。

作为无线基站，9160 G2 使用 802.11 WDS 与有线基站和移动数据终端进行通信。

作为 RRM，9160 G2 与移动数据终端之间无线电链路的运行和时间直接受控于使用时分复用无线电协议的网络控制器（请参阅下文中的“时分复用和蜂窝切换”）。它通过网络连接到网络控制器。

时分复用和蜂窝切换

在无线电链路上有两种工作方法。第一种方法被称为**蜂窝切换**。它在概念上与蜂窝状电话系统相似。在这里，各个基站使用不同的无线电信道。移动数据终端监控无线电链路，自动切换为无线电接收最佳的信道此蜂窝切换功能对主机是透明的。

第二种方法称为**时分复用**。在这里，站点中所有的远程无线电模块 (RRM) 基站均使用同一个信道。网络控制器通过 UDP/IP 网络协调轮询序列，这样 RRM 就不会同时进行传输。此时分复用功能对主机也是透明的。时分复用适合于事务率较低的站点。

可以在一个 Psion Teklogix 系统内组合使用蜂窝切换和时分复用：站点可以在两个或更多信道上运行，多个分组的时分复用基站使用一个信道，并在信道之间进行蜂窝切换。

在所有上述情况下，操作人员可以在整个站点中自由移动，且不会丢失通信。Psion Teklogix 系统会在不提醒用户的情况下，处理基站之间的信道切换和交。

对于用作基站或 RRM 的运行方式，应按照以下小节所述，相应地设置 *Configuration Main Menu*（配置主菜单）屏幕上 *Base Station Configuration*（基站配置）页面中的参数。

此外，必须应用相应的射频和主机参数。射频参数显示在 *Narrow Band*（窄带射频）的 *Radio*（射频）页面中，如第 22.3.1 节中所述。主机参数如第 242 页的“第 22.4.4 节 Hosts（主机）菜单”中所述。



注释：首先，应按第 4 章：“设置和启动的快速步骤”和第 5 章：“配置基本设置”中所述，设置 9160 G2 的主要参数。有关 RF 协议的详细信息，请参阅以下小节。

22.2 无线电协议

RF 协议以高效方式共用一个无线电信道，从而允许移动数据终端与基站进行通信。Psion Teklogix 系统使用两类 RF 协议中的一种：Psion Teklogix 自适应轮询/争用协议或非专有 IEEE 802.11 协议。

用作基站或 RRM 时，9160 G2 使用自适应轮询/争用协议。9160 G2 支持基站和 802.11 接入点同时运行。

22.2.1 自适应轮询/争用协议

自适应轮询/争用协议始终在波特率高达 19.2 kb/s 的窄带射频系统上使用，还可在速率更高的扩频系统上使用。

使用此协议运行的移动数据终端从 9160 G2 接收到轮询后才会进行传输。移动数据终端通常整体轮询。每次轮询后，会向移动数据终端组分配用于响应询的响应窗口。如果发生“冲突”——多台移动数据终端尝试在一个特定窗口中响应轮询——则正在轮询的 9160 G2 会划分重组，直到冲突的移动数据端可以在不冲突的情况下响应轮询。

此协议的自适应功能允许对响应窗口进行调整，以适应高 RF 或低 RF 的通信条件，并且当某台移动数据终端有大量需要收发的数据时可防止数据队列长。

使用自适应轮询/争用协议的系统可使用蜂窝选项，使移动数据终端操作人员可以漫游站点，在覆盖区域之间传输通信时保证通信不会中断。

如果未启用蜂窝基站，那么每次操作人员从一个基站覆盖区域移动到另一个区域时，移动数据终端屏幕上会显示消息“RESET: Press Enter”（重置：按下 Enter）。

22.3 窄带菜单

22.3.1 窄带射频配置设置

从 *Narrow Band*（窄带）菜单选项中选择 *Radio*（射频）子菜单后，9160 G2 显示它所设置的运行模式（基站或 RRM）的 *Narrow Band Radio Configuration Settings*（窄带射频配置设置）。显示的页面允许您设置 9160 G2 的状态，并检索 RA1001A 无线通讯卡的永久性通讯设置。

图 22.1 窄带射频设置概览

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View NarrowBand radio configuration settings

Radio Card: **Installed**

Radio Card Status: ☒ Enabled ☐ Disabled

Update

General Parameters:
Modulation: 2 Level
Baud Rate: 9600
Band Start: 450 MHz
Band Size: 20 MHz
Frequency Step: 12500 Hz
Channel Bandwidth: 25000 Hz
Collision Threshold: 1154ms
TX Delay, 4 Level: 11ms
Preamble, 2 Level: 10DEL,1SOH chars
Preamble, 4 Level: 6DEL,1SOH chars

Tuning Values:
Data Squelch: 62
Frequency Adjust: -100
Power: 88
Deviation, 4 Level: 66
Deviation, 2 Level: 44
Local Oscillator Adjust: 0
Demodulator Adjust: 181
TCXO Adjust: 122

Frequencies:

Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

Radio Card Status （无线通讯卡状态）

此参数可启用或禁用窄带射频。出于测试目的而要求没有无线电干扰时，可以暂时禁用此卡。按下 **Update** （更新）按钮初始化更改。

22.3.1.1 RA1001A 射频参数

Narrow Band Radio Configuration Settings （窄带射频配置设置）页面显示 RA1001A 窄带射频的 *General* （常规）、*Frequencies* （频率）和 *Tuning Values* （调谐值）参数。这些是制造商的设置，不可配置。下图中显示了这些设置：

图 22.2 RA1001A 射频参数

General Parameters:	
Modulation:	2 Level
Baud Rate:	9600
Band Start:	450 MHz
Band Size:	20 MHz
Frequency Step:	12500 Hz
Channel Bandwidth:	25000 Hz
Collision Threshold:	1154ms
TX Delay, 4 Level:	11ms
Preamble, 2 Level:	10DEL,1SOH chars
Preamble, 4 Level:	6DEL,1SOH chars

图 22.3 RA1001A 射频调谐值

Tuning Values:	
Data Squelch:	62
Frequency Adjust:	-100
Power:	88
Deviation, 4 Level:	66
Deviation, 2 Level:	44
Local Oscillator Adjust:	0
Demodulator Adjust:	181
TCXO Adjust:	122

图 22.4 RA1001A 射频频率

Frequencies:		
Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

22.3.2 Connectivity Options (连接选项)

当您选择此子菜单时，显示的页面允许您将 9160 G2 设置为在基站或 RRM 模式下运行。

22.3.3 Connectivity Options (连接选项)： Base Station (基站) 模式

对于 Operating Mode (操作模式) 设置为 Base Station (基站) 的 9160 G2，进入 Connectivity Options (连接选项) 子菜单后，将显示 Polling Protocol Parameters (轮询协议参数) 和 Radio Parameters (射频参数)。

图 22.5 轮询协议参数和射频参数概览

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode:

Base Station

Base Station

RRM

Auto-Startup:

☒ Enabled

☐ Disabled

Shared Channel:

☐ Enabled

☒ Disabled

Polling Protocol Parameters:

Number of Poll Windows:

3

(Range 2..4)

Size of Poll Windows:

8

(Range 5..32)

Maximum Message Segment Size:

100

(Range 32..116)

Number of Retries:

3

(Range 1..7)

Collision Size:

6

(Range 3..10)

Free Window Factor:

0

(Range 0..7)

Message Mode Limit:

4

(Range 0..7)

Callsign Period:

0

(Range 0..60)

Callsign String:

Teklogix

(Max 10 letters or digits)

Radio Parameters:

Sync Delay:

22

(Range 3..45)

Remote Tx On:

13

(Range 3..60)

Active Channel:

1

(Range 1..20)

Update

Operating Mode（操作模式）

此参数允许您将 9160 G2 的操作模式设为 **Base Station**（基站）或 **RRM**。

Auto-Startup（自动启动）

当 9160 G2 重新启动时，此参数立即启用轮询。如果将 *Auto-Startup*（自动启动）设为 **Disabled**（禁用），9160 G2 将会等待，直到从网络控制器中初始化轮询。

Shared Channel（共用信道）

Shared Channel（共用信道）仅在荷兰使用以满足政府要求。设为 **Enabled**（启用）时，将对轮询实行时间限制。每 2 秒一次轮询之后，会有 0.5 秒的静音 — 不发生任何轮询。

此外，如果在信道上检测到另一个运营商，9160 G2 将停止在该信道上进行无线电传输，直到路径清除。

22.3.3.1 Polling Protocol Parameters（轮询协议参数）

Polling Protocol Parameters:		
Number of Poll Windows:	<input type="text" value="3"/>	(Range 2..4)
Size of Poll Windows:	<input type="text" value="8"/>	(Range 5..32)
Maximum Message Segment Size:	<input type="text" value="100"/>	(Range 32..116)
Number of Retries:	<input type="text" value="3"/>	(Range 1..7)
Collision Size:	<input type="text" value="6"/>	(Range 3..10)
Free Window Factor:	<input type="text" value="7"/>	(Range 0..7)
Message Mode Limit:	<input type="text" value="4"/>	(Range 0..7)
Callsign Period:	<input type="text" value="0"/>	(Range 0..60)
Callsign String:	<input type="text" value="Teklogix"/>	(Max 10 letters or digits)

Number of Poll Windows（轮询窗口数量）

此参数定义 9160 G2 将使用的轮询窗口的数量。分配给此参数的值取决于所使用的移动数据终端数量和无线电链路协议。表 22.1 显示了如何确定分配给 *Number of Poll Windows*（轮询窗口的数量）参数的值。

表 22.1 轮询窗口的数量 - 蜂窝协议

移动数据终端的数量	窗口的最小数量
1-16	2
17-81	3
82-256	4

Size of Poll Windows (轮询窗口的大小)

为此参数分配的值确定了在正常轮询窗口中，可以在 9160 G2 和移动数据终端之间传递的最大消息。可以调整窗口大小，以适合从 5 到 32 个字符的任何位置。

较大窗口会增加轮询周期和响应时间。较小窗口会增加消息和长消息轮询的数量，同时增加响应时间。



重要说明：在“蜂窝”模式下，此参数的最小值为 8。

Maximum Message Segment Size (最大消息段大小)

此参数确定了可以在消息模式下传递至移动数据终端或在长消息模式下从移动数据终端传递的最大单条消息。在 9160 G2 基站中，在此参数中输入的值必须大于或等于在网络控制器或 9160 G2 微型控制器中输入的值。此参数的围介于 32 和 116 个字符之间。（较长的消息会分为多个包。）默认值为 100。

Number of Retries (重试次数)

此参数确定了未收到移动数据终端的确认时 9160 G2 尝试重发消息的次数。（这些重试在连续轮询中不一定会发生，因为未完成的消息会返回至消息队的底部。）所有重试次数用完后，移动数据终端“脱机”工作。直到移动数据终端“联机”工作后，9160 G2 才会向其传输消息。允许值的范围为 1 到 7。

Collision Size (冲突大小)

此参数降低了将无线电链路上的随机噪音解释为移动数据终端之间冲突的可能性。当 9160 G2 不必要地解决冲突时，响应时间会增加。

Collision Size (冲突大小) 会在收到错误消息 (CRC、CD 丢失等) 前，对收到的字符数量设置上限。如果此参数的值为 8，则在无线电链路上紧随其后出现了错误消息的 8 个或更少字符将被视为噪音。如果超过 8 个字符，则被视为冲突。可接受的值为 3 到 10。

Free Window Factor (自由窗口系数)

在此参数中输入的值确定是否使用“自由窗口模式”。在自由窗口模式下，未分配任何其他窗口的所有移动数据终端均可使用自由窗口。

在此参数中输入值 0 (零)，将禁用自由窗口模式。增加此参数值可提高在自由窗口中传输消息的可能性。

Message Mode Limit (消息模式限值)

此参数定义了消息模式轮询开始前，必须加入传输队列的消息数量的上限。接受的值为 0 到 7，其中 0 禁用消息模式。



注释：移动数据终端和过去事件的数量也是确定是否启动消息模式的算法的组成部分。

Callsign Period（呼号周期）

定期传输呼号作为有声摩斯电码信号。此参数指定了呼号传输之间的时间间隔（以分钟为单位）。可接受的值为 **0** 到 **60**。联邦机构加拿大工业部和美国联邦通信委员会要求，各系统每隔 15 分钟传输一次自己的识别呼号。

在不要求呼号的国家/地区，将此参数设为 **0** 可阻止传输任何呼号，实现移动数据终端内更短的轮询暂停和更快的信道切换。

Callsign String（呼号字符串）

此字符串限长 **10** 个字符。所有字符均为数字或字母。在传输的呼号的开头添加前缀“DE”（发送方）。

22.3.3.2 Radio Parameters（射频参数）

Radio Parameters:		
Sync Delay:	<input type="text" value="18"/>	(Range 3..45)
Remote Tx On:	<input type="text" value="4"/>	(Range 3..60)
Active Channel:	<input type="text" value="1"/>	(Range 1..20)

Sync Delay（同步延迟）



重要说明：在不清楚了解无线电协议时间设置的情况下，不应在出厂设置中更改此参数。

Sync Delay（同步延迟）指定基站传输时间和第一个响应窗口之间的延迟，以字符倍数测量延迟。为此参数分配的值必须与系统中的其他基站和移动数据终端兼。RA1001A 射频提供两级或四级调制，分别提供 4800 bps 和 9600 bps 的波特率，或 9600 bps 和 19200 bps 的波特率。

以 9600 波特运行的两级调制窄带射频的默认设置为 **23**。

以 19200 波特运行的四级调制窄带射频的默认设置为 **31**。

Remote Txon（远程传输开启时间）

Remote Txon（远程传输开启时间）适应移动数据终端（远程）中射频的开启时间。它指定了输出实时数据前发送至射频的填充字符数量。由于此参数基于字符倍，因此具体数字取决于无线电链路波特率。

在所有移动数据终端和基站设备上，分配给 *Remote Txon*（远程传输开启时间）的值必须是一致的。允许的值范围为 **3** 到 **60**。



重要说明：在不了解无线电协议的时间设置的情况下，不应在出厂设置中更改此参数。

Active Channel（活动信道）

此参数确定了 9160 G2 使用的无线电信道。它使信道可用于移动数据终端的信道搜索。必须使用在 *Narrow Band Radio Configuration Settings*（窄带射频配置设置）页面中显示的频率，对选定的信道进行配置。有关相关信道和频率的列表，请参阅第 223 页的图 22.4。

22.3.4 Connectivity Options（连接选项）：RRM 模式

对于 Operating Mode 设为 RRM 的从属 9160 G2，进入 *Connectivity Options*（连接选项）子菜单后，9160 G2 显示 RRM 参数。

Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode:

RRM

Remote Radio Module Parameters:

IP Port:

16132

Update

IP Port（IP 端口）

此参数允许您输入作为 RRM 从属设备运行的 9160 G2 所使用的监听端口号。端口号为 **1024** 到 **32767** 之间的值。



重要说明：在这里输入的端口号必须与在网络控制器的 RRM 配置中为此 9160 G2 输入的端口号匹配。

22.4 Connectivity（连接）菜单

9160 G2 无线网关可以用作基站或远程无线电模块 (RRM)，它使用一系列主机平台，方便移动数据终端与无线基站和网络控制器（Psion Teklogix 9500 通讯服务器或 9160 G2 无线网关）之间的通信。此外，网络控制器还可以是运行 Psion Teklogix SDK（处理程序）的主机。

9160 G2 还可用作网络上另一台 9160 G2 的从属基站。

图 22.6 基站配置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

View Base Station configuration settings

Slave Base Stations:

Number of configured Slave Base Stations: 0

Base Station Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed Base Station

IP Address: 0.0.0.0 Port: 16100

Message Size: 100 (Range 32..116)

Auto-Startup: ☒ Enabled ☐ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Base Station.

Default

Update

Cancel

22.4.1 基站配置设置

基站使用 Psion Teklogix 专有协议，通过无线电链路进行通信。基站可以通过以太网使用 TCP/IP 连接到网络控制器。由于基站通过无线电链路和移动数据端进行通信，因此 9160 G2 使用自适应轮询/争用 RF 协议（请参阅第 220 页的“无线电协议”了解协议详情）。

9160 G2 控制无线电链路的运行和时间设置。各基站使用不同的无线电信道，而移动数据终端使用蜂窝切换在基站间漫游。

以下页面上显示的选项和参数允许您将 9160 G2 配置为通过以太网连接至多达 32 台从属 9160 G2 基站的主基站。主 9160 G2 连接到 9500 通讯服务器，或连接到多达 6 台运行 Psion Teklogix 软件开发工具包的主机。使 *Connectivity*（连接）下的 *Base Station*（基站）选项，可以在系统中添加一个新的从属基站，或更改现有从属基站上的参数。

按下 **Update**（更新）按钮将保存您的设置；按下 **Default**（默认）按钮将重新加载该基站的默认配置值。

Number of Configured Slave Base Stations（已配置的从属基站数量）

您最多可以配置 32 个从属 9160 G2 基站。

Base Station Number（基站编号）

此参数表示分配的基站编号。从下拉列表中选择 **Base Station Number**（基站编号）后，显示可以修改或删除的该主机的参数。通过选择未分配的编号并配置其参数，可以添加新的从属基站。

Status（状态）

使用此参数可启用或禁用从属基站。

Description（描述）

在此参数中输入的名称可用作识别从属基站 IP 地址的另一种方式。

IP Address（IP 地址）

此参数提供从属基站的对应 IP 地址。*IP Address*（IP 地址）必须是唯一值，这样才能够识别网络上的各个从属基站。

接受值的范围为 0.0.0.0 到 239.255.255.255。

IP 端口的默认值为 16100。

Message Size （消息大小）

Message Size （消息大小）确定可以传递至移动数据终端的最大单条消息。此参数的范围介于 **32** 和 **380** 个字符之间。（较长的消息分为多个包。）

对于轮询协议基站，上限值为 **116**。

Auto-Startup （自动启动）

当此参数设为 **Enabled** （启用）时，从属基站将在主 **9160 G2** 启动时开始轮询。当 *Auto-Startup* （自动启动）设为 **Disabled** （禁用）时，未收到主机的开始轮询命令前，基站不会开始轮询。

22.4.2 RRM 组配置设置

9160 G2 不仅可用作远程无线电模块（RRM，请参阅第 228 页的“Connectivity Options （连接选项）：RRM 模式”），还可控制其他 RRM。要使用 9160 G2 控制 RRM，必须配置 RRM 组。一个 RRM 组可以由 1 至 4 个 RRM 组成。

一个 RRM 组中的所有 RRM 在同一个无线电信道上运行。9160 G2 协调一个 RRM 组中所有 RRM 的传输（因此，控制 9160 G2 有时也被称为“时分复用主机”）。

图 22.7 RRM 组配置设置概览

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View RRM Groups configuration settings

RRM Groups:

Number of Configured RRM Groups:0

RRM Group Number:1

Status:

Enabled

Disabled

Description:Unnamed RRM Group

Auto-Startup:

Enabled

Disabled

Shared Channel:

Enabled

Disabled

Polling Protocol Parameters:

Number of Poll Windows:3(Range 2..4)

Size of Poll Windows:8(Range 5..32)

Maximum Message Segment Size:100(Range 32..116)

Number of Retries:3(Range 1..7)

Collision Size:6(Range 3..10)

Free Window Factor:0(Range 0..7)

Message Mode Limit:4(Range 0..7)

Callsign Period:0(Range 0..60)

Callsign String:Teklogix(Max 10 letters or digits)

Radio Parameters:

Sync Delay:22(Range 3..45)

Remote Tx On:13(Range 3..60)

Active Channel:1(Range 1..20)

Group Parameters:

Combination 1:

(Sequence of RRM indices)

Combination 2:

(Sequence of RRM indices)

Remote Radio Modules:

	Enabled	Description	IP Address : Port	
1	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
2	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
3	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
4	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132

Update

22.4.2.1 RRM Groups （RRM 组）

RRM Groups:

Number of Configured RRM Groups: 0

RRM Group Number: 1 ▼

Status: ☐ Enabled ☒ Disabled

Description:

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

在此屏幕中，用户可以设置新 RRM 组的选项。各 RRM 必须是 RRM 组的成员，9160 G2 中可配置多个 RRM 组。一个 RRM 组可包含 1 至 4 个 RRM。

此屏幕与第 223 页的 “Connectivity Options （连接选项）：Base Station （基站）模式” 中的屏幕非常相似，不同之处在于，这些射频菜单中配置的参数适用于 9160 G2 中的 RA1001A 射频，而这里配置的参数适用于其他远程 9160 G2 (RRM)。

Number of Configured RRM Groups （已配置 RRM 组的数量）

显示在此 9160 G2 中配置的 RRM 组的数量。

RRM Group Number （RRM 组编号）

此参数表示分配的 RRM 组编号。从下拉列表中选择 **RRM Group Number** （RRM 组编号）后，显示可以修改或删除的该组的参数。通过选择未分配的编号并配置其参数，可以添加新的 RRM 组。

Status （状态）

该参数可启用或禁用此 RRM 组。

Description （描述）

此文本框允许用户输入新 RRM 组的名称。该值可以是任何文本字符串。默认值是 **Unnamed RRM Group** （未命名的 RRM 组）。

Auto-Startup （自动启动）

当此参数设为 **Enabled** （启用）时，9160 G2 会在启动时建立与此 RRM 组中的 RRM 的通信，并开始自动轮询。当 *Auto-Startup* （自动启动）设为 **Disabled** （禁用）时，9160 G2 会在启动时建立与此 RRM 组中的 RRM 的通信，但未收到主机的开始轮询命令前，不会在此 RRM 组中开始轮询。9160 G2 启动时，如果 RRM 组中至少有一个 RRM 在运行，则轮询开始。

Shared Channel （共用信道）

如果此参数设为 **Enabled** （启用），则 9160 G2 会在轮询前检查此 RRM 组使用的无线电信道上的其他通信。

如果此参数设为 **Disabled** （禁用），则 9160 G2 会假设其独享此 RRM 组的无线电信道，并在不检查无线通信的情况下轮询。

在荷兰安装系统时需要使用该参数。

22.4.2.2 Polling Protocol Parameters （轮询协议参数）



警告： 这些参数已为您的系统预先配置，未正确理解它们是如何影响无线链路时不要对其进行更改。

Polling Protocol Parameters:		
Number of Poll Windows:	<input type="text" value="3"/>	(Range 2..4)
Size of Poll Windows:	<input type="text" value="8"/>	(Range 5..32)
Maximum Message Segment Size:	<input type="text" value="100"/>	(Range 32..116)
Number of Retries:	<input type="text" value="3"/>	(Range 1..7)
Collision Size:	<input type="text" value="6"/>	(Range 3..10)
Free Window Factor:	<input type="text" value="0"/>	(Range 0..7)
Message Mode Limit:	<input type="text" value="4"/>	(Range 0..7)
Callsign Period:	<input type="text" value="0"/>	(Range 0..60)
Callsign String:	<input type="text" value="Teklogix"/>	(Max 10 letters or digits)

Number of Poll Windows （轮询窗口数量）

此文本框允许用户指定 RRM 在发送轮询后用于监听移动数据终端响应的轮询窗口的数量。允许值的范围为 **2 到 4**。默认值为 **3**。

Size of Poll Windows （轮询窗口的大小）

此文本框允许用户指定此 RRM 组的 RRM 用于监听移动数据终端响应的轮询窗口的大小。允许值的范围为 **5 到 32**。默认值为 **8**。

Maximum Message Segment Size （最大消息段大小）

此文本框允许用户指定通过 Psion Teklogix 无线网络发送的最大消息段的大小（以字节数为单位）。较大的消息分为几部分。允许值的范围为 **32 到 116**。默认值为 **100**。

Number of Retries （重试次数）

此文本框允许用户指定 RRM 未收到移动数据终端的确认时，在声明移动数据终端脱机前，重新传输消息至移动数据终端的次数。允许值的范围为 **1 到 7**。默认值为 **3**。

Collision Size （冲突大小）

此文本框允许用户指定 RRM 收到的被解释为干扰 Psion Teklogix 设备传输的噪音的最小字符数量。超过此阈值后，RRM 开始解决冲突。允许值的范围为 **3 到 10**。默认值为 **6**。

Free Window Factor （自由窗口系数）

此文本框允许用户指定任何移动数据终端传输过程中，RRM 在其轮询中包含自由窗口的可能性。允许值的范围为 **0 到 7**。默认值为 **0**。

Message Mode Limit （消息模式限值）

此文本框允许用户指定在轮询传输中包含消息模式轮询的可能性。允许值的范围为 **0 到 7**。默认值为 **4**。

Callsign Period （呼号周期）

此文本框允许用户指定呼号传输之间的时间量。该参数以分钟为单位。0（零）值表示未传输任何呼号。允许值的范围为 **0 到 60**。默认值为 **0**。

Callsign String （呼号字符串）

此文本框允许用户指定作为 RRM 的呼号传输的文本。该文本作为摩斯电码传输。默认值为 **Teklogix**。

22.4.2.3 Radio Parameters （射频参数）

Radio Parameters:		
Sync Delay:	<input type="text" value="22"/>	(Range 3..45)
Remote Tx On:	<input type="text" value="13"/>	(Range 3..60)
Active Channel:	<input type="text" value="1"/>	(Range 1..20)

因为对于给定的时分复用 RRM 组，有些射频参数是相同的，因此用户只需在 9160 G2 上配置一次；然后，9160 G2 会将这些参数传递到该组中的 RRM。这些数包括同步延迟 (*Sync Delay*)、远程传输开启时间 (*Remote Txon*) 以及要使用的信道编号 (*Active Channel*)。

尽管该组各个 RRM 中的 RA1001A 窄带射频是单独配置的， 9160 G2 假设它们的配置是一致的。为确保这一点， 9160 G2 会查看各个 RRM 返回的特定参数。这些数包括无线电波特率和传输开启时间。

这些参数与同一组中的其他 RRM 返回的值进行比较。显示错误消息说明这些值不匹配，但最坏的情况是，该值已被选择使用。



警告： 这些参数已为您的系统预先配置，未正确理解它们是如何影响无线电链路时不要对其进行更改。

Sync Delay （同步延迟）

此文本框允许用户指定在 RRM 的传输和第一个响应窗口之间插入的延迟字符的数量。允许值的范围为 **3 到 45**。默认值为 **22**。

Remote Txon （远程传输开启时间）

此文本框允许用户指定在移动数据终端发送消息数据前通过其射频发送的填充字符的数量。允许值的范围为 **3 到 60**。默认值为 **13**。

Active Channel （活动信道）

此文本框允许用户指定 RRM 组中的所有 RRM 使用的无线电信道。允许值的范围为 **1 到 20**。默认值为 **1**。

22.4.2.4 Group Parameters （组参数）

Group Parameters:	
Combination 1:	<input type="text"/> (Sequence of RRM indices)
Combination 2:	<input type="text"/> (Sequence of RRM indices)

Combination （组合）

这些文本框允许用户指定称为*组合*的 RRM 子组。如果此 RRM 组中的两个或多个 RRM 的覆盖区域不重叠，则非重叠 RRM 可同时轮询。这可加快系统响应时间并减少网络上的信号量。未分配组合的 RRM 会在组合轮询后单独轮询。

例如，如果 RRM 组有 3 个 RRM，且 RRM 1 和 3 不重叠，则 RRM 1 和 3 可以放入一个子组（*Combination 1*）。然后，它们将同时轮询。RRM 2 可放入另一个子组（*Combination 2*）。轮询在两个子组之间交替。

要配置组合，请将 RRM 的编号放入该组合的文本框内。编号与 *Remote Radio Modules*（远程无线电模块）菜单上 RRM 列表中指定的 RRM 的编号相对应（请参阅第 237 页）。例如，*Combination 1* 的文本框中的“13”会将 RRM 1 和 3 放入该子组。



注释：配置 RRM 组合时，确保已配置的 RRM 按顺序排列，且未丢失编号，而丢失编号的情况会在删除和添加 RRM 时发生。组合使用 RRM 的顺序与其在列表中显的顺序相同，而不是与它们在列表中的编号相同。

22.4.2.5 Remote Radio Modules（远程无线电模块）

Remote Radio Modules:				
	Enabled	Description	IP Address : Port	
1	<input checked="" type="checkbox"/>	Built-in	10.128.75.174	16132
2	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
3	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
4	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132

该菜单显示组成此 RRM 组的 RRM，包括在以 RRM 模式运行的 9160 G2 的 *Connectivity Options*（连接选项）子菜单中设置的描述、IP 地址和端口号（请参阅第 228 页的“Connectivity Options（连接选项）：RRM 模式”）。可从此菜单启用或禁用各个 RRM。

22.4.3 无线电链路功能配置设置

从 *Connectivity*（连接）选项列表中进入 *Radio Link Features*（无线电链路功能）后，将打开轮询和蜂窝参数的配置设置页面。

图 22.8 无线电链路功能配置设置概览

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

View Radio Link Features configuration settings

Radio Link Features:

Operate in Cellular Mode:

Enabled

Disabled

Poll ID:

35

 Range (0..255)

Polling Protocol Terminal Timeout:

60

 Range (1..240)

Percent Polling Protocol Terminal Timeout:

75

 Range (50..90)

Direct TCP Connections for TekTerm:

Enabled

Disabled

Direct TCP Check Duplicate Terminal Number:

Enabled

Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number:

2

 Range (2..365)

Automatic Radio Address

First Address:

1024

 Last Address:

2048

 Ranges (1..3840)

Automatic Terminal Number

Group Ranges (1..1024)

				Comments
1	<div>0</div>	...	<div>0</div>	
2	<div>0</div>	...	<div>0</div>	
3	<div>0</div>	...	<div>0</div>	
4	<div>0</div>	...	<div>0</div>	
5	<div>0</div>	...	<div>0</div>	

Update

22.4.3.1 Radio Link Features （无线电链路功能）

Radio Link Features:

Operate in Cellular Mode:

☒ Enabled ☐ Disabled

Poll ID:

35

Range (0..255)

Polling Protocol Terminal Timeout:

60

Range (1..240)

Percent Polling Protocol Terminal Timeout:

75

Range (50..90)

Direct TCP Connections for TekTerm:

☐ Enabled ☒ Disabled

Direct TCP Check Duplicate Terminal Number:

☒ Enabled ☐ Disabled

Expiration period (in days) for Automatic Radio Address and Terminal Number:

2

Range (2..365)

Operate in Cellular Mode （以蜂窝模式运行）

要用作蜂窝基站，此参数应设为 **Enabled** （启用）。



注释：还必须将 9500 通讯服务器设为蜂窝模式。

Poll ID （轮询 ID）

在窄带射频的自适应轮询/争用协议中，*Poll ID* （轮询 ID）用于向各个基站分配唯一的地址。随着移动数据终端从一个基站移动到另一个，基站将此地址传输至移动数据终端，识别多基站系统中的个 9160 G2。

Polling Protocol Terminal Timeout （轮询协议终端超时）

此参数确定了 9160 G2 声明其脱机前移动数据终端不工作的时间（以分钟为单位）。发生这种情况前，*Percent Polling Protocol Terminal Timeout* （轮询协议终端超时百分比）参数将声明移动数据终端脱机工作（参见下文）。

该移动数据终端从系统上移除后，需要重新初始化才能与 9160 G2 进行通信。该参数可减少在支持未进行通信的移动数据终端时导致的无线电链路上的销。允许值的范围为 **1** 到 **240**。

Percent Polling Protocol Terminal Timeout （轮询协议终端超时百分比）

此参数确定了 9160 G2 声明其脱机前允许移动数据终端不工作的时间。此时间表示为 *Polling Protocol Terminal Timeout* （轮询协议终端超时）参数的百分比（参见上文）。例如，如果 *Polling Protocol Terminal Timeout* （轮询协议终端超时）为 60，则该参数设为 75%，然后超时为 60 分钟 x 75% = 45 分钟。

脱机移动数据终端仍然被视为系统的组成部分。9160 G2 将对发送到脱机移动数据终端的消息排队。移动数据终端保持脱机状态，直到其传输一条联机信息。此参数值的范围为 **50** 到 **90**。

Direct TCP Connections for TekTerm （TekTerm 的直接 TCP 连接）

启用此参数后，当 9160 G2 通过 TCP/IP 用作主机的基站时，存储在 Psion Teklogix 移动数据终端中的 *TekTerm* 程序可直接连接至 9160 G2。

Direct TCP Check Duplicate Terminal Number （直接 TCP 检查重复终端号）

启用此参数时，9160 G2 将会拒绝尝试使用已被另一台移动数据终端使用的终端号进行连接的直接 TCP 移动数据终端。禁用时，最近连接的移动数据终端将优先于使用相同终端号的其他移动数据终端。

22.4.3.2 Automatic Radio Address （自动射频地址）

Automatic Radio Address		
First Address:	<input type="text" value="1024"/>	Last Address: <input type="text" value="2048"/>
Ranges (1..3840)		

使用无线电链路的各 Psion Teklogix 移动数据终端有唯一的射频地址编号，该编号是由 9160 G2 通过启用此参数自动分配的。

要**启用**该参数，第一个和最后一个射频地址编号的值必须介于 **1** 和 **3840** 之间。默认的值范围为 **1024 ... 2084**。要**禁用**该参数，将值设为 **0**。



注释： 启用该参数时：

1. 必须禁用 *Direct TCP Connections for TekTerm* （TekTerm 的直接 TCP 连接）（请参阅第 240 页）。
2. 必须启用移动数据终端中的 *Auto ID* （自动 ID）参数，才能自动分配射频地址。
3. 对于运行 802.IQ 以及使用 *Automatic Radio Address* （自动射频地址）和 *Automatic Terminal Number* （自动终端号）的会话的 9150 或 9160 G2 基站，请勿启用 *Auto Startup* 自动启动）（请参阅第 295 页）。

Expiration Period （有效期）

该参数指定了 9160 G2 声明其即将 “到期” 前，特定射频地址或终端号不工作的天数。可以将过期的地址或终端号重新分配给另一个射频或会话。



注释：要使用此功能，建议您启用 SNTP，并通过一个 SNTP 服务器来提供准确的过期时间。

22.4.3.3 Automatic Terminal Number （自动终端号）

为在移动数据终端中创建的各个应用会话分配一个终端号。此终端号有助于唯一识别与该会话之间收发的所有传输。

Automatic Terminal Number			
Group Ranges (1..1024)			Comments
1	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
2	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
3	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
4	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
5	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>

可自动为应用会话分配终端号。控制器还提供用于 TESS 和 ANSI 会话的组号。最多可以定义五组终端会话，并且可以向各组指定不同的终端号范围以进自动分配。这些范围在组之间不重叠。

这些组仅适用于 TESS 和 ANSI 会话。在移动数据终端中，TESS 或 ANSI 终端应用程序指定它们所属的组，并使用属于该组的 Automatic Terminal Number （自动终端号）分配范围。

所有其他会话类型假设 Automatic Terminal Number （自动终端号）分配范围为 1 到 3840，且不使用 “组” 参数。使用 Automatic Terminal Number （自动终端号）分配非 ANSI 和非 TESS 仿真（例如，远程插座）必须将其终端范围设为从 1 开始，并且此范围必须足够大才能容纳所有移动数据终端。

Radio Link Features （无线电链路功能）屏幕提供各个 Automatic Terminal Number （自动终端号）组的多个参数：由一个较低的终端号和一个较高的终端号指定的范围及备注。注是可用于描述该组的 ASCII 文本字符串。



注释: 启用 *Automatic Terminal Number* (自动终端号) 时:

1. 必须禁用 *Direct TCP Connections for TekTerm* (TekTerm 的直接 TCP 连接) (请参阅第 240 页)。
2. 必须启用移动数据终端中的 *Auto Session* (自动会话) 参数, 才能自动分配终端会话编号。

22.4.4 Hosts (主机) 菜单

9160 G2 用作基站时, 它必须与 “主机” (9500 通讯服务器) 或使用 Psion Teklogix 软件开发工具包 (SDK) 的主机进行通信。因此必须将与 9160 G2 通信的各主网络控制器、SDK 主机或主基站配置为主机。*Connectivity* (连接) 选项的 *Hosts* (主机) 页面显示从下拉列表中选择的主机的描述 (请参阅第 243 页的图 22.9)。

此选项中的菜单页面显示系统上出现的主机名。最多支持六台主机。配置主机后, 选择该主机的 **Host Number** (主机编号) 后, 将列出可修改或删除的参数。

图 22.9 基站主机配置设置概览

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

9010 Configuration:

No Online/Offline: ☐ Enabled ☒ Disabled

Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. Default

Update Cancel

配置的主机数量

Connectivity（连接）选项的 **Hosts**（主机）页面显示在系统上配置的主机数量。最多支持六台主机。

Host Number（主机编号）

该参数显示已分配的主机编号。从下拉列表中选择 **Host Number**（主机编号）后，将显示该主机中可以修改或删除的参数。通过选择未分配的编号并配置其参数，可以添加新的主机。

在多主机环境下切换主机时，RF 移动数据终端上也会显示主机编号。

Status（状态）

对于与此主机之间通信的移动数据终端，必须启用 **Status**（状态）。

Description（描述）

此文本框允许您为主机使用的协议命名。协议是移动数据终端通过各种物理介质（例如以太网和无线电链路连接）与主机进行通信的方法。

9160 G2 用作基站时，它使用网络连接与 **9010/TCP/IP** 主机通信。9010 协议是 Psion Teklogix 开发的专有异步协议，它使用 **TESS**（Teklogix 屏幕子系统）或 **ANSI** 数据流与移动数据终端进行通信。有关详细信息，参阅 *9500 通信服务器*、*SDK*、*TESS* 或 *ANSI* 相应的《*Psion Teklogix 用户手册*》。

First Terminal/Last Terminal（第一个终端/最后一个终端）

这些参数中输入的值指定了与主机通信的移动数据终端范围内的第一个和最后一个终端。这些终端编号与此特定主机对应。终端号的范围为 **1** 到 **3840**。

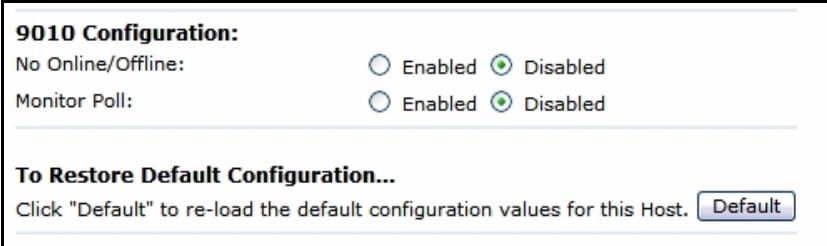
To Restore Default Configuration（要还原默认配置）

在 **Host**（主机）菜单页面的底部，可以单击 **Default**（默认）重新加载该主机的默认配置值。

Updating Settings（更新设置）

在主机配置过程中的任何时间点，您可以通过单击该页面底部相应的按钮，*更新设置*或*取消配置过程*。

22.4.4.1 9010 Configuration（9010 配置）



9010 Configuration:

No Online/Offline: ☐ Enabled ☒ Disabled

Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. [Default](#)

No Online/Offline（不联机/脱机）

如果此参数设为 **Enabled**（启用），则当移动数据终端的状态在联机和脱机之间切换时，9160 G2 基站**不会**通知主机。如果此参数设为 **Disabled**（禁用），9160 G2 会通知主机有关任何移动数据终端状态发生的变化。该参数的默认设置为 **Disabled**（禁用）。

Monitor Poll（监测轮询）

主机通常会在约 40 秒内将消息或空轮询发送至 9160 G2。如果此参数设为 **Enabled**（启用），9160 G2 基站从此主机监测消息和轮询；如果它未在 40 秒内收到消息或轮询，会关闭连接。该参数的默认设置为 **Disabled**（禁用）。

23.1 概述	249
23.2 微型控制器配置菜单	250
23.3 主机菜单	250
23.4 主机菜单选项	253
23.4.1 3274 仿真	254
23.4.1.1 仿真选项	254
23.4.1.2 TESS Options (TESS 选项)	255
23.4.1.3 Telnet Protocol Options (Telnet 协议选项)	265
23.4.1.4 Function Key Mappings (功能键映射)	268
23.4.2 5250 仿真	269
23.4.2.1 Emulation Options (仿真选项)	269
23.4.2.2 TESS Options (TESS 选项)	270
23.4.2.3 Telnet Protocol Options (Telnet 协议选项)	279
23.4.2.4 Function Key Mappings (功能键映射)	283
23.4.3 ANSI 仿真	284
23.4.3.1 仿真选项	284
23.4.3.2 Telnet Protocol Options (Telnet 协议选项)	287
23.4.3.3 Auto-Telnet/Auto-login (自动 Telnet/自动登录)	289
23.4.3.4 Function Key Mappings (功能键映射)	292

23.1 概述

Psion Teklogix 系统中的网络控制器可执行大量重要任务。其中之一是 *仿真*：在主机协议和 Psion Teklogix 移动数据终端使用的协议之间转换数据。

数据从主机发送至移动数据终端以提供显示内容，并将移动数据终端的操作结果返回至主机，此数据被称为数据流。主机可向移动数据终端提供各种型的数据流。

Psion Teklogix 移动数据终端可直接接受的数据流只有两种：*TESS* 和 *ANSI*。*TESS*（Teklogix 屏幕子系统）是 Psion Teklogix 移动数据终端使用的专用数据流。*ANSI* 数据流是有线 *ANSI* 移动数据终端使用的标准数据流类型。主机提供其它类型数据流必须转换为 *TESS* 或 *ANSI* 才能用于 Psion Teklogix 移动数据终端。这种转换可通过网络控制器中的仿真软件来实现。

9160 G2 无线网关具有仿真功能，可用作微型控制器。将 9160 G2 配置为微型控制器时，Psion Teklogix 移动数据终端可通过 9160 G2（不是 9500 通信服务器）模拟 *ANSI*、*5250* 或 *3274* 移动数据终端。



重要说明：9160 G2 专门用作小型低交易量站点的微型控制器。而支持 50 台以上移动数据终端的系统需要使用 9500 通信服务器。

9160 G2 无线网关用作微型控制器时，可支持最多 32 个联网基站和 50 台移动数据终端。9160 G2 微型控制器还可管理无线 LAN 配置。

9160 G2 配置为微型控制器时，可支持以下仿真类型：

- 通过以太网 LAN 使用 TCP/IP 的 5250 仿真。
- 通过以太网 LAN 使用 TCP/IP 的 3274 仿真。
- 通过以太网 LAN 使用 TCP/IP 的 ANSI 仿真。



注释：首先应按照本手册前面章节所述设置 9160 G2 主要参数。

也可使用 802.IQv2 协议将 9160 G2 集成到 mapRF 系统中（有关详细信息，请参阅第 299 页的“802.IQ v2 Features（802.IQ v2 功能）菜单”）。



注释：只有在通过控制台提示时使用密码解锁之后，才能使用微型控制器功能。

23.2 微型控制器配置菜单

用作微型控制器运行时，应该正确设置 *Hosts*（主机）页面中的参数。从 *Connectivity*（连接性）选项列表中，进入 *Hosts*（主机）后将打开 *Configuration Settings For A Base Station's Host*（基站主机的配置设置）页面。有关配置无线电协议参数的更多信息，请参阅第 237 页的“无线电链路功能配置设置”。

23.3 主机菜单

此选项中的菜单页面显示系统上出现的主机名。最多支持六台主机。对于与 9160 G2 微型控制器通信的每台主机，“Host（主机）”必须进行配置。配置主机后，选择该主机的 **Host Number**（主机编号）后，将列出可修改或删除的参数。

图 23.1 主机配置设置概述

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Maintenance

Configuration

Upgrade

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: Enabled Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

Emulation: 5250

5250 Emulation Options:

Write Error Code: Advisory text

Use International EBCDIC:

Allow null character in fixed fields:

TESS Options:

Field Underline Remapping: None

Alarm:

Clear:

Passthru:

Procedures:

Local:

Host Print:

Remote Print:

Pages: 8

Transmit Line: 0

AIAG: 0

Visible Match Character: 0

Hidden Match character: 0

Serial I/O: 0

Print Line: 0

Print Form Length: 0

Barcode: 0

Entry Line: 0

Field Overhead: 5

Command Region: 0, 0, 0, 0

Telnet Protocol Options:

Terminal Type: IBM-5251-11

Host Port: 23

Maximum Sessions per Terminal: 4

First Local Terminal Port: 10000

Local IP Address to Bind: 0.0.0.0

First Terminal Listen Port: 0

Actively Negotiate with Host:

Auto-telnet: DISABLE

Auto-telnet Host:

Auto-telnet without User Action:

Enable Virtual Device Names:

Configure Device Names: Configure

Device Name Prefix:

Function Key Mappings:

F1: F1 F14: F14 F27: F17

F2: F2 F15: F15 F28: F18

F3: F3 F16: CLEAR F29: UP

F4: F4 F17: PRINT F30: SESS

F5: F5 F18: HELP F31: ENTER

F6: F6 F19: F19 F32: ENTER

F7: F7 F20: F20 F33: ENTER

F8: F8 F21: F21 F34: ENTER

F9: F9 F22: F22 F35: ENTER

F10: F10 F23: F23 F36: ENTER

F11: F11 F24: F24 F37: ENTER

F12: F12 F25: DOWN F38: SELECTOR

F13: F13 F26: F16 F39: ENTER

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. Default

Update Cancel

When the 9160 acts as a Base Station, it must communicate with a "host" - a 9500 or 9400 network Controller, or a host computer using Psion Teklogix Software Development Kit (TSDK).

This page allows you to select the host names present on the system. Up to six hosts can be supported. A "host" must be configured for each master network controller, TSDK host, or master Base Station that communicates with the 9160.

Number Of Configured Hosts （配置的主机数量）

Connectivity（连接）选项的 *Hosts*（主机）页面显示在系统上配置的主机数量。最多支持六台主机。

Host Number （主机编号）

该参数显示已分配的主机编号。从下拉列表中选择 **Host Number**（主机编号）后，将显示该主机中可以修改或删除的参数。通过选择未分配的编号并配置其参数，可以添加新的主机。

在多主机环境下切换主机时，RF 移动数据终端上也会显示主机编号。

Status （状态）

对于与此主机之间通信的移动数据终端，必须启用 Status（状态）。

Description （描述）

此文本框允许您为主机使用的协议命名。协议是移动数据终端通过各种物理介质（例如以太网和无线电链路连接）与主机进行通信的方法。

9160 G2 用作基站时，它使用网络连接与 **9010/TCP/IP** 主机通信。9010 协议是 Psion Teklogix 开发的专有异步协议，它使用 TESS（Teklogix 屏幕子系统）或 ANSI 数据流与移动数据终端进行通信。有关详细信息，参阅 *9500 通信服务器*、*SDK*、*TESS* 或 *ANSI* 相应的《*Psion Teklogix 用户手册*》。

First Terminal/Last Terminal （第一个终端/最后一个终端）

这些参数中输入的值指定了与主机通信的移动数据终端范围内的第一个和最后一个终端。这些终端编号与此特定主机对应。终端号的范围为 **1** 到 **3840**。

仿真

此下拉菜单提供了 9160 G2 无线网关支持的主机仿真列表。9160 G2 与 Psion Teklogix 移动数据终端和基站一同使用，可以模拟 IBM 3278-2、5251-11 和 5555-B01 移动数据终端以及 ANSI 移动数据终端。

协议是移动数据终端通过各种介质（例如以太网和无线通信链路连接）与主机进行通信的方法。9160 G2 支持 TCP/IP 协议。支持的仿真包括：

- 9010/ TCP/IP（有关详细信息，请参见以下内容）。
- 3274 仿真（有关配置参数，请参见第 254 页到第 268 页）。
- 5250 仿真（有关配置参数，请参见第 269 页到第 283 页）。
- ANSI 仿真（有关配置参数，请参见第 284 页到第 292 页）。

9160 G2 无线网关用作基站时，它使用 9010 仿真（Psion Teklogix 开发的专有异步协议）与 9500 通信服务器通信或使用 Psion Teklogix 软件开发套件 (SDK) 的主机进行通信。有关将 9160 G2 配置为基站及 9010 仿真的更多信息，请参阅第 22 章：“9160 G2 用作基站”。

9160 G2 无线网关用作微型控制器时，它使用 3274 和 5250 仿真协议与 IBM 主机通信，或通过 ANSI 仿真协议与 ANSI 移动数据终端通信。

还原默认配置

在 Host（主机）菜单页面的底部，可以单击 **Default**（默认值）重新加载该主机的默认配置值。

更新设置

在主机配置过程中的任何时间点，您可以通过单击该页面底部相应的按钮，*更新*设置或*取消*配置过程。

23.4 主机菜单选项

选择现有 *Host Number*（主机编号）时，9160 G2 会显示主机的配置参数。5250、3274 和 ANSI 仿真有四个子菜单：主机的 *Emulation Options*（仿真选项）、*TESS Options*（TESS 选项）、*Telnet Protocol Options*（Telnet 协议选项）和 *Function Key Mappings*（功能键映射）（有关该页面的概述，请参见第 251 页的图 23.1）。

23.4.1 3274 仿真

23.4.1.1 仿真选项

3274 Emulation Options:
Is Host Fujitsu: ☐
Use International EBCDIC: ☐
Allow null character in fixed fields: ☐

通过 IBM 3274 或 IBM 5250 仿真，9160 G2 微型控制器可将来自主机的应用数据流转换为 TESS（Teklogix 屏幕子系统）命令。本页的一些参数可控制主机屏幕向 TESS 的转换。

Is Host Fujitsu（是主机 Fujitsu）

此参数启用后，9160 G2 微型控制器要求来自主机的数据包含 Fujitsu 主机发出的命令等。启用此参数之后，将使标准 IBM 格式代码（用于启动字段和设置缓冲区等）替换为 Fujitsu 主机使用的代码。

Use International EBCDIC（使用国际 EBCDIC）

此参数启用后，9160 G2 微型控制器可使用国际 EBCDIC 字符集，交换字符 **!** 和 **]** 的位置。

Allow null character in fixed fields（固定字段可存在 Null 字符）

此参数启用后，对于拥有视觉视频属性（反相显示）的字段，9160 G2 微型控制器允许其空格处出现 Null 字符。3274 主机仿真默认为禁用。

23.4.1.2 TESS Options （TESS 选项）

TESS Options:

Alarm:

☐

Clear:

☐

Passthru:

☐

Procedures:

☐

Local:

☐

Host Print:

☐

Remote Print:

☐

Pages:

8

(Range 1..79)

Transmit Line:

0

(Range 0..24)

AIAG:

0

(Range 0..255)

Visible Match Character:

0

(Range 0..255)

Hidden Match character:

0

(Range 0..255)

Serial I/O:

0

(Range 0..255)

Print Line:

0

(Range 0..24)

Print Form Length:

0

(Range 0..24)

Barcode:

0

(Range 0..255)

Entry Line:

0

(Range 0..24)

Field Overhead:

5

(Range 0..80)

Command Region:

0

,

0

,

0

,

0

Alarm （警报）

此参数启用后，如果 *Command Region* （命令区域）参数规定位置的应用程序屏幕上出现词语 “ALARM （警报）”，移动数据终端将发出蜂鸣声 （请参见第 264 页）。词语 “ALARM （警报）” 应为仅供显示字段。



注释：必须启用 *Command Region* （命令区域）参数之后，此参数才生效。

Clear （清除）

此参数启用后，9160 G2 微型控制器将为填充为空格的输入字段创建一个空条目字段。

一些主机应用程序依赖显示字符的视频属性突出显示字段，对输入字段尤其如此。例如，应用程序屏幕可能使用反相显示定义所有字段并使用空格填充字段。这对支持反相显示的移动数据终端有效。但是，对于不支持反相显示的移动数据终端，由于字段完全由空格组成，因此该字段不可见。

默认情况下，显示在 Psion Teklogix 移动数据终端的所有空输入字段可通过在移动数据终端配置中选择的“输入字符”实现突出显示。



注释：只对从主机接收的屏幕执行此操作。发送至主机的数据不受影响。

Passthru （直通）

此参数启用后，9160 G2 使主机能够直接向 RF 移动数据终端的串行端口发送数据。最常用于打印。

准备用于传递的主机屏幕

在将要通过移动数据终端串行端口发送的屏幕中，词语 **PASSTHRU** （大写）必须显示在第一行，从第二列开始。欲发送至移动数据终端的实际数据可从第一行以下的任何位置开始。

通过 5250 或 3274 仿真，属性在屏幕缓冲区占据一个位置。第 2 列和词语“PASSTHRU”末尾之间的属性将随后的所有字符向右“推移”一个位置。因此，需的任何属性均应位于第一行第 1 列（位于词语“PASSTHRU”之前）。

示例：

列：1 2 3 4 5 6 7 8 9
第 1 行：@ P A S S T H R U @
第 2 行：@ P A R T : 1 2 3 4 5

其中@ 是一个属性。

9160 G2 向移动数据终端打印机发送数据完毕后，将向主机发送 *ENTER* 键。主机必须在收到 *ENTER* 键之后才可向此移动数据终端发送更多屏幕（包括其它 PASSTHRU 屏幕）。



注释：有关在移动数据终端上设置 Passthru （直通）参数参数的信息，请参阅相关移动数据终端的用户手册。

Procedures（过程）

此参数启用后，主机可能通过 9160 G2 向移动数据终端发送 TESS 过程。TESS 程序是一组 TESS 命令，可由 TESS 执行过程命令执行此操作。

Local（本地）

此参数启用后，9160 G2 使主机能够提供需要加载的页面，作为移动数据终端中的 TESS 过程。

在移动数据终端的菜单上选择本地过程。移动数据终端可在离线状态下执行这些程序。移动数据终端在线之后，它们将这些功能的结果发送至主机。



注释：同时，*Procedures（过程）* 参数必须启用，*Local（本地）* 才起作用。

Host Print（主机打印）

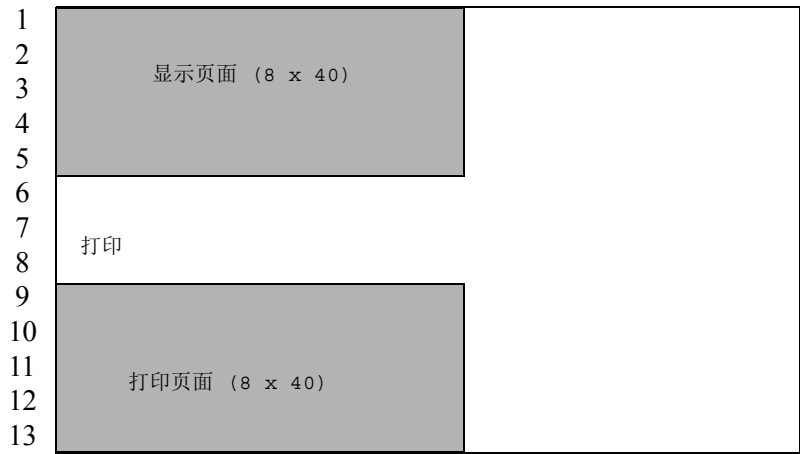
启用此参数后，主机可向移动数据终端发送额外数据，并指示移动数据终端打印该数据。这与 *Local Print（本地打印）* 功能正好相反，在本地打印中，移动数据终端发出初始打印请求。

传递到打印机的文本格式化为 24 x 80 的应用程序屏幕。如果主机可启动打印操作，则可打印文本。若 24 x 80 屏幕第 13 行第 2 列开始处出现词语 “PRINT（打印）”（大写），则 9160 G2 可将额外文本识别为打印页。词语 “PRINT（打印）” 定义为仅显示文本。

打印页面位于移动数据终端显示页面的下方（参见下图）。打印页面的大小通常与移动数据终端显示页面的大小相同（假设在移动数据终端配置中，面长度小于 12 行）。

Host Print（主机打印） 启用时，9160 G2 接收来自主机的应用程序屏幕之后，将打印页面传送至移动数据终端。

图 23.2 包含打印页面的应用程序屏幕



注释:

1. 与 *Passthru*（直通）选项不同，使用 *Host Print*（主机打印）时，不会向打印机发送取消命令。
2. 在打印机发出命令时，必须在移动数据终端的 *TESS* 功能菜单下启用打印支持；有关详细信息，请参阅相关的移动数据终端用户手册。

Remote Print（远程打印）

此参数启用后，在移动数据终端发出请求时（通过从移动数据终端发送“F17”功能键，或从旧移动数据终端发送“PRINT（打印）”键），9160 G2 可将打印页面发至移动数据终端。9160 G2 将功能响应发送回主机。

这与 *Host Print*（主机打印）相反，主机打印通过主机发出初始打印请求。



注释: 移动数据终端必须启用打印支持。有关详细信息，请参阅相关移动数据终端用户手册。

Pages（页数）

此参数可确定存储在移动数据终端上的主机屏幕（或页面）的数量，最多为 **79**。

移动数据终端能够存储其显示的每个屏幕的数据页面，从而 9160 G2 可减少传输至移动数据终端的数据。9160 G2 可保留储存在移动数据终端中每个页面图像。收到应用程序屏幕之后，9160 G2 尝试匹配屏幕与存储的页面。如果移动数据终端的内存中已经存在类似页面，9160 G2 将指示移动数据终端重新示页面的副本；控制器只发送必要的更改。如果未发现匹配的内容，将通过无线链路将整个页面发送至移动数据终端。



注释：若移动数据终端上有相应的参数，已保存页面的**实际**数量将为两个值中的**较小者**。

Transmit Line（传输线路）

此功能启用后，操作员将数据输入到 *transmit-upon-entry*（输入时传输）字段时，将自动传输移动数据终端上所有修改的数据。

本文本框中的值将指定屏幕上哪一行被指定为传输行。屏幕上，传输行上方或传输行上的最后一个输入字段将被确定为 *transmit-upon-entry*（输入时传输）字段。传输行下方行中的任何输入字段均不可指定为 *transmit-upon-entry*（输入时传输）字段。

值为 **0**（零）时将禁止此功能。值为 **24** 时，每个应用程序屏幕上的最后一个输入字段将被指定为 *transmit-upon-entry*（输入时传输）。

AIAG

此参数可为条码读取器输入的内容提供自动查找和填充功能。将条码数据输入移动数据终端之后，移动数据终端将在当前页面搜索可接受条码数据的“AIAG”字段。通过应用程序预装到“AIAG”字段的数据可确定条码数据是否被接受。

在 9160 G2 微型控制器中，ASCII 字符的十进制值（**0** 到 **255**）设置为与主机上的“AIAG Field Identifier”（AIAG 字段标识符）的设置匹配。值为 **0**（零）时将禁用此功能。

预装数据的格式如下所示：

<模式> <AIAG 前缀（数据）>

该命令使用的模式字符允许不同的操作模式，以适应各种应用程序操作。自动查找和填充操作仅适用于从条码读取器接收的数据。模式和 AIAG 前缀的描述如第 260 页的表 23.1 所列。这些模式在主机中设置。

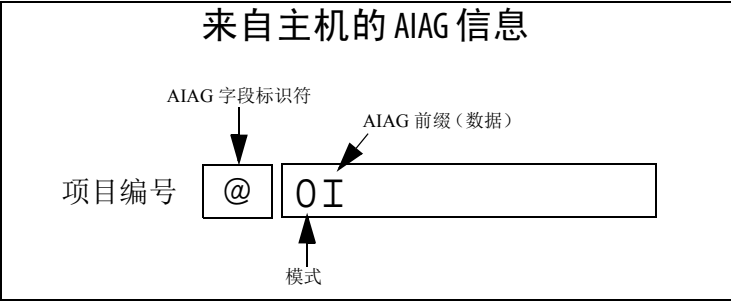
表 23.1 模式功能及 AIAG 前缀描述

模式	功能
0	显示前缀，发送前缀至主机。
1	不显示前缀，发送前缀至主机。
2	显示前缀，不发送前缀至主机。
3	不显示前缀，不发送前缀至主机。
+4	所有 AIAG 字段在填充 4 组时，上述值加 4 将导致传送至主机。如果有任何字段采用此位组，且使用操作员输入的内容填充此位组的所有字段，则“按下”功能 0。
+8	上述值加 8 可重写先前输入的数据。
+16	上述值加 16 表示搜索和填充的光标位置优先级。
AIAG 前缀 (数据)	AIAG 字段中需要匹配的文本。

示例：

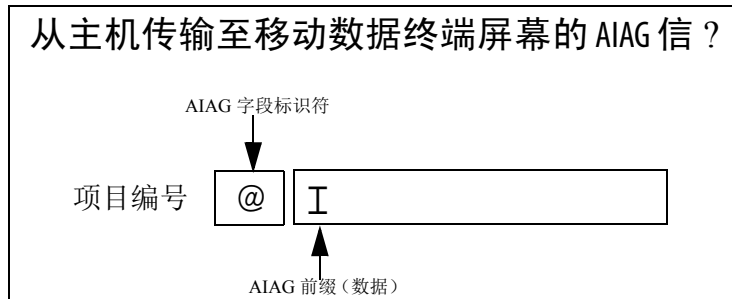
以下示例屏幕中的信息可在主机定义并主机发送。其中包括 “AIAG Identifier”（AIAG 标识符） - 将此标识为 AIAG 字段的标签 - 随后是模式（在此示例中模式为 0）和 “AIAG 前缀” - I。

图 23.3 从主机发送的 AIAG 字段



信息达到移动数据终端屏幕之后，可使用 “AIAG Identifier”（AIAG 标识符）为扫描的信息查找相应的 AIAG 字段。由于在主机设置了模式 0，移动数据终端屏幕上显示 “AIAG Prefix”（AIAG 前缀） - I；屏幕完成操作之后，前缀将发送回主机。

图 23.4 发送至移动数据终端的 AIAG 字段



Visible Match Character （可见匹配字符）

在输入字段前面直接插入专用 ASCII 字符，应用程序可区分输入字段中的“匹配字段”。例如，假设可见匹配字段定义为尖括号“>”。

在输入字段前面插入“>”将其标识为匹配字段，如下图所示。

部件号> _____

该参数的范围（0 到 255）代表 ASCII 字符的十进制值。值为 0（零）时将禁用此功能。在 9160 G2 中输入的 ASCII 十进制值必须与应用程序设置的值一致。

要使用 *Visible Match*（可见匹配）功能，主机将数据预装到匹配输入字段，该数据将显示在移动数据终端屏幕上。发送至移动数据终端的预装数据可包括精确字符和特殊匹配字符，或两者的组合。有关 Psion Teklogix 移动数据终端识别的匹配字符，请参阅表 23.2。

如果条目与预装数据不匹配，将显示条目。同时，移动数据终端将发出蜂鸣音，且光标移至匹配字段的第一个位置。操作员可在匹配字段创建另一个目或将光标移到新的字段。在匹配字段创建条目（即使是不匹配预装数据的条目）之后，该条目将在下一次传输过程中作为部分移动数据终端修改据发送至主机。

表 23.2 匹配字符

字符	描述
#	匹配一个数字。
&	匹配一个字母（不区分大小写）。
^	匹配一个大写字母。
_	匹配一个小写字母。
	匹配一个字母数字字符。
"	匹配一个字母、数字或空格。
?	匹配一个标点字符。
'	匹配任何字符。
:	将字段中的所有字符位置与前面的字符匹配。
;	将所有剩余字符（不一定为字段的剩余字符）与前面的字符匹配。

示例：
假设您想要使用部件号预加载输入字段。如果部件号已知，您可使用此部件号预加载字段。如果需要更多灵活性，部件号由两个字母数字字符，以及字符和四位数字构成，即字段的匹配字符串为 **&& - ####**。

Hidden Match Character（隐藏匹配字符）

与“可见匹配”字段中的数据不同，“隐藏匹配”字段中的预装数据不显示在移动数据终端中。



注释：有关字段匹配的详细信息，请参阅第 261 页的“Visible Match Character（可见匹配字符）”。

该参数的范围（**0** 到 **255**）代表 ASCII 字符的十进制值。值为 **0**（零）时将禁用此功能。在 9160 G2 中输入的 ASCII 十进制值必须与应用程序设置的值一致。

Serial I/O （串口 I/O）

Serial I/O （串口 I/O）字段为特殊输入和固定字段，可接受串行端口输入并可输出至串行端口。通过在字段前面加一个特殊字符，应用程序即可将此字段识别为 *Serial I/O* （串口 I/O）。

如果此字符位于固定字段之前，数据将发送至移动数据终端的串行端口。如果此字符位于输入字段之前，字段将接受来自移动数据终端串行端口的数。

该参数的范围（**0** 到 **255**）代表 ASCII 字符的十进制值。值为 **0** （零）时将禁止此功能。

Print Line （打印行）

您可使用此参数在应用程序屏幕中输入打印页面的起始行编号（另请参见 *Entry Line* （输入行））。值最大为 **24**，可打印此显示页面；值为 **0** （零）时将禁用此功能。

Print Form Length （打印表单长度）

使用此参数可设置打印机的表单长度，以行为单位。范围为 **0** 到 **24**。

Barcode （条码）

Barcode-input-only （仅条码输入）字段为特殊输入字段，仅接受来自条码读取器的输入。通过在字段前面加一个特殊字符，应用程序即可将输入字段识别为 *barcode-input-only* （仅条码输入）。

该参数的范围（**0** 到 **255**）代表 ASCII 字符的十进制值。值为 **0** （零）时将禁止此功能。

Entry Line （输入行）

如果屏幕左上角部分没有输入字段，或输入字段位于此行或下方的行，则此参数包含显示的第一行编号。

使用 *Entry Line* （输入行）参数可在主机屏幕内自动偏移，以便移动数据终端显示的区域可包含通常超出边界的输入字段。一些 Psion Teklogix 移动数据终端显示屏尺较小，因此仅显示应用程序屏幕的左上角。

Field Overhead （字段开销）

此参数包含两个固定字段之间允许的最大字符数目，9160 G2 仍可以将这两个字段合并为一个字段。

有时，9160 G2 可合并两个相邻的固定字段，然后将其作为一个字段发送。这样可以减少无线链路的开销。

例如，两个字段为分开的 4 个字符，此参数为 “5”，则这两个字段可合并为一个字段。

Command Region （命令区域）

此参数定义了主机屏幕中 9160 G2 检查该是否存在保留命令的区域。

Command Region （命令区域）文本框中的四个数字表示命令区域左上角和右下角的行地址和列地址。每一对的第一个文本框包含行数；第二个文本框包含列数。行值的范为 **0** 到 **24**；列值的范围为 **0** 到 **80**。

例如，如需将主机屏幕的最后两行定义为命令区域，可输入值 23, 1 和 24, 80。

目前，仅支持 *ALARM* （警报）命令（有关此命令的详细信息，请参阅第 255 页）。一旦命令区域中的任何位置出现词语 “ALARM” （警报），9160 G2 将向移动数据终端发送 TESS 蜂鸣声。

23.4.1.3 Telnet Protocol Options （Telnet 协议选项）

Telnet Protocol Options:

Terminal Type:

IBM-3278-2

Host Port:

23

(Range 1..32767)

Maximum Sessions per Terminal:

4

(Range 1..127)

First Local Terminal Port:

10000

(Range 1..32767)

Local IP Address to Bind:

0.0.0.0

First Terminal Listen Port:

0

(Range 0..32767)

Actively Negotiate with Host:

☐

Configure LU Names:

☐

Configure

LU Name Prefix:

Send IAC Interrupt Process as a System Request:

☐

Send IAC Break as an Attention Key:

☐

Auto-telnet:

DISABLE

Auto-telnet Host:

Auto-telnet without User Action:

☒

Terminal Type （终端类型）

您可使用此参数选择该主机 9160 G2 模拟的移动数据终端的类型。目前，可用于 3274 Emulation （3274 仿真）的移动数据终端包括 **IBM 3278-2** 和 **IBM 3278-2-E**。

Host Port （主机端口）

您可使用此参数输入选定 3274 Emulation （3274 仿真）主机连接的主机端口值。默认值为 **23**。

Maximum Sessions per Terminal （每个终端的最大会话数量）

此参数即每台移动数据终端可发起 Telnet 会话的最大数量。范围为 **1** 到 **127**，默认值为 **4**。

First Local Terminal Port （第一个本地终端端口）

此参数指在出站 Telnet 会话中第一台移动数据终端连接的本地端口号。默认值为 **10000**。

Local IP Address to Bind （要绑定的本地 IP 地址）

此参数指在进行出站 Telnet 会话时第一台移动数据终端连接的 9160 G2 中的网络适配器的 IP 地址。

First Terminal Listen Port （第一个终端监听端口）

此参数指定了 9160 G2 用于监听 Telnet 连接移动数据终端请求的第一个端口号。要启用此参数，该值至少为 **1024**。要禁用此监听端口，该值必须为 **0**。

默认值为 **0**（禁用）。

Actively Negotiate with Host （主动与主机协商）

启用此参数后，9160 G2 开始在 Telnet 连接设置期间与主机协商。不建议用于大部分主机。

Configure LU Names （配置 LU 名称）

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

<input type="checkbox"/>	Edit	Terminal Number	LU Name
<input type="checkbox"/>	[Edit]	1	ABC
<input type="checkbox"/>	[Edit]	5	THING

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

每个配置的移动数据终端需要一个 LU 名称。您可使用此页面分配 LU 名称（另请参阅下文的 *LU Name Prefix*（LU 名称前缀）。LU 名称必须是唯一的，且与移动数据终端的终端号相关联。LU 名称可包含最多 10 个字母数字字符；输入时，小写字符转换为大写符。

LU Name Prefix（LU 名称前缀）

如果未指定移动数据终端的 LU 名称，9160 G2 将向 LU 前缀附加终端号（如果需要，采用前导零构成五位数）来创建完整的 LU 名称。

Send IAC Interrupt Process as a System Request（将 IAC 中断进程作为系统请求发送）

启用此参数后，9160 G2 将 IAC 中断进程作为 3274 系统请求向主机发送。

Send IAC Break as an Attention Key（将 IAC 中断作为注意键发送）

启用此参数后，9160 G2 将 IAC 中断请求作为 3274 注意键向主机发送。

Auto-telnet（自动 telnet）

您可使用此参数禁用或启用移动数据终端与本主机之间的 Telnet 会话自动连接。

可提供以下两种选择：**Disable**（禁用）和 **Auto-Telnet**（自动 Telnet）。默认值为 **Disable**（禁用）。

Auto-Telnet（自动 Telnet）设为 **Disable**（禁用）时，必须从移动数据终端手动启动移动数据终端与主机之间的 Telnet 会话。

启用 *Auto-Telnet*（自动 Telnet）后，9160 G2 将在终端号映射到该主机上的每个移动数据终端启动 Telnet 会话。在移动数据终端和主机之间可启动其它 Telnet 会话，但是必须手动启动。

启用 *Auto-Telnet*（自动 Telnet）后，9160 G2 将在启动时和关闭 Telnet 会话时自动建立与主机的 Telnet 会话。



注释：只有“在线”（在 Psion Teklogix RF 网络上打开并正确操作）的移动数据终端才可启动 *Auto-Telnet*（自动 Telnet）会话。

Auto-telnet Host（自动 Telnet 主机）

此参数包含主机的主机名称或 IP 地址，以便主机与 9160 G2 连接 *Auto-Telnet*（自动 Telnet）会话。



注释：此文本框中的主机名称必须可通过 9160 G2 解析：9160 G2 必须能够获取其 IP 地址。例如，主机名称可能对应 9160 G2 主机列表中的条目，或者 9160 G2 能够询域名服务器。
任何可用于移动数据终端 TCP> 提示的主机名称均可应用于此。

Auto-telnet Without User Action （在用户不操作的情况下自动 Telnet）

若启用此项，控制器将立即打开每台初始化的移动数据终端到主机的连接，无需用户按 [ENTER] 键。

23.4.1.4 Function Key Mappings （功能键映射）

Function Key Mappings:


F1:	F1	F14:	PA2	F27:	F13
F2:	F2	F15:	PA3	F28:	F14
F3:	F3	F16:	CLEAR	F29:	F15
F4:	F4	F17:	F17	F30:	SESS
F5:	F5	F18:	F18	F31:	F16
F6:	F6	F19:	F19	F32:	ENTER
F7:	F7	F20:	F20	F33:	ENTER
F8:	F8	F21:	F21	F34:	ENTER
F9:	F9	F22:	F22	F35:	ENTER
F10:	F10	F23:	F23	F36:	ENTER
F11:	F11	F24:	F24	F37:	ENTER
F12:	F12	F25:	SYSREQ	F38:	ENTER
F13:	PA1	F26:	ATTN	F39:	ENTER

功能键

Function Key （功能键）参数允许您选择一个代码，当您在移动数据终端上按下功能键时即可将代码发送到主机。每个功能键可选自同一代码范围，但是每个功能键的默认代码不同。默认值如本页所示。

23.4.2 5250 仿真

23.4.2.1 Emulation Options （仿真选项）



5250 Emulation Options:

Write Error Code: Advisory text ▼

Use International EBCDIC: ☐

Allow null character in fixed fields: ☐

通过 IBM 5250 或 IBM 3274 仿真，9160 G2 微型控制器可将来自主机的应用数据流转换为 TESS（Teklogix 屏幕子系统）命令。本页的一些参数可控制主机屏幕向 TESS 的转换。

Write Error Code （写入错误代码）

如果选择此处的 *advisory text*（咨询文本），9160 G2 将向移动数据终端发送错误代码，作为咨询文本写入屏幕底部。如果选择 *screen text*（屏幕文本），9160 G2 会将错误代码作为常规屏幕文本发送。

Use International EBCDIC （使用国际 EBCDIC）

此参数设为 **Enabled**（启用）后，9160 G2 将交换 EBCDIC 字符表中的 **!** 和 **]** 字符的位置。

Allow null character in fixed fields （固定字段可存在 Null 字符）

此参数设为 **Enabled**（启用）后，对于拥有视觉视频属性（例如反相显示）的字段，9160 G2 微型控制器允许其空格处出现 Null 字符。5250 主机仿真的默认值为启用。

23.4.2.2 TESS Options （TESS 选项）

TESS Options:

Field Underline Remapping:	None
Alarm:	<input type="checkbox"/>
Clear:	<input type="checkbox"/>
Passthru:	<input type="checkbox"/>
Procedures:	<input type="checkbox"/>
Local:	<input type="checkbox"/>
Host Print:	<input type="checkbox"/>
Remote Print:	<input type="checkbox"/>
Pages:	8 (Range 1..79)
Transmit Line:	0 (Range 0..24)
AIAG:	0 (Range 0..255)
Visible Match Character:	0 (Range 0..255)
Hidden Match character:	0 (Range 0..255)
Serial I/O:	0 (Range 0..255)
Print Line:	0 (Range 0..24)
Print Form Length:	0 (Range 0..24)
Barcode:	0 (Range 0..255)
Entry Line:	0 (Range 0..24)
Field Overhead:	5 (Range 0..80)
Command Region:	0, 0, 0, 0

Field Underline Remapping （字段下划线重新映射）

您可选择更改所显示字符的视频属性，来突出显示输入字段。选项包括 *None*（无）、*Blink*（闪烁）、*Bold*（粗体）和 *Reverse*（反相）。

Alarm （警报）

此参数启用后，如果 *Command Region*（命令区域）参数规定位置的应用程序屏幕上出现词语“ALARM（警报）”（大写），移动数据终端将发出蜂鸣声（请参见第 279 页）。词语“ALARM（警报）”应为仅供显示字段。



注释：必须启用 *Command Region*（命令区域）参数之后，此参数才生效。

Clear （清除）

此参数启用后，9160 G2 微型控制器将为填充为空格的输入字段创建一个空条目字段。

一些主机应用程序依赖显示字符的视频属性突出显示字段，对输入字段尤其如此。例如，应用程序屏幕可能使用反相显示定义所有字段并使用空格填充字段。这对支持反相显示的移动数据终端有效。但是，对于不支持反相显示的移动数据终端，由于字段完全由空格组成，因此导致字段不可见。

默认情况下，显示在 Psion Teklogix 移动数据终端的所有空输入字段可通过在移动数据终端配置中选择的“输入字符”实现突出显示。*Clear*（清除）功能可在含有空格的输入字段处创建空输入字段。



注释：只对从主机接收的屏幕执行此操作。发送至主机的数据不受影响。

Passthru （直通）

此参数启用后，9160 G2 使主机能够直接向 RF 移动数据终端的串行端口发送数据。最常用于打印。

准备用于传递的主机屏幕

在将要通过移动数据终端端口发送的屏幕上，词语 **PASSTHRU**（大写）必须显示在第一行，从第二列开始。欲发送至移动数据终端的实际数据可从第一行以下的任何位置开始。

通过 5250 或 3274 仿真，属性在屏幕缓冲区占据一个位置。第 2 列和词语“PASSTHRU”末尾之间的属性将随后的所有字符向右推移一个位置。因此，所需任何属性均应位于第一行第 1 列（位于词语“PASSTHRU”之前）。

示例：

```
列： 1 2 3 4 5 6 7 8 9
第 1 行： @ P A S S T H R U @
第 2 行： @ P A R T : 1 2 3 4 5
```

其中 @ 是一个属性。

9160 G2 向移动数据终端打印机发送数据完毕后，将向主机发送 ENTER 键。主机必须在收到 ENTER 键之后才可此移动数据终端发送更多屏幕（包括其它 PASSTHRU 屏幕）。



注释：有关在移动数据终端上设置 Passthru（直通）参数的信息，请参阅相关移动数据终端的用户手册。

Procedures （过程）

此参数启用后，主机可能通过 9160 G2 向移动数据终端发送 TESS 过程。TESS 程序是一组 TESS 命令，可由 TESS 执行过程命令执行此操作。

Local （本地）

此参数启用后，9160 G2 使主机能够提供需要加载的页面，作为移动数据终端中的 TESS 过程。

在移动数据终端的菜单上选择本地过程。移动数据终端可在离线状态下执行这些程序。移动数据终端在线之后，它们将这些功能的结果发送至主机。



注释：同时，Procedures （程序）参数必须启用，Local （本地）才起作用。

Host Print （主机打印）

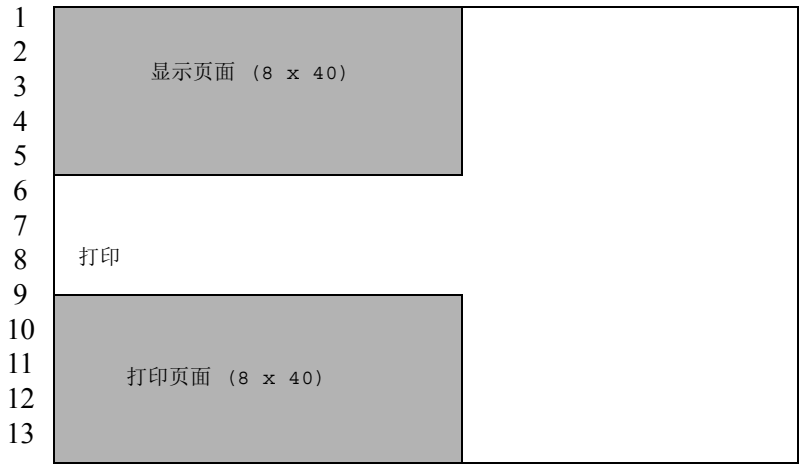
启用此参数后，主机可向移动数据终端发送额外数据，并指示移动数据终端打印该数据。这与 Local Print （本地打印）功能正好相反，在本地打印中，移动数据终端发出初始打印请求。

传递到打印机的文本格式化为 24 x 80 的应用程序屏幕。如果主机可启动打印操作，则可打印文本。若 24 x 80 屏幕第 13 行第 2 列开始处出现词语 “PRINT （打印）”（大写），则 9160 G2 可将额外文本识别为打印页。词语 “PRINT （打印）” 定义为仅显示文本。

打印页面位于移动数据终端显示页面的下方（参见第 273 页的图 23.5）。打印页面的大小通常与移动数据终端显示页面的大小相同（假设在移动数据终端配置中，页面长度小于 12 行）。

Host Print （主机打印）启用时，9160 G2 接收来自主机的应用程序屏幕之后，将打印页面传送至移动数据终端。

图 23.5 包含打印页面的应用程序屏幕



注释:

1. 与 *Passthru*（直通）选项不同，使用 *Host Print*（主机打印）时，不会向打印机发送取消命令。
2. 在打印机发出命令时，必须在移动数据终端的 *TESS* 功能菜单下启用打印支持；有关详细信息，请参阅相关的移动数据终端用户手册。

Remote Print（远程打印）

此参数启用后，在移动数据终端发出请求时（通过从移动数据终端发送“F17”功能键，或从旧移动数据终端发送“PRINT（打印）”键），9160 G2 可将打印页面发至移动数据终端。9160 G2 将功能响应发送回主机。

这与 *Host Print*（主机打印）相反，主机打印通过主机发出初始打印请求。



注释: 在移动数据终端必须启用打印支持。有关详细信息，请参阅相关移动数据终端用户手册。

Pages（页数）

此参数可确定存储在移动数据终端上的主机屏幕（或页面）的数量，最多为 **79**。移动数据终端能够存储其显示的每个屏幕的数据页面，从而 9160 G2 可减少传输至移动数据终端的数据。9160 G2 可保留储存在移动数据终端中每个页面图像。收到应用程序屏幕之后，9160 G2 尝试匹配屏幕与存储的页面。

如果移动数据终端的内存中已经存在类似页面，9160 G2 将指示移动数据终端重新显示页面的副本；控制器只发送必要的更改。如果未发现匹配的内容将通过无线链路将整个页面发送至移动数据终端。



注释：若移动数据终端上有相应的参数，已保存页面的**实际**数量将为两个值中的**较小者**。

Transmit Line （传输线路）

此功能启用后，操作员将数据输入到 *transmit-upon-entry* （输入时传输）字段时，将自动传输移动数据终端上所有修改的数据。

本文本框中的值将指定屏幕上哪一行被指定为 *传输行*。屏幕上，传输行上方或传输行上的最后一个输入字段将被确定为 *transmit-upon-entry* （输入时传输）字段。传输行下方行中的任何输入字段均不可指定为 *transmit-upon-entry* （输入时传输）字段。

值为 **0** （零）时将禁用此功能。值为 **24** 时，将使每个应用程序屏幕上的 *最后一个* 输入字段指定为 *transmit-upon-entry* （输入时传输）。

AIAG

此参数可为条码读取器输入的内容提供自动查找和填充功能。将条码数据输入移动数据终端之后，移动数据终端将在当前页面搜索可接受条码数据的 “AIAG” 字段。通过应用程序预装到 “AIAG” 字段的数据可确定条码数据是否被接受。在 9160 G2 微型控制器中，ASCII 字符的十进制值（**0** 到 **127**）设置为与主机上的 “AIAG Field Identifier” （AIAG 字段标识符）的设置匹配。值为 **0** （零）时将禁止此功能。

预装数据的格式如下所示：

<模式> <AIAG 前缀（数据）>

该命令使用的模式字符允许不同的操作模式，以适应各种应用程序操作。自动查找和填充操作仅适用于从条码读取器接收的数据。模式和 AIAG 前缀的述如下表所列。这些模式在主机中设置。

表 23.3 模式功能及 AIAG 前缀描述

模式	功能
0	显示前缀，发送前缀至主机。
1	不显示前缀，发送前缀至主机。
2	显示前缀，不发送前缀至主机。

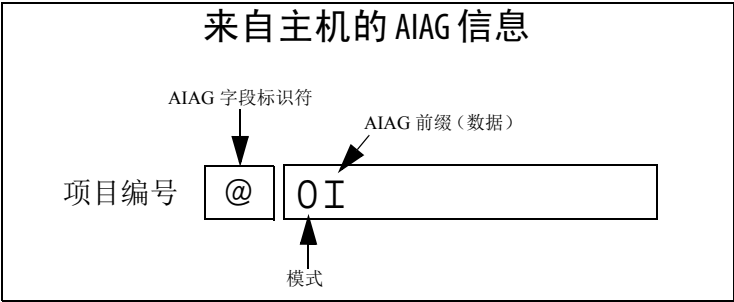
表 23.3 模式功能及 AIAG 前缀描述

模式	功能
3	不显示前缀，不发送前缀至主机。
+4	所有 AIAG 字段在填充 4 组时，上述值加 4 将导致传送至主机。如果有任何字段采用此位组，且使用操作员输入的内容填充此位组的所有字段，则“按下”功能 0。
+8	上述值加 8 可重写先前输入的数据。
+16	上述值加 16 表示搜索和填充的光标位置优先级。
AIAG 前缀 (数据)	AIAG 字段中需要匹配的文本。

示例：

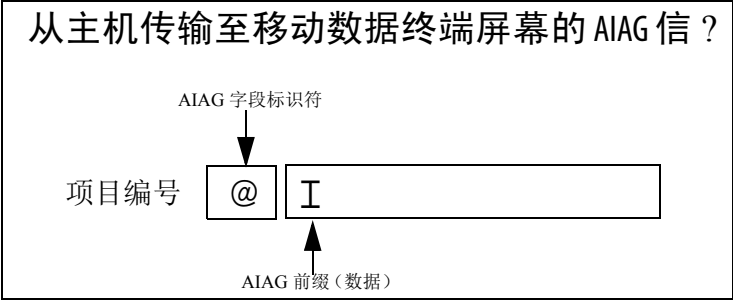
以下示例屏幕中的信息可在主机定义并 从主机发送。其中包括“AIAG Identifier”（AIAG 标识符）- 将此标识为 AIAG 字段的标签 - 随后是模式（在此示例中模式为 0）和“AIAG 前缀”- I。

图 23.6 从主机发送的 AIAG 字段



信息达到移动数据终端屏幕之后，可使用“AIAG Identifier”（AIAG 标识符）为扫描的信息查找相应的 AIAG 字段。由于在主机设置了模式 0，移动数据终端屏幕上显示“AIAG Prefix”（AIAG 前缀）- I；屏幕完成操作之后，前缀将发送回主机。

图 23.7 发送至移动数据终端的 AIAG 字段



Visible Match Character （可见匹配字符）

在输入字段前面直接插入专用 ASCII 字符，应用程序可区分输入字段中的“匹配字段”。例如，假设可见匹配字段定义为尖括号“>”。在输入字段前面插入“>”将其标识为匹配字段，如下图所示。

部件号> _____

该参数的范围（0 到 255）代表 ASCII 字符的十进制值。值为 0（零）时将禁用此功能。在 9160 G2 中输入的 ASCII 十进制值必须与应用程序设置的值一致。

要使用 *Visible Match*（可见匹配）功能，主机将数据预装到匹配输入字段，该数据将显示在移动数据终端屏幕上。发送至移动数据终端的预装数据可包括精确字符和特殊匹配字符，或两者的组合。有关 Psion Teklogix 移动数据终端识别的匹配字符，请参阅下表。

如果条目与预装数据不匹配，将显示条目。同时，移动数据终端将发出蜂鸣音，且光标移至匹配字段的第一个位置。操作员可在匹配字段创建另一个目或将光标移到新的字段。在匹配字段创建条目（即使是不匹配预装数据的条目）之后，该条目将在下一次传输过程中作为部分移动数据终端修改据发送至主机。

表 23.4 匹配字符

字符	描述
#	匹配一个数字。
&	匹配一个字母（不区分大小写）。
^	匹配一个大写字母。
_	匹配一个小写字母。

表 23.4 匹配字符 （续）

字符	描述
	匹配一个字母数字字符。
"	匹配一个字母、数字或空格。
?	匹配一个标点字符。
'	匹配任何字符。
:	将字段中的所有字符位置与前面的字符匹配。
;	将所有剩余字符 （不一定为字段的剩余字符）与前面的字符匹配。

示例:

假设您想要使用部件号预加载输入字段。如果部件号已知，您可使用此部件号预加载字段。如果需要更多灵活性，部件号由两个字母数字字符，以及字符和四位数字构成，即字段的匹配字符串为 `&& - ####`。

Hidden Match Character （隐藏匹配字符）

与“可见匹配”字段中的数据不同，“隐藏匹配”字段中的预装数据不显示在移动数据终端中。



注释: 有关字段匹配的详细信息，请参阅第 276 页的“Visible Match Character （可见匹配字符）”。

该参数的范围（**0** 到 **255**）代表 ASCII 字符的十进制值。值为 **0**（零）时将禁用此功能。在 9160 G2 中输入的 ASCII 十进制值必须与应用程序设置的值一致。

Serial I/O （串口 I/O）

Serial I/O（串口 I/O）字段为特殊输入和固定字段，可接受串行端口输入并可输出至串行端口。通过在字段前面加一个特殊字符，应用程序即可将此字段识别 *Serial I/O*（串口 I/O）。

如果此字符位于固定字段之前，数据将发送至移动数据终端的串行端口。如果此字符位于输入字段之前，字段将接受来自移动数据终端串行端口的数。

该参数的范围（**0** 到 **255**）代表 ASCII 字符的十进制值。值为 **0**（零）时将禁用此功能。

Print Line （打印行）

您可使用此参数在应用程序屏幕中输入打印页面的起始行编号（另请参见 *Entry Line*（输入行））。值最大为 **24**，可打印此显示页面；值为 **0**（零）时将禁用此功能。

Print Form Length （打印表单长度）

使用此参数可设置打印机的表单长度，以行为单位。范围为 **0** 到 **24**。

Barcode （条码）

Barcode-input-only（仅条码输入）字段为特殊输入字段，仅接受来自条码读取器的输入。通过在字段前面加一个特殊字符，应用程序即可将输入字段识别为 *barcode-input-only*（仅条码输入）。

该参数的范围（**0** 到 **255**）代表 ASCII 字符的十进制值。值为 **0**（零）时将禁用此功能。

Entry Line （输入行）

如果屏幕左上角部分没有输入字段，或输入字段位于此行或下方的行，则此参数包含显示的第一行编号。

使用 *Entry Line*（输入行）参数可在主机屏幕内自动偏移，以便移动数据终端显示的区域可包含通常超出边界的输入字段。一些 Psion Teklogix 移动数据终端显示屏尺较小，因此仅显示应用程序屏幕的左上角。

Field Overhead （字段开销）

此参数包含两个固定字段之间允许的最大字符数目，9160 G2 仍可以将这两个字段合并为一个字段。

有时，9160 G2 可合并两个相邻的固定字段，然后将其作为一个字段发送。这样可以减少无线链路的开销。

例如，两个字段为分开的 4 个字符，此参数为“5”，则这两个字段可合并为一个字段。

Command Region （命令区域）

此参数定义了主机屏幕中 9160 G2 检查该是否存在保留命令的区域。

Command Region （命令区域）文本框中的四个数字表示命令区域左上角和右下角的行地址和列地址。每一对的第一个文本框包含行数；第二个文本框包含列数。行值的范为 **0** 到 **24**；列值的范围为 **0** 到 **80**。

例如，如需将主机屏幕的最后两行定义为命令区域，可输入值 *23, 1* 和 *24, 80*。

目前，仅支持 *ALARM* （警报）命令（有关此命令的详细信息，请参阅第 270 页）。一旦命令区域中的任何位置出现词语 “ALARM” （警报），9160 G2 将向移动数据终端发送 TESS 蜂鸣声。

23.4.2.3 Telnet Protocol Options （Telnet 协议选项）

Telnet Protocol Options:

Terminal Type:

IBM-5251-11

Host Port:

23

(Range 1..32767)

Maximum Sessions per Terminal:

4

(Range 1..127)

First Local Terminal Port:

10000

(Range 1..32767)

Local IP Address to Bind:

0.0.0.0

First Terminal Listen Port:

0

(Range 0..32767)

Actively Negotiate with Host:

Auto-telnet:

DISABLE

Auto-telnet Host:

Auto-telnet without User Action:

Enable Virtual Device Names:

- Configure Device Names:

Configure

- Device Name Prefix:

Terminal Type （终端类型）

您可使用此参数选择该主机 9160 G2 模拟的移动数据终端的类型。目前，可用于 *5250 Emulation* （5250 仿真）的移动数据终端包括：**IBM 5251-11**、**IBM 5555-B01** 和 **IBM 3179-2**。

Host Port （主机端口）

您可使用此参数输入选定 *5250 Emulation* （5250 仿真）主机连接的主机端口值。默认值为 **23**。

Maximum Sessions per Terminal （每个终端的最大会话数量）

此参数即每台移动数据终端可发起 Telnet 会话的最大数量。范围为 **1** 到 **127**，默认值为 **4**。

First Local Terminal Port （第一个本地终端端口）

此参数指在出站 Telnet 会话中第一台移动数据终端连接的本地端口号。默认值为 **10000**。

Local IP Address to Bind （要绑定的本地 IP 地址）

此参数指在进行出站 Telnet 会话时第一台移动数据终端连接的网络适配器的 IP 地址。

First Terminal Listen Port （第一个终端监听端口）

此参数指定了 9160 G2 用于监听 Telnet 连接移动数据终端请求的第一个端口号。要将此参数设为 **Enabled** （启用），该值至少为 **1024**。要将此监听端口设为 **Disabled** （禁用），该值必须为 **0**。

默认值为 **0** （禁用）。

Actively Negotiate with Host （主动与主机协商）

启用此参数后，9160 G2 开始在 Telnet 连接设置期间与主机协商。不建议用于大部分主机。

Auto-telnet （自动 telnet）

您可使用此参数禁用或启用移动数据终端与本主机之间的 Telnet 会话自动连接。

可提供以下两种选择：**Disable** （禁用）和 **Auto-Telnet** （自动 Telnet）。默认值为 **Disable** （禁用）。

Auto-Telnet （自动 Telnet）设为 **Disabled** （禁用）时，必须从移动数据终端手动启动移动数据终端与主机之间的 Telnet 会话。

启用 *Auto-Telnet* （自动 Telnet）后，9160 G2 将在终端号映射到该主机上的每个移动数据终端启动 Telnet 会话。在移动数据终端和主机之间可启动其它 Telnet 会话，但是必须手动启动。

启用 *Auto-Telnet*（自动 Telnet）后，9160 G2 将在启动时和关闭 Telnet 会话时自动建立与主机的 Telnet 会话。



注释：只有“在线”（在 Psion Teklogix RF 网络上打开并正确操作）的移动数据终端才可启动 *Auto-Telnet*（自动 Telnet）会话。

Auto-telnet Host（自动 Telnet 主机）

此参数包含主机的主机名称或 IP 地址，以便主机与 9160 G2 连接 *Auto-Telnet*（自动 Telnet）会话。



注释：此文本框中的主机名称必须可通过 9160 G2 解析：9160 G2 必须能够获取其 IP 地址。例如，主机名称可能对应 9160 G2 主机列表中的条目，或者 9160 G2 能够询域名服务器。任何可用于移动数据终端 TCP> 提示的主机名称均可应用于此。

Auto-telnet Without User Action（在用户不操作的情况下自动 Telnet）

若启用此项，控制器将立即打开每台初始化的移动数据终端到主机的连接，无需用户按 [ENTER] 键。

Enable Virtual Device Names（启用虚拟设备名称）

启用此参数后，9160 G2 与主机协商获取虚拟设备名称，用于 Telnet 连接。

Configure Device Names （配置设备名称）

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

<input type="checkbox"/> Edit	Terminal Number	LU Name
<input type="checkbox"/> [Edit]	1	ABC
<input type="checkbox"/> [Edit]	5	THING

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

每个配置的移动数据终端需要一个 LU 名称。您可使用此页面分配 LU 名称（另请参阅下文的 *Device Name Prefix*（设备名称前缀））。LU 名称必须是唯一的，且与移动数据终端的终端号相关联。LU 名称可包含最多 10 个字母数字字符；输入时，小写字符转换为大写字符。

Device Name Prefix （设备名称前缀）

如果未指定移动数据终端的 LU 名称，9160 G2 将向 LU 前缀附加终端号（如果需要，采用前导零构成五位数）来创建完整的 LU 名称。

23.4.2.4 Function Key Mappings （功能键映射）

Function Key Mappings:

F1:	F1	F14:	F14	F27:	F17
F2:	F2	F15:	F15	F28:	F18
F3:	F3	F16:	CLEAR	F29:	UP
F4:	F4	F17:	PRINT	F30:	SESS
F5:	F5	F18:	HELP	F31:	ENTER
F6:	F6	F19:	F19	F32:	ENTER
F7:	F7	F20:	F20	F33:	ENTER
F8:	F8	F21:	F21	F34:	ENTER
F9:	F9	F22:	F22	F35:	ENTER
F10:	F10	F23:	F23	F36:	ENTER
F11:	F11	F24:	F24	F37:	ENTER
F12:	F12	F25:	DOWN	F38:	SELECTOR
F13:	F13	F26:	F16	F39:	ENTER

Function Key （功能键）

Function Key （功能键）参数允许您选择一个代码，当您在移动数据终端上按下功能键时即可将代码发送到主机。每个功能键可选自同一代码范围，但是每个功能键的默认代码不同。默认值如本页所示。

23.4.3 ANSI 仿真

23.4.3.1 仿真选项

ANSI Emulation Options:

Maximum Screen Size:

24

rows

80

columns

Host Timeout:

15

(Range 0..255)

Escape Timeout:

12

(Range 0..255)

Threshold:

200

(Range 0..999)

Echo:

☒

Function Key Remapping:

☐

Arrow Key Remapping:

☐

Page Saving:

☒

Page Saving consider Double Byte Characters:

☐

RLE:

☐

Convert 7 to 8 bits:

☐

Lower Character Set (GL):

ASCII

Upper Character Set (GR):

ASCII

Terminal Initialization Data:

Host Initialization Data:

Maximum Screen Size （最大屏幕尺寸）

您可使用 *Maximum Screen Size* （最大屏幕尺寸）按照行和列在移动数据终端设置所需的最大屏幕尺寸。此功能可确保使用该页保存选项时内存的优化利用（请参见第 286 页的“Page Saving（页面保存）”）。

范围为 **24 x 80**（最小设置）到 **60 x 132**（最大设置）。默认设置为 **24 x 80**。

Host Timeout （主机超时）

Host Timeout（主机超时）是接受来自主机的大量数据的间隔（以滴答计数，或 1/60 秒）。范围为 **0** 到 **255**，默认值为 **15**。

如果超时过时之后，9160 G2 未收到来自主机的任何字符，则假设主机已经发送数据完毕，正在等待用户输入（换句话说，假设数据屏幕已经完成）。



重要说明: 必须启用 *Page Saving*（页面保存）参数(第 286 页)，才能更改 *Host Timeout*（主机超时）中的值。

Escape Timeout （转义超时）

Escape Timeout （转义超时）是指 9160 G2 保留来自主机的 “ESC” 并将接收的下一字节作为部分转义序列的时长（以滴答声为单位，即 1/60 秒）。范围为 0 到 255，默认值为 12。

超时过后，主机将发送另一个 “ESC” 字符，开始转义序列。



注释：这对 ESC 在数据包末端时尤为重要。

Threshold （阈值）

Threshold （阈值）是移动数据终端屏幕更新数据的最小字节数，必须在 9160 G2 将屏幕存储为新的 “已保存页面” 之前从主机获取该值。范围为 0 到 999，默认值为 200。



重要说明：必须启用 *Page Saving* （页面保存）参数(第 286 页)，才能更改 *Host Threshold* （阈值）中的值。

Echo （回音）

此参数启用后，9160 G2 可使用 “智能” 回音。此模式可通过减少无线传输数量减少发送至移动数据终端的数据量。

通常，如果一个字符模式应用程序正在使用，每个击键将通过一次传输发送至主机，同时主机将通过另一次传输对字符发出回音。“智能” 回音启用后，如果主机回音与移动数据终端发送的数据匹配，则 9160 G2 不向移动数据终端发送主机回音。从而减少了无线传输的数量。

采用这种模式也可减少或避免在键盘输入字符和在主机显示字符之间的时间延迟。等待回音的最大字符数为 25。其它字符将发送至主机，但是不显示。



注释：

1. 此参数还可用于确定 ANSI 参数查询是否发送至移动数据终端。
2. 此外，还需在移动数据终端启用 “Smart” Echo （“智能” 回音）（请参阅相关移动数据终端的用户手册）。

Function Key Remapping （功能键重映射）

此参数启用后，9160 G2 按照 *Function Key Remapping* （功能键重映射）页（第 292 页）中的定义重新映射此主机连接的功能键。

Arrow Key Remapping（箭头键重映射）

此参数启用后，9160 G2 按照 Function Key Remapping（功能键重映射）页（第 292 页）中的定义重新映射此主机连接的箭头键。

Page Saving（页面保存）

此参数启用后，9160 G2 可使用页面保存减少传输至移动数据终端的数据。

9160 G2 可保留储存在移动数据终端中每个页面的图像。收到应用程序屏幕之后，9160 G2 尝试匹配屏幕与存储的页面。如果移动数据终端已经存在该页面，9160 G2 将指示移动数据终端重新显示已存储的页面副本；无需通过无线链路发送该页的数据。若 9160 G2 未找到该页的匹配内容，则将整个页面发送移动数据终端。默认值为启用。



注释： 启用页面保存后，已保存页面的数量将与移动数据终端设置的数量一致。有关详细信息，请参阅相关移动数据终端用户手册。

如果使用双字节字符集（如汉语或韩语），请参阅下文的“页面保存考虑双字节字符”参数。

Page Saving Consider Double Byte Character（页面保存考虑双字节字符）

使用双字节字符集（如韩语或韩语）时，*Page Saving*（页面保存）（详情见上）将允许部分覆盖双字节字符集，这样可产生单字节不可打印的屏幕数据，或由两个不同字符的半个字符构成新的非预期字。此外，移动数据终端可转换屏幕上的数据，以截断不良数据。

启用 *Page Saving Consider Double Byte Character*（页面保存考虑双字节字符）后，*Page Saving*（页面保存）将任何孤立的半个双字节字符替换为一个空格，以防止修改的字符和截断的数据显示在移动数据终端上。默认值为禁用。



注释： 只有使用双字节字符集时才使用本选项。

RLE

此参数启用后，9160 G2 将其通过无线通信链路发送的数据上使用运行长度编码 (RLE)。RLE 压缩从主机发送至移动数据终端的重复字符。如果数据流中发现重复字符，将发送第一个字符，随后发送一个短的转义序列（3 或 4 个字符），通知移动数据终端该字符重复的次数。这样，RLE 可压缩数据，减少无线链路流量的总量。

Convert 7 to 8 Bits （将 7 位转换为 8 位）

此参数设为 **Enabled**（启用）后， 9160 G2 可将发送至移动数据终端的 ANSI 数据流中的 7 位控制序列转换为 8 位等值序列。从而将双字符转义序列替换为单个等效字符，实现压缩数的目的。

Lower Character Set (GL) （小写字符集(GL)）

应与移动数据终端中选用的字符集相同。只有当 Page Saving（页面保存）已启用时才使用此参数。

Upper Character Set (GR) （大写字符集(GR)）

应与移动数据终端中选用的字符集相同。只有当 Page Saving（页面保存）已启用时才使用此参数。

Terminal Initialization Data （终端初始化数据） <1/> / Host Initialization Data （主机初始化数据）

每次重置移动数据终端之后，这些字段可用于输入从控制器发送至移动数据终端/主机的数据。例如，这些字段可用于发出主机刷新的请求，或在主机登录时重置移动数据终端设置的字符集的请求。

不可打印字数据可以十六进制 (\xnn) 或八进制 (\nnn) 形式输入。例如，转义字符可输入为 \x1b 或 \033。

这些参数最长可为 256 个字符。如果字段为空，则不发送数据。

23.4.3.2 Telnet Protocol Options （Telnet 协议选项）

Telnet Protocol Options:

Terminal Type:

VT100

Host Port:

23

(Range 1..32767)

Maximum Sessions per Terminal:

4

(Range 1..127)

Close Host sessions on Terminal reset:

☐

First Local Terminal Port:

10000

(Range 1..32767)

Local IP Address to Bind:

0.0.0.0

First Terminal Listen Port:

0

(Range 0..32767)

TCP Session Request Key:

1

(Range 0..255)

Session Cycle Key:

2

(Range 0..255)

Last Active Session Key:

5

(Range 0..255)

rminal Type （终端类型）

此参数指定了 9160 G2 模拟的移动数据终端的类型。文本框中输入的字符可以为主机接受的任何 ASCII 字符串，**最多为 32 个字符**。默认值为 **VT100**。

Host Port （主机端口）

此参数指定用于选定 ANSI 主机连接的主机端口的值。默认值为 **23**。

Maximum Sessions per Terminal （每个终端的最大会话数量）

此参数即每台移动数据终端可发起 Telnet 会话的最大数量。范围为 **1 到 127**，默认值为 **4**。

Close Host Sessions on Terminal Reset （终端重置时关闭主机会话）

此参数设为 **Engabled**（启用）后，将收到终端重置消息，该终端号的主机会话将关闭。默认值为 **Disabled**（禁用）。

First Local Terminal Port （第一个本地终端端口）

此参数指定了 9160 G2 尝试与第一个移动数据终端建立 Telnet 连接的终端号。默认值为 **10000**。其它 Telnet 会话分配给更高的端口号。

Local IP Address to Bind （要绑定的本地 IP 地址）

此参数指定了连接至本主机的 9160 G2 接口的 IP 地址。此参数可与本地端口号一起使用，为每个终端会话创建唯一的套接字。

First Terminal Listen Port （第一个终端监听端口）

此参数指定了 9160 G2 用于监听 Telnet 连接移动数据终端请求的第一个端口号。要启用此参数，该值至少为 **1024**。要禁用此监听端口，该值必须为 **0**。

默认值为 **0**（禁用）。

TCP Session Request Key （TCP 会话请求密钥）

此参数包含字符的十进制 ASCII 字符代码，将提示移动数据终端请求新的 ANSI 终端会话。范围为 **0 到 255**，默认值为 **1**。

Session Cycle Key （会话周期密钥）

此参数包含字符的十进制 ASCII 字符代码，将提示移动数据终端显示下个 ANSI 终端会话。范围为 **0 到 255**，默认值为 **2**。

Last Active Session Key （上个主动会话密钥）

此参数包含字符的十进制 ASCII 字符代码，将提示移动数据终端显示上个 ANSI 终端会话。范围为 **0** 到 **255**，默认值为 **5**。

23.4.3.3 Auto-Telnet/Auto-login （自动 Telnet/自动登录）

Auto-Telnet / Auto-Login:

Auto-telnet/login Enable:

DISABLE

Auto-telnet Host:

Auto-telnet Terminal Prompt:

Press ENTER to login.

Auto-login User ID:

Auto-login Password:

Auto-login User ID prompt:

gin:

Auto-login Password prompt:

word:

Auto-login failed login:

incorrect

Auto-telnet without User Action:

☐

Auto-telnet without User Action Timing Delay:

25

(Range 0..255)

Maximum of Auto-telnet Retries:

0

(Range 0..255)

Allow TCP Sessions:

☒

Auto-telnet/login Enable （自动 Telnet/登录启用）

您可使用此参数禁用或启用移动数据终端与本主机之间的 Telnet 会话自动连接。可提供以下选择：**DISABLE**（禁用）；**AUTO-TELNET**（自动 TELNET）；**AUTO-TELNET/LOGIN**（自动 TELNET/登录）。默认值为 **DISABLE**（禁用）。

Auto-Telnet（自动 Telnet）设为 **Disable**（禁用）时，必须从移动数据终端手动启动移动数据终端与主机之间的 Telnet 会话。

启用 *Auto-Telnet*（自动 Telnet）后，9160 G2 将在终端号映射到该主机上的每个移动数据终端启动 Telnet 会话。在移动数据终端和主机之间可启动其它 Telnet 会话，但是必须手动启动。



注释：只有“在线”（在 Psion Teklogix RF 网络上打开并正确操作）的移动数据终端才可启动 *Auto-Telnet*（自动 Telnet）会话。

启用 *Auto-Telnet*（自动 Telnet）和 *Auto-login*（自动登录）后，9160 G2 将在终端号映射到该主机的每个移动数据终端启动 Telnet 会话。然后，使用本页面提供的用户 ID 和密码登录到主机进行会话。



注释：用户 ID 和密码与自动登录主机的所有自动 Telnet 会话的用户 ID 和密码相同。

Auto-telnet Host （自动 Telnet 主机）

此参数包含主机的主机名称或 IP 地址，以便主机与 9160 G2 连接 Auto-Telnet（自动 Telnet）会话。



注释：此文本框中的主机名称必须可通过 9160 G2 解析：9160 G2 必须能够获取其 IP 地址。例如，主机名称可能对应 9160 G2 主机列表中的条目，或者 9160 G2 能够询域名服务器。

任何可用于移动数据终端 TCP> 提示的主机名称均可应用于此。

Auto-telnet Terminal Prompt （自动 Telnet 终端提示）

此参数包含向用户显示用于发出登录请求的文本。字符可为任何 ASCII 字符串，或八进制/十六进制数字构成的数字转义序列。

八进制转义序列采用以下格式之一：\0d、\0dd 或 \0ddd，其中 ‘d’ 可为 0-7 的任何数字。如果 ‘ddd’ 大于十进制 256，显示的字符代码值将为十进制 ddd/256 剩余的部分。

十六进制转义序列采用以下格式之一：\xh 或 xhh，其中 ‘h’ 可为 0-9 的任何数字，或 a-f/A-F 的任何字母值。



注释：\0 视为一个字符，代码值为 0。

每一行中允许的值不超过 60 个字符。默认值是无文本，只需按下 <ENTER> 键登录。

Auto-login User ID （自动登录用户 ID）

此参数包含 9160 G2 向主机显示的用于自动登录会话的用户 ID。字符可为主机接受的任何 ASCII 字符串，**最多为 32 个字符**。

Auto-login Password （自动登录密码）

此参数包含 9160 G2 向主机显示的用于自动登录会话的密码。字符可为主机接受的任何 ASCII 字符串，**最多为 32 个字符**。

Auto-login User ID Prompt （自动登录用户 ID 提示）

9160 G2 将对此文本框中的文本与主机显示的文本进行比较。若两者匹配，9160 G2 假设主机已经发送了用户名请求，并向主机发送回 *Auto-Login User ID*（自动登录用户 ID）参数中指定的用户 ID。字符可为任何 ASCII 字符串，**最多为 32 个字符**。默认文本为 **gin**：



注释：匹配字符串尽可能短，只要足够唯一识别用户 ID 提示即可。字符串不可包含由空格字符隔开的多部分字词，因为一些主机发送除空格字符以外的字符在屏幕上表示空格。

Auto-login Password Prompt （自动登录密码提示）

9160 G2 将对此文本框中的文本与主机显示的文本进行比较。若两者匹配，9160 G2 将假设主机已经发送了密码请求，且向主机发送回 *Auto-Login Password* （自动登录密码）参数中指定的密码。字符可为任何 ASCII 字符串，**最多为 32 个字符**。默认文本为 **word**：



注释：匹配字符串尽可能短，只要足够唯一识别密码提示即可。字符串不可包含由空格字符隔开的多部分字词，因为一些主机发送除空格字符以外的字符在屏幕上表示空格。

Auto-login Failed Login （自动登录失败）

9160 G2 将对此文本框中的文本与主机显示的文本进行比较。若两者匹配，9160 G2 将假设主机已经发送了一个字符串，通知移动数据终端登录尝试失败。接下来，9160 G2 会在移动数据终端屏幕上显示 *Auto-Telnet Terminal Prompt* （自动 Telnet 终端提示），请求用户手动登录。字符可为任何 ASCII 字符串，**最多为 32 个字符**。默认文本**不正确**。



注释：匹配字符串尽可能短，只要足够唯一识别登录失败提示即可。字符串不可包含由空格字符隔开的多部分字词，因为一些主机发送除空格字符以外的字在屏幕上表示空格。

Auto-telnet Without User Action （在用户不操作的情况下自动 Telnet）

若启用此项，控制器将立即打开每台初始化的移动数据终端到主机的连接，无需用户按 [ENTER] 键。若选择此项，推荐更改 *Auto Telnet Terminal Prompt* （自动 Telnet 终端提示），以便建议用户在连接尝试期间耐心等待。

Auto-telnet Without User Action Timing Delay （在没有用户操作定时延迟的情况下自动 Telnet）

启用此选项后，*Auto-Telnet Without User Action* （在没有用户操作定时延迟的情况下自动 Telnet）选项可在两次连接尝试之间延迟指定时间（毫秒）。

Maximum Of Auto-telnet Retries （自动 Telnet 最多重试次数）

放弃前自动进行的连接尝试次数。

Allow TCP Sessions （允许 TCP 会话）

启用此参数后，**9160 G2** 使移动数据终端用户能够根据提示切换提示或会话（自动登录或 TCP）。如果 *Allow TCP Sessions* （允许 TCP 会话）**被禁用**，所有新会话将以自动登录会话格式打开。

可根据提示使用请求会话（通常为移动数据终端上的 <CTRL> *a* ）更改提示类型（如果其他类型的提示 可用）。

也可根据提示使用切换会话（移动数据终端上的 <CTRL> *b* [下一次会话]，或 <CTRL> *e* [下一次会话]）。根据提示切换会话时，移动数据终端状态（未登录）将进行适当调整，以匹配会话切换所做的调整。

默认值为启用。

23.4.3.4 Function Key Mappings（功能键映射）

Function Key Mappings:		
F1: 1b,4f,50,00,00,00,00,00	F11: 1b,5b,32,33,7e,00,00,00	F21: 1b,5b,31,7e,00,00,00,00
F2: 1b,4f,51,00,00,00,00,00	F12: 1b,5b,32,34,7e,00,00,00	F22: 1b,5b,32,7e,00,00,00,00
F3: 1b,4f,52,00,00,00,00,00	F13: 1b,5b,32,35,7e,00,00,00	F23: 1b,5b,33,7e,00,00,00,00
F4: 1b,4f,53,00,00,00,00,00	F14: 1b,5b,32,36,7e,00,00,00	F24: 1b,5b,34,7e,00,00,00,00
F5: 1b,5b,31,36,7e,00,00,00	F15: 1b,5b,32,38,7e,00,00,00	F25: 1b,5b,35,7e,00,00,00,00
F6: 1b,5b,31,37,7e,00,00,00	F16: 1b,5b,32,39,7e,00,00,00	F26: 1b,5b,36,7e,00,00,00,00
F7: 1b,5b,31,38,7e,00,00,00	F17: 1b,5b,33,31,7e,00,00,00	F27: 1b,5b,34,31,7e,00,00,00
F8: 1b,5b,31,39,7e,00,00,00	F18: 1b,5b,33,32,7e,00,00,00	F28: 1b,5b,34,32,7e,00,00,00
F9: 1b,5b,32,30,7e,00,00,00	F19: 1b,5b,33,33,7e,00,00,00	F29: 1b,5b,34,33,7e,00,00,00
F10: 1b,5b,32,31,7e,00,00,00	F20: 1b,5b,33,34,7e,00,00,00	F30: 1b,5b,34,34,7e,00,00,00
Up: 1b,5b,41,00,00,00,00,00	Down: 1b,5b,42,00,00,00,00,00	Right: 1b,5b,43,00,00,00,00,00
Left: 1b,5b,44,00,00,00,00,00		

功能键

Function Key（功能键）参数允许您选择一个代码，当您在移动数据终端上按下功能键时即可将代码发送到主机。每个功能键可选自同一代码范围，但是每个功能键的默认代码不同。默认值如上面的屏幕所示。

802.IQ 设置

24

24.1 802.IQ 的功能	295
24.1.1 802.IQ v1/v2 通用功能	295
24.1.2 802.IQ v1 功能	298
24.1.3 802.IQ v2 Features （802.IQ v2 功能）菜单	299
24.2 更新 802.IQ 设置	299

24.1 802.IQ 的功能

802.IQ 是 Psion Teklogix 专有的增强型 802.11 协议，它使得移动数据终端能够在同时支持 TCP/IP 和 802.IQ 协议的网络中的无线 LAN 下运行。802.IQ 协议提供两版本：802.IQ v1 和 802.IQ v2。9160 G2 无线网关可以同时支持协议的两个版本（移动数据终端只能使用一个）。

802.IQ v1 协议是无线 LAN 路由方案，在 802.11 无线网络中提供比 TCP/IP 路由更高的性能。移动数据终端可以使用 TCP/IP 或 802.IQ v1 协议与 9160 G2 接入点通信，这样便实现了系统的双操作性。有关 802.IQv1 的更多信息和配置菜单，请参阅第 298 页。

802.IQ v2 协议是 802.IQ v1 协议的增强版本，通过 UDP 层传输数据包。它提供 802.IQ v1 具有的所有功能，此外还增添了一些新的功能，包括通过 RF 进行软件升级，在控制器和移动数据终端之间添加第三方接入点，以及集成进 mapRF 系统（如果需要）。有关配置 802.IQ v2 微型控制器的信息，请参阅第 299 页。

24.1.1 802.IQ v1/v2 通用功能



重要说明: 仅可在有线 9160 G2 上启用 802.IQ。

请勿在有线 9160 G2 桥接网络上配置 802.IQ，因为会通过 WDS 链路将 802.IQ 信标从一个网络发送至另一个网络（请参阅第 20 章：“无线分布系统”）。

Auto-Startup（自动启动）

此参数会在 9160 G2 重新启动时立即启用 802.IQ。9160 G2 用作网络控制器下的基站或 9160 G2 微型控制器时，必须禁用此参数。

默认值为禁用。



重要说明: 如果自动启动的设置不正确，移动数据终端就无法正常工作。

Beacon Period （信标周期）

802.IQ 信标是发送至支持 802.IQ 的所有移动数据终端的广播。信标允许移动数据终端确定何时在基站之间漫游。它使得移动数据终端能够确定是否重启站或控制器，并且如果重启，何时恢复。如果重启控制器，移动数据终端会关闭所有会话，并完全重新初始化。如果重启基站，或移动数据终端移动到另一个 9160 G2，则完成热初始化（不会丢失任何数据）。

Beacon Period（信标周期）参数可接受的值范围为 **1** 到 **20** 秒。默认值为 **2**。

Terminal Offline Timeout （终端离线超时）

此参数设置了 9160 G2 上的 802.IQ 任务发送离线消息至蜂窝主机声明移动数据终端脱机之前的时间（单位：分钟）。

可接受的值范围为 **1** 到 **240**。默认值为 **5**。

图 24.1 802.IQ 配置设置概述

Basic Settings	Modify 802.IQ settings
User Management	
Cluster	802.IQ v1/v2 Common Features:
Access Points	Auto-Startup: <input type="checkbox"/>
Sessions	Beacon Period: <input type="text" value="2"/> (Range 1..20)
Channel Management	Terminal Offline Timeout: <input type="text" value="5"/> (Range 1..240)
Wireless Neighborhood	
Security	802.IQ v1 Features:
Status	Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Interfaces	Initial RTT: <input type="text" value="1000"/> (Range 10..10000)
Events	Protocol Type ID: <input type="text" value="2457"/> (Range 1501..65535)
Transmit/Receive	Forward 802.IQ packets only: <input type="checkbox"/>
Client Associations	802.IQ v1 Beacon Interfaces:
Neighboring Access Points	Wired: <input type="checkbox"/>
	WLAN0: <input type="checkbox"/>
	WLAN1: <input type="checkbox"/>
	WDS0: <input type="checkbox"/>
	WDS1: <input type="checkbox"/>
	WDS2: <input type="checkbox"/>
	WDS3: <input type="checkbox"/>
Manage	
Ethernet Settings	802.IQ v2 Features:
802.11 Settings	Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
802.11 Advanced Settings	Beacon UDP port: <input type="text" value="8888"/> (Range 5001..65535)
VWN	<input type="button" value="Update"/>
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	
Hosts	
802.IQ	

24.1.2 802.IQ v1 功能

从 *Connectivity* 选项的 *802.IQ* 选项卡进入 *802.IQ v1 Features*（802.IQ v1 功能）菜单（请参阅第 297 页的图 24.1）。

Enabled（启用）

此参数启用或禁用 802.IQ v1 功能。默认值为 **Disabled（禁用）**。

Initial RTT（初始 RTT）

参数 *Initial RTT*（初始 RTT）（往返时间）用于帮助确定接入点传输到终端确认的占用时间（单位：毫秒）。接入点通过计算各台移动数据终端进行大量传输的平均占用时间，继续调节可接受的往返时间。如收到确认的时间大于算得出的平均往返时间，接入点将重新发送该次传输。

由于接入点无法在未进行大量传输的情况下计算出平均往返时间，因此需要一个起始点或“初始往返时间”。接入点使用分配给“初始 RTT”参数的时间作为往返时间计算的起始值。一旦接入点开始与移动数据终端收发数据，将会调整此值，以反映传输和确认之间的实际平均往返时间。

可接受的值范围为 **10** 到 **10000**。默认值为 **1000**。

Protocol Type ID（协议类型 ID）

此参数可用于识别 802.IQ 协议类型，避免与使用相同协议类型的其他生成的以太网类型数据包产生冲突。

可接受的值范围为 **1536** 到 **65535**。默认值为 **2457**。



重要说明: 协议类型 ID 默认值很少更改。如果更改协议类型，则必须更改所有移动数据终端设备以匹配。

Forward 802.IQ Packets Only（仅转发 802.IQ 包）

在无线和有线系统之间桥接数据包时，此参数使 9160 G2 自动筛选出并丢弃所有非 802.IQ v1 的数据包。默认设置为 **Disabled（禁用）**。

802.IQ v1 Beacon Interfaces（802.IQ v1 信标接口）

选择发送信标的接口。

可用的接口包括：*Wired（有线）*、*WLAN0*、*WLAN1*、*WDS0*、*WDS1*、*WDS2*、*WDS3*。

24.1.3 802.IQ v2 Features (802.IQ v2 功能) 菜单

从 *Connectivity* (连接) 选项的 *802.IQ* 选项卡进入 *802.IQ v2 Features* (802.IQ v2 功能) 菜单 (请参阅第 297 页的图 24.1)。

Enabled (启用)

此参数启用或禁用 802.IQv2 协议。

默认值为 **Disabled** (禁用)。

Beacon UDP Port (信标 UDP 端口)

此参数识别用于信标广播的 UDP 端口。如果网络上有多个 802.IQv2 控制器, 则必须更改该参数以分离系统。该参数还必须与移动数据终端上相应的参数配。值范围为 **5001** 到 **65535**。默认值为 **8888**。

24.2 更新 802.IQ 设置

要更新 802.IQ 设置:

1. 导航至 *802.IQ Settings* (802.11 设置) 页面。
2. 根据需要配置设置。
3. 单击 **Update** (更新) 按钮应用更改。

网络时间协议服务器

25

25.1 导航至时间设置	303
25.2 启用或禁用网络时间协议 (NTP) 服务器	304
25.3 更新设置	304

网络时间协议 (NTP) 是同步网络上的计算机时钟时间的 Internet 标准协议。NTP 服务器传输协调世界时 (UTC，也被称为格林威治标准时间) 到它们的客户端系统。NTP 向服务器发送定期时间请求，使用返回的时间戳调整其时钟，包括时区的调整。时间戳将用于指示日志消息中每个事件的日期和时间。请参阅 <http://www.ntp.org>，了解有关 NTP 的更多信息。以下小节介绍如何配置产品名称使用指定的 NTP 服务器。

25.1 导航至时间设置

要启用 NTP 服务器，导航至 *Services* (服务) > *Time* (时间) 选项卡，并如下所述更新字段。

图 25.1 时间设置

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWLN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

Modify how the access point discovers the time

Local Time

Mon Jun 18 18:41:53 UTC 2007

Network Time Protocol (NTP)

☒ Enabled ☐ Disabled

NTP Server

Time Zone

Custom

UTC +0000

Update

25.2 启用或禁用网络时间协议 (NTP) 服务器

要将接入点配置为使用网络时间协议 (NTP) 服务器，首先**启用**NTP，然后选择您想使用的 NTP 服务器。（要关闭网络上的 NTP 服务，在接入点上禁用 NTP。）

表 25.1 NTP 设置

字段	描述
<i>Local Time</i> (当地时间)	每次更新时显示当地时间。
<i>Network Time Protocol (NTP)</i> (网络时间协议 (NTP))	<p>NTP 为接入点提供了从网络上的服务器获取并保留其时间的方式。使用 NTP 服务器后，您的 AP 便能够在日志消息和会话信息中提供正确的时间。</p> <p>有关 NTP 的更多信息，请参阅 http://www.ntp.org。</p> <p>选择启用或禁用网络时间协议 (NTP) 服务器：</p> <ul style="list-style-type: none">• 要启用 NTP 服务器，单击 Enabled（启用）。• 要禁用 NTP 服务器，单击 Disabled（禁用）。
<i>NTP Server</i> (NTP 服务器)	<p>启用 NTP 后，选择您想要使用的 NTP 服务器。</p> <p>您可以通过主机名或 IP 地址指定 NTP 服务器，但建议不要使用 IP 地址，因为 IP 地址更容易更改。</p>
<i>Time Zone</i> (时区)	<p>下拉列表上显示时区列表（例如，“EST (-05:00)”），并显示设置自定义值的选项。选择 <i>Custom</i>（自定义）后，选中的方框旁显示两个文本框，您可以在其中输入缩写以及 UTC 的偏差。与 UTC 的自定义偏差显示为 UTC 以东的小时和分钟。例如，-0800 表示 UTC 以西 8 小时（即太平洋标准时间），而 +0930 表示 UTC 以东 9 小时 30 分（即澳大利亚中部标准时间）。</p> <p>不提供夏令时调整。</p>

25.3 更新设置

要更新时间设置，请执行以下操作：

1. 导航至 *Time*（时间）选项卡页面。
2. 根据需要配置时间设置。
3. 单击 **Update**（更新）按钮应用更改。

备份和还原配置

26

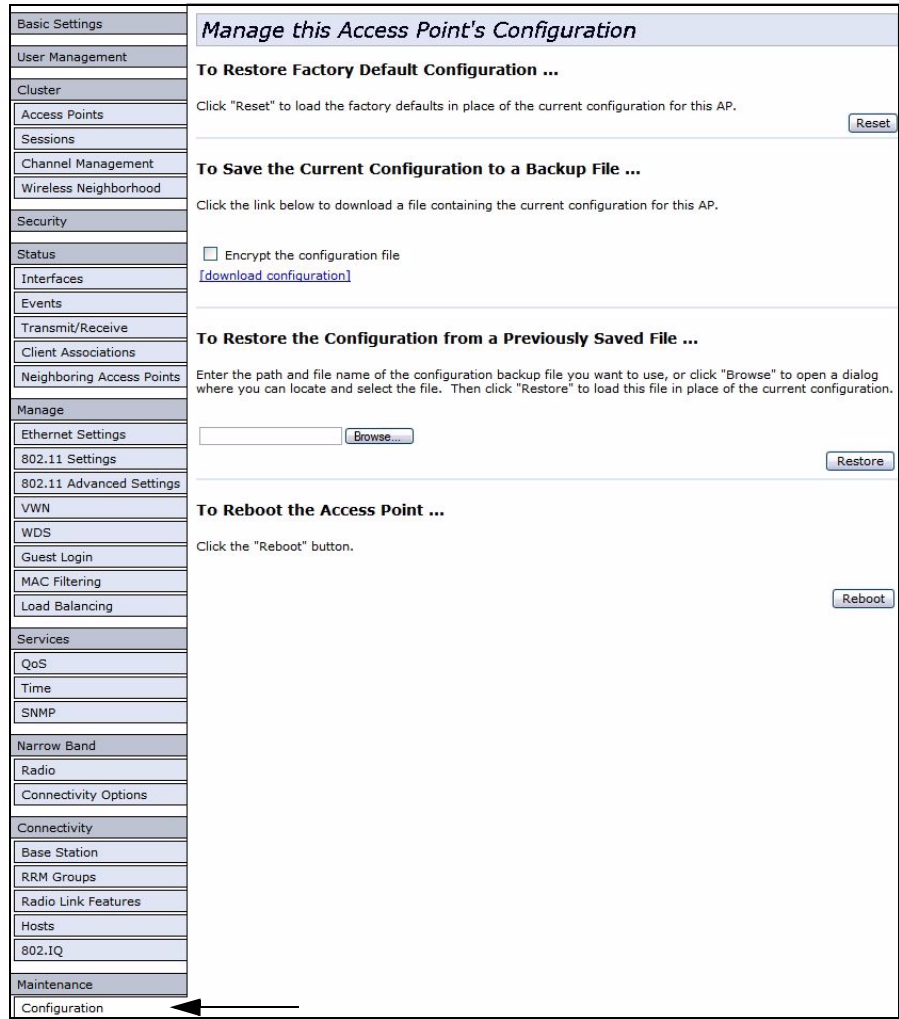
26.1 导航至 AP 的配置设置	307
26.2 重置出厂默认配置	308
26.3 将当前配置保存到备份文件	308
26.4 从之前保存的文件还原配置	308
26.5 重启接入点	309
26.6 升级固件	309
26.6.1 更新	310
26.6.2 验证固件升级	311

您可以将产品名称上当前设置的副本保存到备份配置文件。以后可使用该备份文件将接入点还原为先前保存的配置。

26.1 导航至 AP 的配置设置

要管理接入点的配置，请导航至 *Maintenance*（维护）> *Configuration*（配置）选项卡，然后如下所述使用界面。

图 26.1 AP 配置概述



26.2 重置出厂默认配置

如果您使用产品名称时遇到问题并尝试过所有其他故障排除方法，请使用 *重置配置* 功能。此操作将还原出厂默认值并清除所有设置，包括新密码或无线设置等设置。

1. 单击 **Maintenance**（维护）> **Configuration**（配置）选项卡。
2. 单击 **Reset**（重置）按钮。

系统将还原出厂默认设置。



注释：请谨记，如果您在此页面上重置配置，则仅仅是重置此接入点的配置，而不会重置集群中其他接入点的配置。

有关出厂默认设置的信息，请参阅第 25 页的“产品名称的默认设置”。

26.3 将当前配置保存到备份文件

要将接入点当前设置的副本保存到备份配置文件（.cbk 格式），请执行以下操作：

1. 单击 **download configuration**（下载配置）链接。

将显示 *File Download or Open*（下载或打开文件）对话框。

2. 在第一个对话框中，选择 *Save*（保存）选项。

将显示文件浏览器。

3. 使用文件浏览器导航至您想要保存该文件的目录，然后单击 **OK**（确定）保存文件。

您可以保留默认的文件名 (config.cbk) 或重命名该备份文件，但务必使用 .cbk 扩展名保存文件。

26.4 从之前保存的文件还原配置

要将接入点的配置还原为之前保存的设置，请执行以下操作：

1. 通过在 *Restore*（还原）文本框中输入完整路径和文件名，或单击 **Browse**（浏览）并选择该文件，选择您想要使用的备份配置文件。

（只有那些使用备份功能创建并保存为 .cbk 备份配置文件的文件才能使用还原功能，例如 config.cbk。）



重要说明：仅可将配置文件还原到型号与获取配置文件的网关型号相同的 9160。

例如，9160 G2 型号“9160 无线网关”将无法还原从 9160 G2 型号“9160 无线网关（双射频）”中保存的配置文件。

2. 单击 **Restore**（还原）按钮。

接入点将会重启。



注释：单击 **Restore**（还原）后，接入点将会重启。将显示“reboot”（重启）确认对话框，随后会显示“rebooting”（重启中）状态消息。请等待重启过程完成（1 到 2 分）。稍后，尝试访问下一步中所述的管理 Web 页面；AP 重启前无法访问这些页面。

接入点重启后，通过再次单击其中一个选项卡（如果 UI 仍然显示）或在浏览器中输入接入点的 IP 地址，访问管理 Web 页面。现在，您应该看到配置设置还原为从您从备份文件检索的原始设置。

26.5 重启接入点

出于维护目的或作为故障排除措施，您可以如下所示重启产品名称。

1. 单击 **Maintenance**（维护）> **Configuration**（配置）选项卡。
2. 单击 **Restore**（还原）按钮。

接入点将会重启。

26.6 升级固件

当产品名称固件的新版本可用时，您可以在设备上升级该固件，以使用新功能和增强功能。



重要说明：请勿从与您正在升级的接入点相关联的无线客户端升级该固件。这样会导致升级失败。而且，将解除所有无线客户端的关联，且不允许有任何新关联

如果您遇到这种情况，解决办法是使用有线客户端获取对接入点的访问。

- 创建从 PC 到接入点的有线以太网连接。
- 显示管理 UI。

使用有线客户端重复升级过程。



注释：您必须对各个接入点执行升级，无法在集群中自动升级固件。

请记住，固件升级成功后，将接入点配置还原为出厂默认设置。（请参阅第 25 页的“产品名称的默认设置”。）

要升级特定接入点上的固件，请执行以下操作：

1. 在该接入点的管理 Web 页面上导航至 *Maintenance*（维护）> *Upgrade*（升级）。

Upgrade firmware

Model

9160 Wireless Gateway NB (Dual Radio)

Platform

PTX9160G2

Firmware Version

E187k

New Firmware Image

Browse...

Please note:

Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

Upgrade

系统将显示有关当前固件版本的信息，并提供升级新固件映像的选项。

2. 如果您知道新固件映像文件的路径，请在 *New Firmware Image*（新的固件映像）文本框中输入。或者，请单击 **Browse**（浏览）按钮并找到该固件映像文件。



注释：提供的固件升级文件必须为以下格式：
`<FileName>.upgrade.tar`

请勿尝试使用 `<FileName>.bin` 文件或其他格式的文件进行升级，都不能成功升级。

26.6.1 更新

1. 单击 **Update**（更新）应用新的固件映像。
单击 **Update**（更新）进行固件升级后，会显示弹出的确认窗口，说明升级过程。
2. 单击 **OK**（确定）确认升级并开始升级过程



重要说明：在弹出的确认窗口中单击 *Update*（更新）和 *OK*（确定）后，固件升级过程开始。

接入点不可用时，升级过程可能需要几分钟时间。升级过程中，请勿关闭接入点的电源。升级完成后，接入点将会重启并使用出厂默认配置设置恢复常操作。

26.6.2 验证固件升级

要验证固件升级是否成功完成，请查看 *Upgrade*（升级）选项卡（以及 *Basic Settings*（基本设置）选项卡）上显示的固件版本。如果升级成功，将显示升级后的版本名称或版本号。

27.1 外形描述315
27.2 环境要求315
27.3 AC 电源要求315
27.4 以太网供电要求316
27.5 处理器和内存316
27.6 网络接口316
27.7 射频316



注释：性能规格为额定值，如有变更恕不另行通知。

27.1 外形描述

机箱：	乌黑色， FR2000 Bayblend 材料
尺寸：	≤ 30 x 20 x 12.5 厘米 （11.8 x 7.9 x 4.9 英寸）
重量：	≤ 2.25 kg (5.0 lbs.) （不包括无线通信设备、 天线和选件）

27.2 环境要求

工作温度：	0°C 至 45°C （32°F 至 113°F）
工作相对湿度：	10% 至 90%
存放温度：	-0°C 至 70°C （-32°F 至 158°F）
防尘防水：	IP42 或更高
振动：	EH0002 （仅限运输振动）
可靠性：	MTBF 25,000 小时 (MIL-HDBK-217F)

27.3 AC 电源要求

通过标准 IEC320 接头的通用输入。连接时禁用以太网供电 （发现 802.3af）

输入电压：	100 - 240 VAC （额定值）
电流：	5.0 A （最大值）



警告： 在快卸底座上的接地螺钉与 9160 G2 上适合连接至室外安装天线的任何接地焊接点之间，必须连接一根长度不超过 3 米的接地线。

27.4 以太网供电要求

与 IEEE 802.3af 兼容（连接 AC 电源时禁用）。	
输入电压：	37-57 VDC
板载	
电源：	2.5W（假设从以太网供电满 12.5 瓦特时， $\eta=0.8$ ）
双 802.11b 射频：	4W
逻辑主板：	6W

27.5 处理器和内存

以 266 MHz 运行的 Intel IXP420 处理器	
8 MB Flash ROM	
32 MB SDRAM	

27.6 网络接口

板载以太网：	10BaseT/100BaseT (10/100 Mb/s) 卡，具有自动协商，半双工和全双工。自动感应数据速率。
--------	---

27.7 射频

不带集成天线的 Mini-PCI 卡 802.11A/G 射频	
不带集成天线的 Mini-PCI 卡 802.11G 射频	
发射功率	100 mW（FCC 国家/地区）； 50 mW（ETSI）
频率范围	2.4 - 2.5 GHz (802.11b/g)； 5.15 - 5.825 GHz (802.11a)
数据速率	802.11b： 1、 2、 5.5、 11 Mb/s 802.11a/g： 6、 9、 12、 18、 24、 36、 48、 54 Mb/s

信道 编号	FCC:	11 (802.11b/g) 和 12 (802.11a)
	ETSI:	13 (802.11b/g) 和 19 (802.11a)
	中国:	13 (802.11b/g) 和 4 (802.11a)



注释：所有 802.11a 信道均为非重叠信道。 2.4 GHz 频段中有非重叠信道。

RA1001A - 窄带射频

Psion Teklogix 专有窄带调制（2/4 级 FSK）

III 型 PC 卡外形

发射功率	1W 或 0.5W
频率范围	403-422 MHz、 419-435 MHz、 435-451 MHz、 450-470 MHz、 464-480 MHz、 480-496 MHz、 496-512 MHz
接收灵敏度	< -110dBm @ 19.2kbps （4 级 FSK）
数据速率	4800 bps、 9600 bps、 19.2 kbps

附录 A

端口引脚分配和接线图

A.1 控制台端口

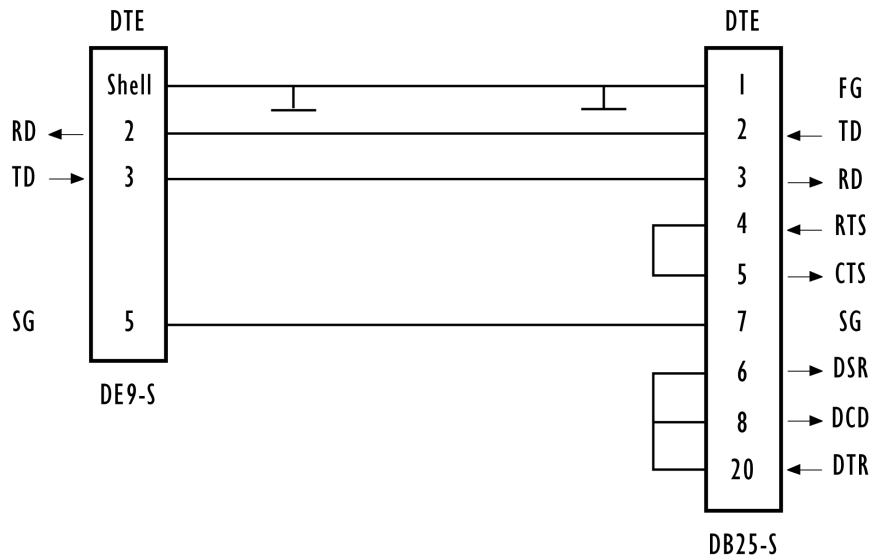
引脚编号	名称	功能	方向
3	TD	传输数据	输出
2	RD	接收数据	输入
5	SG	信号接地	-
4*	DTR	数据终端就绪	输出
7*	RTS	请求发送	输出

* 始终拉高

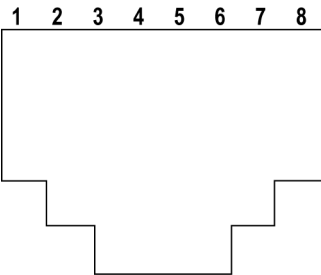
A.2 串行电缆描述

电缆编号	功能	连接	标准长度
19387	将 9160 G2 连接到控制台	直连	6 英尺

控制台端口电缆编号 19387



A.3 RJ-45 连接器引脚分配（10BaseT/100BaseT 以太网）



使用 AC 的 9160 G2		使用以太网供电的 9160 G2*	
1	TD+	1	TD+
2	TD -	2	TD -
3	RD+	3	RD+
4	未使用	4	
5	未使用	5	
6	RD -	6	RD -
7	未使用	7	
8	未使用	8	
		* 9160 G2 还可从提供以太网供电的系统接受数据线对 (1,2) 和 (3,6) 上的 48 VDC 电源偏压。	



注释: 通常，需要以直连方式连接双绞线（10BaseT 或 100BaseT）和集线器。

无线客户端/RADIUS 服务器上的安全设置

B.1 网络基础设施：在内置或外部身份验证服务器之间进行选择	7
B.1.1 使用内置身份验证服务器 (EAP-PEAP)	8
B.1.2 使用具有 EAP-TLS 证书或 EAP-PEAP 的外部 RADIUS 服务器	8
B.2 确保无线客户端软件是最新的	8
B.3 访问 Microsoft Windows 无线客户端安全设置	9
B.4 配置客户端以访问不安全的网络（无安全性）	11
B.5 在客户端上配置静态 WEP 安全性	12
B.6 在客户端上配置 IEEE 802.1x 安全性	15
B.6.1 使用 EAP/PEAP 的 IEEE 802.1x 客户端	15
B.6.2 使用 EAP/TLS 证书的 IEEE 802.1x 客户端	19
B.7 在客户端上配置 WPA/WPA2 Enterprise (RADIUS) 安全性	23
B.7.1 使用 EAP/PEAP 的 WPA/WPA2 Enterprise (RADIUS) 客户端	23
B.7.2 使用 EAP-TLS 证书的 WPA/WPA2 Enterprise (RADIUS) 客户端	27
B.8 在客户端上配置 WPA/WPA2 Personal (PSK) 安全性	30
B.9 配置外部 RADIUS 服务器以识别 9160 G2	33
B.10 获取客户端的 TLS-EAP 证书	37
B.11 配置 RADIUS 服务器用于 VLAN 标记	42
B.11.1 配置 RADIUS 服务器	42

通常情况下, 用户会配置其无线客户端上的安全性, 以访问许多不同的网络 (接入点)。“Available Networks” (可用网络) 列表将会发生变化, 具体取于客户端的位置以及该位置中哪些 AP 在线且可以检测到。¹ 客户端检测到一个 AP 并配置其安全性后, 该 AP 便会保留在客户端的网络列表中, 但显示为可以访问或不可访问, 具体视情况而定。对于您想要连接各个网络 (AP), 请配置客户端的安全性设置, 以匹配该网络当前使用的安全模式。

我们将介绍使用 Microsoft® Windows® 客户端软件进行无线连接的客户端上的安全性设置。之所有使用 Windows 客户端软件为例, 这是因为它在 Windows 计算机和笔记本电脑上具有广泛的可用性。如果您在客户端上使用不同的软件 (例如 Funk Odyssey®), 流程会略有不同, 但需要您提供的配置信息是相同的。



注释: 进行安全配置时, 建议的顺序是: (1) 设置接入点的安全性; (2) 配置各无线客户端的安全性。

我们预计, 刚开始您会从不安全的无线客户端连接至未设置安全性 (“None” (无)) 的接入点。初次连接时, 您可以进入接入点的管理 Web 页面并配安全模式 (Security (安全性))。

*当您为接入点重新配置了安全设置并单击 **Update** (更新) 后, 您的无线客户端将会被取消关联, 并且您将失去与 AP 管理 Web 页面的连接。在某些情况下, 您可能需要对 AP 安全设置进行额外更改, 才能配置客户端。因此, 您必须拥有备用以太网 (有线) 连接。*

以下小节介绍了如何在产品名称所服务网络的无线客户端上设置支持的安全模式。

B.1 网络基础设施; 在内置或外部身份验证服务器之间进行选择

网络安全配置包括公钥基础设施 (PKI)、远程身份验证拨号用户服务 (RADIUS) 服务器和证书颁发机构 (CA), 在它们提供身份验证、授权和计费 (AAA) 的方式方面, 不同的组织之间有着很大的区别。最后, 您的基础设施的细节将会确定客户端如何配置安全性以访问无线网络。本文档提供有关产品名称支持的各种类型的客户端配置的一般准则, 而不是尝试预测并提供各种可能情景的详细信息。

¹ 例外情况是, 将接入点设为禁止广播其网络名称。在这种情况下, SSID 将不会出现在客户端的 Available Networks (可用网络) 列表中。客户端必须在网络接属性中配置确切的网络名称, 才能进行连接。

B.1.1 使用内置身份验证服务器 (EAP-PEAP)

如果您没有 RADIUS 服务器或 PKI 基础设施和/或对许多概念并不熟悉，我们强烈建议您通过在 AP 上使用 *内置身份验证服务器* 的安全性来设置产品名称。这就意味着，将 AP 设置为使用 IEEE 802.1x 或 WPA/WPA2 Enterprise (RADIUS) 安全模式。(内置身份验证服务器使用 EAP-PEAP 身份验证协议。)

- 如果将产品名称设置为使用 IEEE 802.1x 模式和内置身份验证服务器，则如第 B-15 页的“使用 EAP/PEAP 的 IEEE 802.1x 客户端”中所述配置无线客户端。
- 如果将产品名称配置为使用 WPA/WPA2 Enterprise (RADIUS) 模式和内置身份验证服务器，则如第 B-23 页的“使用 EAP/PEAP 的 WPA/WPA2 Enterprise (RADIUS) 客户端”中所述配置无线客户端。

B.1.2 使用具有 EAP-TLS 证书或 EAP-PEAP 的外部 RADIUS 服务器

我们假设，如果您使用外部 RADIUS 服务器并设置了 PKI/CA，那么您就知道如何配置安全基础设施适用的客户端安全性选项，无需这里提供的基础建议。里介绍的与 RADIUS - PKI 环境中进行客户端安全性配置特别相关的主题包括：

- 第 B-19 页的“使用 EAP/TLS 证书的 IEEE 802.1x 客户端”。
- 第 B-27 页的“使用 EAP-TLS 证书的 WPA/WPA2 Enterprise (RADIUS) 客户端”。
- 第 B-33 页的“配置外部 RADIUS 服务器以识别 9160 G2”。
- 第 B-37 页的“获取客户端的 TLS-EAP 证书”。

本文档中不包含有关如何配置 EAP-PEAP 客户端使用外部 RADIUS 服务器的详细信息。

B.2 确保无线客户端软件是最新的

开始前，请谨记，无线客户端的服务包、补丁程序、驱动程序的新版本及其它支持技术推出的节奏非常之快。在客户端安全设置过程中，最常见的问就是，客户端上没有安装合适的驱动程序或更新。例如，如果您在客户端上设置 WPA，请确保您已安装支持 WPA 的驱动程序，而 WPA 是相对较新的技术。即使是当前可用的许多客户端卡，出厂时也不随附最新的驱动程序。

B.3 访问 Microsoft Windows 无线客户端安全设置

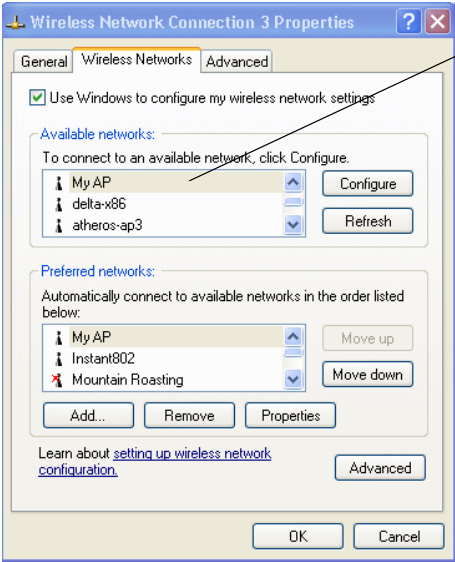
通常情况下，在 Windows XP 上有两种方式可以进入无线客户端的安全属性：

1. 从 Windows 任务栏的 *无线连接* 图标：
 - 右键单击 Windows 任务栏中的无线连接图标，并选择 **View available wireless networks**（查看可用的无线网络）。
 - 选择您要连接的网络的 SSID，并单击 **Advanced**（高级）以显示 *Wireless Network Connection Properties*（无线网络连接属性）对话框。

或

1. 从任务栏左下角的 Windows 开始菜单：
 - 从任务栏的 Windows 开始菜单，依次选择 **Start**（开始）、**My Network Places**（网上邻居），以显示 Network Connections（网络连接）窗口。
 - 从左侧的 *Network Tasks*（网络任务）菜单中，单击 **View Network Connections**（查看网络连接），以显示 *Network Connections*（网络连接）窗口。
 - 选择您要配置的 *Wireless Network Connection*（无线网络连接），单击鼠标右键并选择 **View available wireless networks**（查看可用的无线网络）。
 - 选择您要连接的网络的 SSID，并单击 **Advanced**（高级）以显示 *Wireless Network Connection Properties*（无线网络连接属性）对话框。

Wireless Networks（无线网络）选项卡（应自动显示）列出 *Available networks*（可用网络）以及 *Preferred networks*（首选网络）。



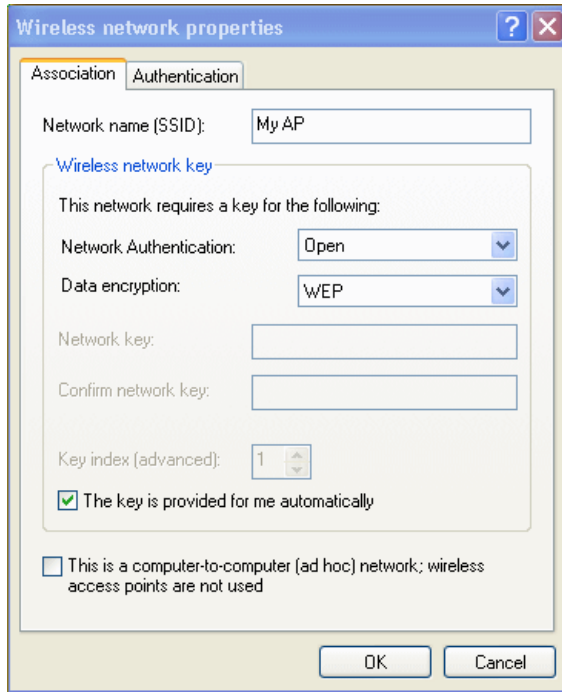
可用网络的列表将根据客户端位置发生变化。
此列表中显示客户端检到的各个网络（或接入点）。
（单击“Refresh”（刷新）后，将会使用最新信息更新该列表。）

对于您想要连接的各个网络，
在客户端上配置安全设置，
以匹配该网络当前使用的
安全模式。

注意：例外情况是，如果将 AP 配置为禁止广播其
网络名称，则此列表上将不会显示该名称。在这种
情况下，您可能需要输入确切的网络名称才能进行
连接。

2. 从 *Available networks* （可用网络）列表中，选择您想要连接的网络的 SSID，
并单击 **Configure** （配置）。

将显示 *Wireless Network Connection Properties* （无线网络连接属性）对话框以
及选定网络的 *Association* （关联）和 *Authentication* （身份验证）选项卡。



如以下小节中所述，使用此对话框配置所有不同类型的客户端的安全性。确保您使用的 *Wireless Network Properties*（无线网络属性）对话框属于您想要在当前配置的无线客户端上访问的网络的网络名称 (SSID)。

B.4 配置客户端以访问不安全的网络（无安全性）

如果您想要连接的接入点或无线网络配置为“None”（无），即表示没有安全性，则您需要对客户端进行相应的配置。如下所述，配置不使用任何安全性进行连接的客户端：将 *Network Authentication*（网络身份验证）设为 **Open**（开放式），将 *Data Encryption*（数据加密）设为 **Disabled**（禁用）。

如果您在具有不安全网络属性的客户端上进行了安全配置，则安全设置会阻止对网络的成功访问，这是由于客户端与接入点之间的安全配置不匹配所造成的。

要将客户端配置为不使用任何安全性，可打开客户端 *Network Properties*（网络属性）对话框，并配置以下设置。



表 B.1 关联设置

<i>Network Authentication</i> （网络身份验证）	Open （开放式）
<i>Data Encryption</i> （数据加密）	Disabled （禁用）

B.5 在客户端上配置静态 WEP 安全性

静态有线等效加密(WEP) 基于静态（不变）密钥，对在无线网络上移动的数据进行加密。加密算法是被称为 RC4 的“流”密码。接入点使用密钥将数据传输至客户端工作。各个客户端必须使用相同的密钥才能对它从接入点接收的数据进行解密。不同的客户端可以使用不同的密钥将数据传输至接入点。（或者，它们可以都使用相同的密钥，但这样会降低安全性，因为这就意味着一个工作站可以解密另一个工作站发送的数据。）

如果您将产品名称配置为使用静态 WEP 安全模式。 ..

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: **Static WEP**

Transfer key index: **1**

Key Length: ☐ 64 bits ☒ 128 bits ☐ 152 bits

Key Type: ☐ ASCII ☒ Hex

WEP Keys: (Characters required: 26)

1: 012345678901234567890123

2: 012345678901234567890123

3:

4:

Authentication: ☒ Open system ☐ Shared key

Update

...然后, 如下所述在各客户端上配置 WEP 安全性。

Wireless network properties

Association | **Authentication**

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: **Open**

Data encryption: **WEP**

Network key:

Confirm network key:

Key index (advanced): **1**

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK **Cancel**

选择 Open (开放式) 或 Shared (共享)

选择 WEP 作为 Data Encryption (数据加密) 模式

输入与设定为传输密钥索引的位置的接入点上的 WEP 密钥匹配的网络密钥 (然后重新键入以确认)

可根据需要设置另一个传输密钥索引, 将来自客户端的数据发送回接入点

禁用自动密钥选项

表 B.2 关联设置

<i>Network Authentication</i> (网络身份验证)	Open （开放式）或 Shared （共享），具体取决于您在接入点上如何配置此选项。 注： 将接入点上的 Authentication Algorithm（身份验证算法）设为 Both （二者）时，设为 Shared （共享）或 Open （开放式）的客户端可以与 AP 进行关联。配置为在共享模式下使用 WEP 的客户必须有有效的 WEP 密钥，才能与该 AP 进行关联。配置为使用 WEP 作为开放式系统的客户端甚至无需有效的 WEP 密钥也可以与该 AP 进行关联（但需要有效的密钥才能真正查看并交换数据）。有关更多信息，请参阅接入点上的联机帮助。
<i>Data Encryption</i> (数据加密)	WEP
<i>Network Key</i> (网络密钥)	提供您在接入点传输密钥索引位置的 <i>Security settings</i> （安全设置）中输入的 WEP 密钥 。 例如，如果将接入点上的 Transfer Key Index（传输密钥索引）设为 1，则对于客户端 Network Key（网络类型），指定您输入的 WEP 密钥作为接入点上的 WEP 密钥 1 。
<i>Key Index</i> （密钥索引）	设置密钥索引以指明在接入点 <i>Security</i> （安全性）页面上指定哪些 WEP 密钥用于将来自客户端的数据发送回接入点。 例如，如果您在接入点上配置了 4 个 WEP 密钥，则可以将此设为 1、2、3 或 4。
<i>The key is provided for me automatically</i> （自动为我提供密钥）	禁用 此选项（单击以取消选中该方框）。
<i>Enable IEEE 802.1x authentication for this network</i> （为此网络启用 IEEE 802.1x 身份验证）	确保 禁用 IEEE 802.1x 身份验证（应取消选中该方框）。 （将加密模式设置为 WEP，会自动禁用身份验证。）

表 B.3 身份验证设置

<i>Enable IEEE 802.1x authentication for this network</i> （为此网络启用 IEEE 802.1x 身份验证）	确保 禁用 IEEE 802.1x 身份验证（应取消选中该方框）。 （将加密模式设置为 WEP，会自动禁用身份验证。）
---	---

在 *Wireless Network Properties*（无线网络属性）对话框上单击 **OK**（确定），即可将其关闭并保存您的更改。

通过静态 WEP 客户端连接至无线网络

静态 WEP 客户端现应能够与接入点关联并进行身份验证。系统不会提示客户端提供 WEP 密钥。当您连接时，自动使用在客户端安全性设置上配置的 WEP 钥。

B.6 在客户端上配置 IEEE 802.1x 安全性

IEEE 802.1x 标准定义了基于端口的身份验证和基础设施，可用于密钥管理。通过使用被称为 EAP Encapsulation Over LAN (EAPOL, EAP LAN 封装) 的协议的 IEEE 802.11 无线网，发送可扩展身份验证协议(EAP) 消息。IEEE 802.1x 提供动态生成的密钥，且定期刷新。RC4 流密码用于加密帧主体及各个 802.11 帧的循环冗余校验 (CRC)。

B.6.1 使用 EAP/PEAP 的 IEEE 802.1x 客户端

产品名称上的内置身份验证服务器使用被称为 “EAP/PEAP” 的受保护的可扩展身份验证协议 (EAP)。

- 如果您在产品名称上使用具有 “IEEE 802.1x” 安全模式的内置身份验证服务器，则需要将无线客户端设置为使用 PEAP。
- 此外，您还需要拥有一台使用 EAP/PEAP 的外部 RADIUS 服务器。如果这样，您需要：
 1. 将产品名称添加到 RADIUS 服务器客户端列表。
 - 并且
 2. 将您的 IEEE 802.1x 无线客户端配置为使用 PEAP。

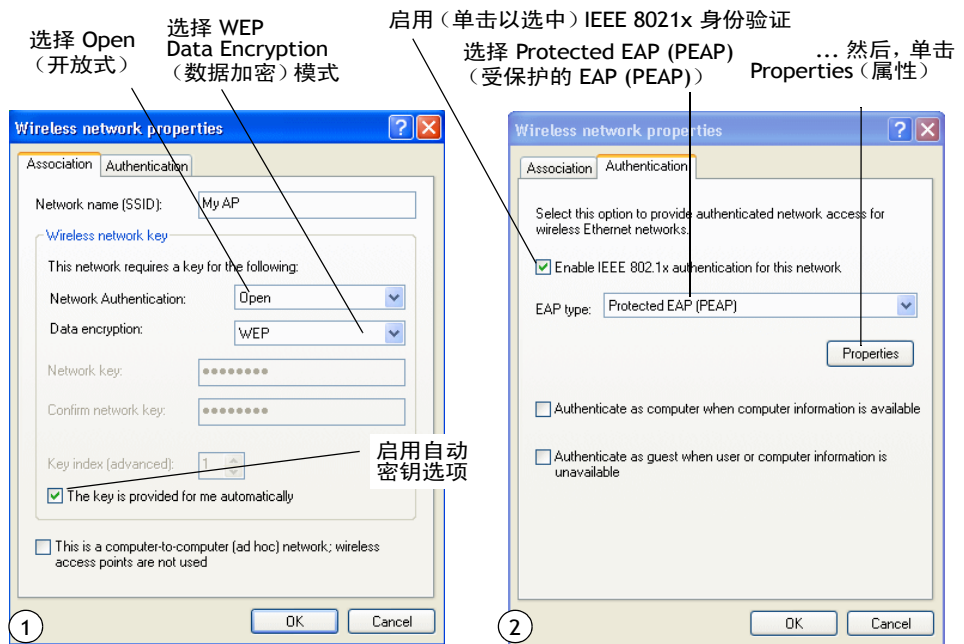


注释: 在以下示例中，假设您使用 9160 G2 无线网关附带的内置身份验证服务器。如果您在使用外部 RADIUS 服务器的 AP 客户端上设置 EAP/PEAP，则客户端配置流不同于本示例，尤其是在证书验证方面。

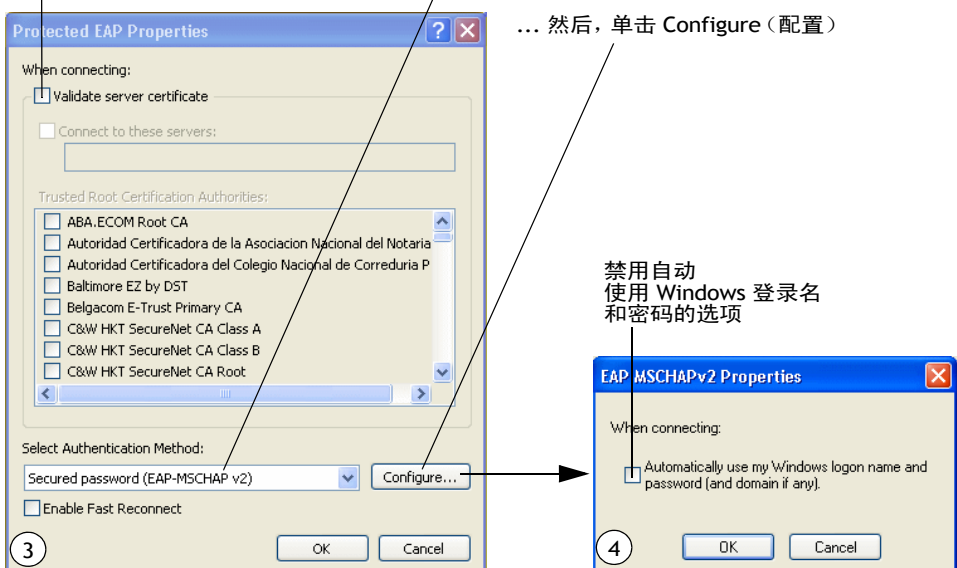
如果您将产品名称配置为使用 IEEE 802.1x 安全模式...

Basic Settings	<h3>Modify Internal Network security settings</h3> <div><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</div> <div>Mode: IEEE802.1x ▼</div> <div><input type="checkbox"/> Use internal radius server</div> <div>Radius IP: 10.128.14.14</div> <div>Radius Key: ●●●●●●●●</div> <div><input type="checkbox"/> Enable radius accounting</div> <div>Update</div>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	

...则如下所述在各个客户端上配置使用 PEAP 身份验证的 IEEE 802.1x 安全性:



禁用 Validate server certificate (验证服务器证书)
选择 Secured password (EAP-MSCHAP v2) (安全密码 (EAP-MSCHAP v2))



1. 在 *Network Properties*（网络属性）对话框的 *Association*（关联）选项卡上配置以下设置。

表 B.4 关联设置

<i>Network Authentication</i> (网络身份验证)	Open（开放式）
<i>Data Encryption</i> (数据加密)	WEP 注： RC4 流密码用于加密帧主体及各个 802.11 帧的循环冗余校验(CRC)。此加密算法与静态 WEP 使用的算法相同；因此，此模式下在客户端上配置的数据加密法是 WEP。
<i>This key is provided for me automatically</i> （自动为我提供密钥）	启用 （单击以选中）此选项。

2. 在 *Authentication*（身份验证）选项卡上配置此设置。

表 B.5 身份验证设置

<i>EAP Type</i> （EAP 类型）	选择 Protected EAP (PEAP) （受保护的 EAP (PEAP)）。
--------------------------	---

3. 单击 **Properties**（属性）将显示 *Protected EAP Properties*（受保护的 EAP 属性）对话框，并配置以下设置。

表 B.6 受保护的 EAP 属性设置

<i>Validate server certificate</i> (验证服务器证书)	禁用 此选项（单击以取消选中该方框）。 注： 此示例假设您在 AP 上使用内置身份验证服务器。如果您在使用外部 RADIUS 服务器的 AP 客户端上设置 EAP/PEAP，则需要验证证书并选择证书，具体取决于您的基础设施。
<i>Select Authentication Method</i> (选择身份验证方法)	选择 Secured password (EAP-MSCHAP v2) （安全密码 (EAP-MSCHAP v2)）。

4. 单击 **Configure**（配置）显示 *EAP MSCHAP v2 Properties*（EAP MSCHAP v2 属性）对话框。
- 在此对话框上，**禁用**（单击以取消选中）*Automatically use my Windows logon name ...*（自动使用我的 Windows 登录名...）选项。
- 在所有对话框（第一个显示的是 *EAP MSCHAP v2 Properties*（EAP MSCHAP v2 属性）对话框）上单击 **OK**（确定）可关闭对话框并保存您的更改。

使用 IEEE 802.1x PEAP 客户端登录到无线网络

IEEE 802.1x PEAP 客户端现应能够与接入点关联。系统将提示客户端用户输入用户名和密码，以对网络进行身份验证。

B.6.2 使用 EAP/TLS 证书的 IEEE 802.1x 客户端

可扩展身份验证协议 (EAP) 传输层安全性 (TLS) 或 EAP-TLS 是支持使用智能卡和证书的身份验证协议。如果您的网络上有一台外部 RADIUS 服务器提供支持，则可以选择将 EAP-TLS 用于 WPA/WPA2 Enterprise (RADIUS) 和 IEEE 802.1x 模式。



注释: 如果您想要将 IEEE 802.1x 模式与 EAP-TLS 证书结合使用进行客户端的身份验证和授权，则必须有一台外部 RADIUS 服务器和一个公钥基础设施 (PKI)，包括在的网络上配置的服务器 — 证书颁发机构 (CA)。RADIUS 服务器、PKI 和 CA 服务器的配置不在此文档的介绍范围内。请参阅这些产品的说明文档。

Microsoft Windows PKI 软件的 Web 上提供一些良好的起点文章，包括：

“如何安装/卸载 Windows 2000 的公钥证书颁发机构”，地址：<http://support.microsoft.com/default.aspx?scid=kb:zh-cn:231881>，以及

“如何配置证书服务器”，地址：

<http://support.microsoft.com/default.aspx?scid=kb:zh-cn:318710#3>。

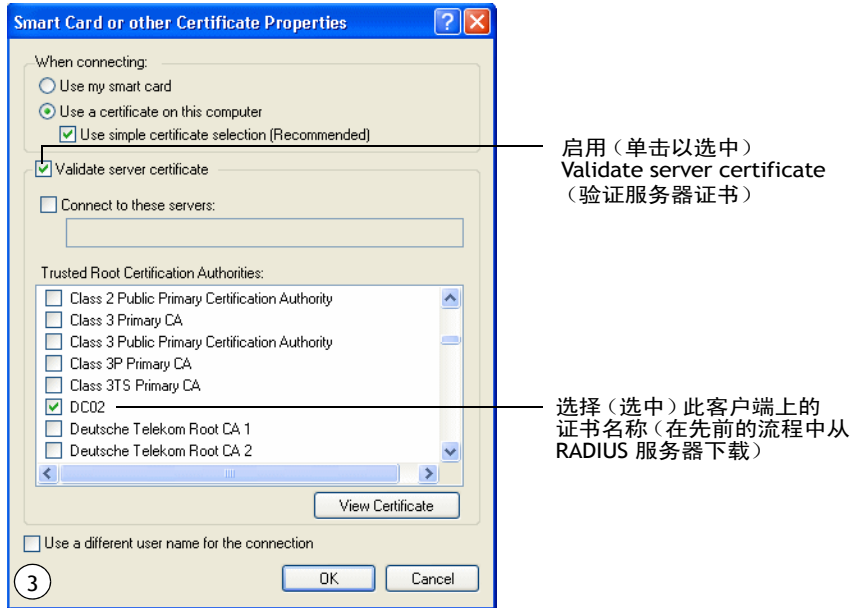
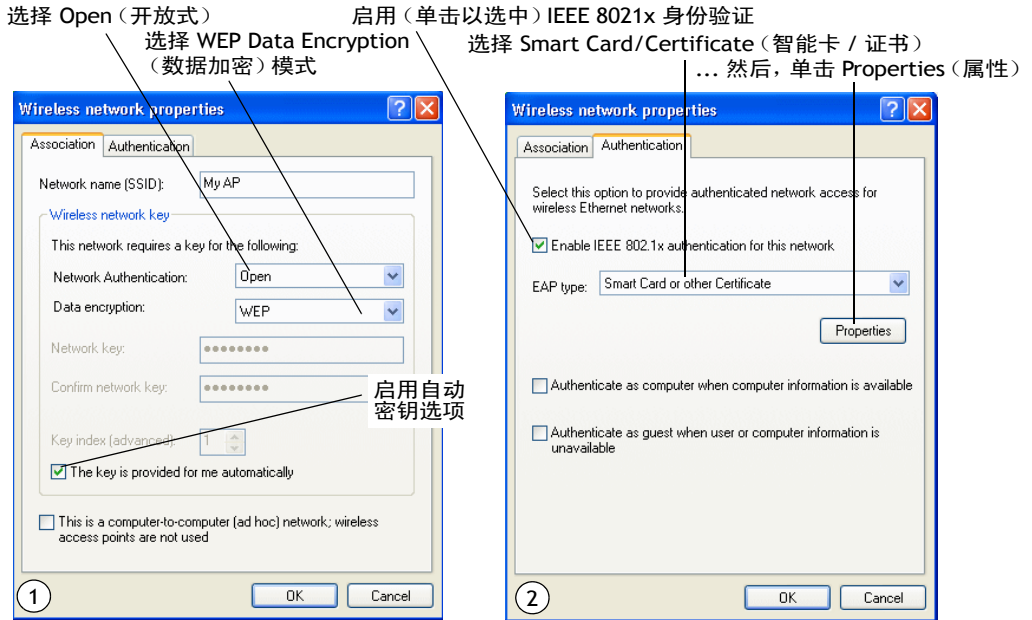
要使用此安全类型，必须执行以下操作：

1. 将产品名称添加到 RADIUS 服务器客户端列表。（请参阅第 B-33 页的“配置外部 RADIUS 服务器以识别 9160 G2”。）
2. 将产品名称配置为使用 RADIUS 服务器（通过提供 RADIUS 服务器 IP 地址作为“IEEE 802.1x”安全模式设置的组成部分）。
3. 如本节中所述，将无线客户端配置为使用 IEEE 802.1x 安全性和“Smart Card or other Certificate”（智能卡或其他证书）。
4. 如第 B-37 页的“获取客户端的 TLS-EAP 证书”中所述获取此客户端的证书。

如果您将产品名称配置为将 IEEE 802.1x 安全模式与外部 RADIUS 服务器配合使用
...

Basic Settings	<h3>Modify Internal Network security settings</h3> <div><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</div> <div>Mode: IEEE802.1x</div> <div><div><input type="checkbox"/> Use internal radius server</div><div>Radius IP: 10.128.14.14</div><div>Radius Key: ●●●●●●●●</div><div><input checked="" type="checkbox"/> Enable radius accounting</div></div> <div>Update</div>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	

...则如下所述在各个客户端上配置使用证书身份验证的 IEEE 802.1x 安全性：



1. 在 *Network Properties*（网络属性）对话框的 *Association*（关联）选项卡上配置以下设置。

表 B.7 关联设置

<i>Network Authentication</i> (网络身份验证)	Open（开放式）
<i>Data Encryption</i> (数据加密)	WEP 注： RC4 流密码用于加密帧主体及各个 802.11 帧的循环冗余校验 (CRC)。此加密算法与静态 WEP 使用的算法相同；因此，此模式下在客户端上配置的数据加密法是 WEP。
<i>This key is provided for me automatically</i> (自动为我提供密钥)	启用（单击以选中）此选项。

2. 在 *Authentication*（身份验证）选项卡上配置这些设置。

表 B.8 身份验证设置

<i>Enable IEEE 802.1x authentication for this network</i> (为此网络启用 IEEE 802.1x 身份验证)	启用（单击以选中）此选项。
<i>EAP Type</i> （EAP 类型）	选择 Smart Card or other Certificate (智能卡或其他证书)。

3. 单击 **Properties**（属性）显示 *Smart Card or other Certificate Properties*（智能卡或其他证书属性）对话框，并启用 **Validate server certificate**（验证服务器证书）选项。

表 B.9 智能卡或其他证书属性设置

<i>Validate server certificate</i> (验证服务器证书)	启用此选项（单击以选中该方框）。
<i>Certificates</i> （证书）	在显示的证书列表中，为该客户端选择 证书 。

在所有对话框上单击 **OK**（确定）并保存您的更改。

4. 要完成客户端配置，您现在必须从 RADIUS 服务器获取证书，并将其安装到此客户端上。有关如何操作的信息，请参阅第 B-37 页的“获取客户端的 TLS-EAP 证书”。

通过使用证书的 IEEE 802.1x 客户端连接到无线网络

IEEE 802.1x 客户端现应能够使用其 TLS 证书连接到接入点。连接时系统会使用您已安装的证书，因此不会提示您输入登录信息。该证书自动发送至 RADIUS 服务器进行身份验证和授权。

B.7 在客户端上配置 WPA/WPA2 Enterprise (RADIUS) 安全性

使用 *远程身份验证拨号用户服务 (WPA2)* 的 *Wi-Fi 受保护访问 2 (RADIUS)* 实施 Wi-Fi 联盟 IEEE **802.11h** 标准，包括 *高级加密标准 (AES)*、*计数器模式/CBC-MAC 协议 (CCMP)* 和 *临时密钥完整性协议 (TKIP)* 机制。此模式要求使用 RADIUS 服务器对用户进行身份验证。

此安全模式还向后兼容仅支持原始 **WPA** 的无线客户端。

当您在接入点上配置 WPA/WPA2 Enterprise (RADIUS) 安全模式时，您可以选择使用内置身份验证服务器或您提供的外部 RADIUS 服务器。

产品名称内置身份验证服务器支持称为“EAP/PEAP”的受保护的扩展身份验证协议 (EAP)，以及为基于 Windows 的计算机和接入点等网络设备间的点对点 (PPP) 连接提供身份验证的 *Microsoft 质询握手身份验证协议第 2 版 (MSCHAP V2)*。

因此，如果您将网络（接入点）配置为使用安全模式，并选择内置身份验证服务器，则必须将客户端工作站配置为使用 WPA/WPA2 Enterprise (RADIUS) 和 EAP/PEAP。

如果该网络（接入点）配置为将此安全模式用于外部 RADIUS 服务器，则必须将客户端工作站配置为使用 WPA/WPA2 Enterprise (RADIUS) 以及为您的 RADIUS 服务器配置使用的安全协议。

B.7.1 使用 EAP/PEAP 的 WPA/WPA2 Enterprise (RADIUS) 客户端

产品名称上的内置身份验证服务器使用称为“EAP/PEAP”的受保护的扩展身份验证协议 (EAP)。

- 如果您在产品名称上使用具有“WPA/WPA2 Enterprise (RADIUS)”安全模式的内置身份验证服务器，则需要将无线客户端设置为使用 PEAP。
- 此外，您还需要拥有一台使用 EAP/PEAP 的外部 RADIUS 服务器。如果这样，您需要：
 1. 将产品名称添加到 RADIUS 服务器客户端列表。
 - 并且
 2. 将您的“WPA/WPA2 Enterprise (RADIUS)”无线客户端配置为使用 PEAP。



注释: 在以下示例中, 假设您使用 9160 G2 无线网关附带的内置身份验证服务器。
如果您在使用外部 RADIUS 服务器的 AP 客户端上设置 EAP/PEAP, 则客户端配置流不同于本示例, 尤其是在证书验证方面。

如果您将产品名称配置为使用 WPA/WPA2 企业版 (RADIUS) 安全模式, 并使用内置身份验证服务器或使用 EAP/PEAP 的外部 RADIUS 服务器 ...

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Modify Internal Network security settings

☒ Broadcast SSID

☐ Station Isolation

Mode:

WPA Enterprise

WPA Versions:

☒ WPA

☒ WPA2

☐ Enable pre-authentication

Cipher Suites:

☒ TKIP

☐ CCMP (AES)

☒ Use internal radius server

Radius IP:

10.128.14.14

Radius Key:

••••••••

☒ Enable radius accounting

Update

...首先, 设置接入点上的用户帐户 (转至 *User Management* (用户管理) 选项卡)

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Manage user accounts

User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions.
Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

☐ Edit

Username

Real name

Status

☐ [Edit]

Darren

Darren Stevens

enabled

☐ [Edit]

Samantha

Samantha Stevens

enabled

Selected users:

Enable

Disable

Remove

[backup or restore the user database]

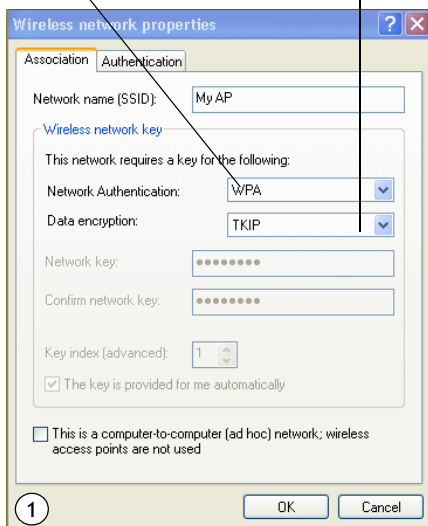
Not Clustered

0 Access Points

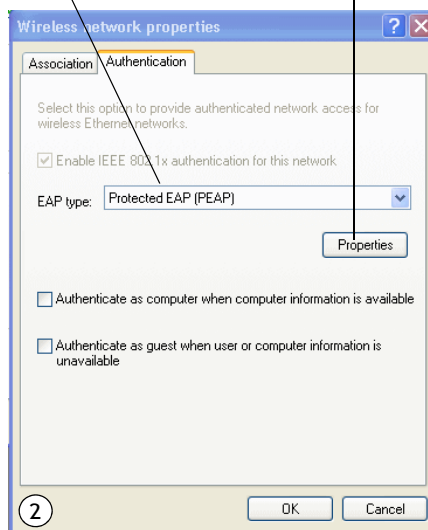
2 User Accounts

...然后, 如下所述在各个客户端上配置使用 PEAP 身份验证的 WPA 安全性。

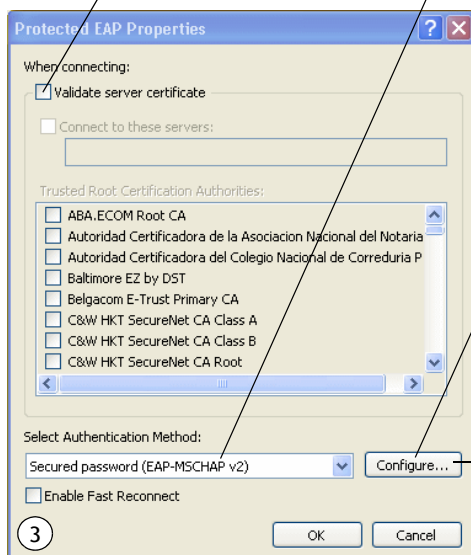
选择 WPA
选择 TKIP 或 AES 作为
Data Encryption (数据加密) 模式



选择 Protected EAP (PEAP) (受保护的 EAP (PEAP))
... 然后, 单击 Properties (属性)



禁用 Validate server certificate (验证服务器证书)
选择 Secured password (EAP-MSCHAP v2) (安全密码 (EAP-MSCHAP v2))



... 然后, 单击 Configure (配置)



1. 在 *Network Properties*（网络属性）对话框的 *Association*（关联）和 *Authentication*（身份验证）选项卡上，配置以下设置。

表 B.10 关联设置

<i>Network Authentication</i> (网络身份验证)	WPA
<i>Data Encryption</i> (数据加密)	TKIP 或 AES ，具体取决于在接入点上是如何配置此选项的。 注： 将接入点上的加密套件设为 Both （二者）时，具有有效 TKIP 密钥的 TKIP 客户端和具有有效 CCMP (AES) 密钥的 AES 客户端能够与该接入点进行关联。有关更多信息，请参阅接入点上的联帮助。

2. 在 *Authentication*（身份验证）选项卡上配置此设置。

表 B.11 身份验证设置

<i>EAP Type</i> (EAP 类型)	选择 Protected EAP (PEAP) （受保护的 EAP (PEAP)）
--------------------------	--

3. 单击 **Properties**（属性）将显示 *Protected EAP Properties*（受保护的 EAP 属性）对话框，并配置以下设置。

表 B.12 受保护的 EAP 属性设置

<i>Validate server certificate</i> (验证服务器证书)	禁用 此选项（单击以取消选中该方框）。 注： 此示例假设您在 AP 上使用内置身份验证服务器。如果您在使用外部 RADIUS 服务器的 AP 客户端上设置 EAP/PEAP，则需要验证证书并选择证书，具体取决于您的基础设施。
<i>Select Authentication Method</i> (选择身份验证方法)	选择 Secured password (EAP-MSCHAP v2) （安全密码 (EAP-MSCHAP v2)）。

4. 单击 **Configure**（配置）显示 *EAP MSCHAP v2 Properties*（EAP MSCHAP v2 属性）对话框。

在此对话框上，**禁用**（单击以取消选中）*Automatically use my Windows logon name ...*（自动使用我的 Windows 登录名...）选项，让系统在登录时提示输入用户名和密码。

在所有对话框（第一个显示的是 *EAP MSCHAP v2 Properties*（EAP MSCHAP v2 属性）对话框）上单击 **OK**（确定）可关闭对话框并保存您的更改。

通过 WPA/WPA2 企业版 (RADIUS) PEAP 客户端登录到无线网络

“WPA/WPA2 企业版 (RADIUS)” PEAP 客户端现应能够与接入点关联。系统将提示客户端用户输入用户名和密码，以对网络进行身份验证。

B.7.2 使用 EAP-TLS 证书的 WPA/WPA2 Enterprise (RADIUS) 客户端

可扩展身份验证协议 (EAP) 传输层安全性 (TLS) 或 EAP-TLS 是支持使用智能卡和证书的身份验证协议。如果您的网络上有一台外部 RADIUS 服务器提供支持，则可以选择将 EAP-TLS 用于 WPA/WPA2 Enterprise (RADIUS) 和 IEEE 802.1x 模式。



注释: 如果您想要将 IEEE 802.1x 模式与 EAP-TLS 证书结合使用进行客户端的身份验证和授权，则必须有一台外部 RADIUS 服务器和一个公钥基础设施 (PKI)，包括在的网络上配置的服务器 — 证书颁发机构 (CA)。RADIUS 服务器、PKI 和 CA 服务器的配置不在此文档的介绍范围内。请参阅这些产品的说明文档。

Microsoft Windows PKI 软件的 Web 上提供一些良好的起点文章，包括：

“如何安装/卸载 Windows 2000 的公钥证书颁发机构”，地址：

<http://support.microsoft.com/default.aspx?scid=kb:zh-cn:231881>，以及

“如何配置证书服务器”，地址：

<http://support.microsoft.com/default.aspx?scid=kb:zh-cn:318710#3>。

要使用此安全类型，必须执行以下操作：

1. 将产品名称添加到 RADIUS 服务器客户端列表。（请参阅第 B-33 页的“配置外部 RADIUS 服务器以识别 9160 G2”。）
2. 将产品名称配置为使用 RADIUS 服务器（通过提供 RADIUS 服务器 IP 地址作为“WPA/WPA2 Enterprise [RADIUS]”安全模式设置的组成部分）。
3. 如本节中所述，将无线客户端配置为使用 WPA 安全性和“Smart Card or other Certificate”（智能卡或其他证书）。
4. 如第 B-37 页的“获取客户端的 TLS-EAP 证书”中所述获取此客户端的证书。

如果您将产品名称配置为将 WPA/WPA2 Enterprise (RADIUS) 安全模式与外部 RADIUS 服务器配合使用 ...

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☒ WPA ☒ WPA2
☐ Enable pre-authentication

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☒ Enable radius accounting

Update

...然后，如下所述在各个客户端上配置使用证书身份验证的 WPA 安全性。

选择 WPA

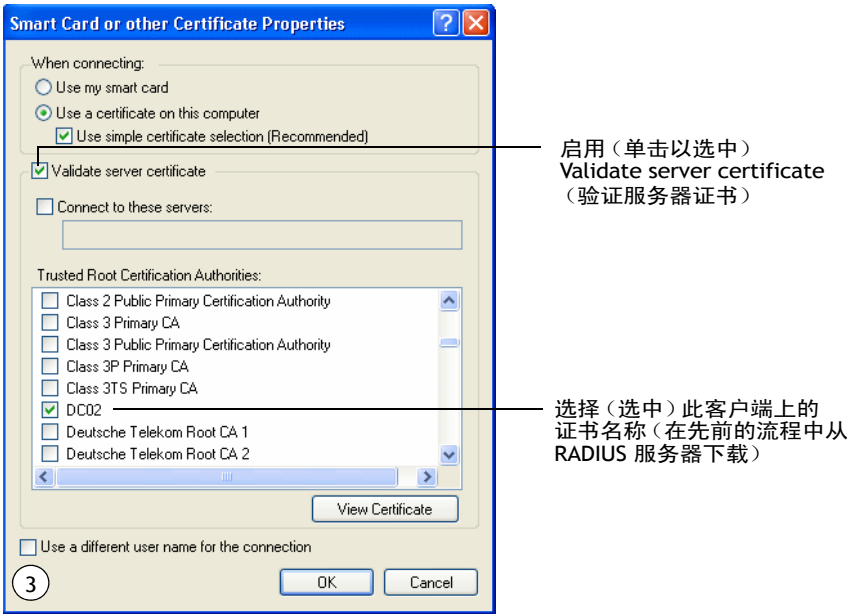
选择 TKIP 或 AES 作为 Data Encryption (数据加密) 模式

选择 Smart Card or other Certificate (智能卡或其他证书), 启 Authenticate as computer (作为计算机进行身份验证 ...)

... 然后, 单击 Properties (属性)

1

2



1. 在 *Network Properties*（网络属性）对话框的 *Association*（关联）选项卡上配置以下设置。

表 B.13 关联设置

<i>Network Authentication</i> (网络身份验证)	WPA
<i>Data Encryption</i> (数据加密)	TKIP 或 AES ，具体取决于在接入点上是如何配置此选项的。 注： 将接入点上的加密套件设为“Both”（二者）时，具有有效 TKIP 密钥的 TKIP 客户端和具有有效 CCMP (AES) 密钥的 AES 客户端能够与该接入点进行关联。有更多信息，请参阅接入点上的联机帮助。

2. 在 *Authentication*（身份验证）选项卡上配置这些设置。

表 B.14 身份验证设置

<i>Enable IEEE 802.1x authentication for this network</i> (为此网络启用 IEEE 802.1x 身份验证)	启用（单击以选中）此选项。
<i>EAP Type</i> (EAP 类型)	选择 Smart Card or other Certificate (智能卡或其他证书)。

- 3. 单击 **Properties** （属性）显示 *Smart Card or other Certificate Properties* （智能卡或其他证书属性）对话框，并启用 **Validate server certificate** （验证服务器证书）选项。

表 B.15 智能卡或其他证书属性设置

Validate server certificate （验证服务器证书）	启用此选项 （单击以选中该方框）。
Certificates （证书）	在显示的证书列表中，为该客户端选择 证书 。

在所有对话框上单击 **OK** （确定）并保存您的更改。

- 4. 要完成客户端配置，您现在必须从 RADIUS 服务器获取证书，并将其安装到此客户端上。有关如何操作的信息，请参阅第 B-37 页的 “获取客户端的 TLS-EAP 证书”。

通过使用证书的 WPA 客户端登录到无线网络

WPA 客户端现应能够使用其 TLS 证书连接到接入点。连接时系统会使用您已安装的证书，因此不会提示您输入登录信息。该证书自动发送至 RADIUS 服务进行身份验证和授权。

B.8 在客户端上配置 WPA/WPA2 Personal (PSK) 安全性

使用 *预共享密钥(PSK) 的 Wi-Fi 受保护访问(WPA)* 是 Wi-Fi 联盟的 IEEE 802.11i 子集，包括 *临时密钥完整性协议(TKIP)*、*高级加密算法(AES)* 和 *计数器模式/CBC-MAC 协议(CCMP)* 机制。PSK 使用预共享密钥，对客户端凭据进行初始检查。

如果您将产品名称配置为使用 WPA/WPA2 Personal (PSK) 安全模式 ...

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Personal

WPA Versions: ☒ WPA ☐ WPA2

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

Key: reoreore

Update

...然后, 如下所述在各客户端上配置 WPA/WPA2 Personal (PSK) 的安全性。

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

选择 WPA-PSK。

选择 TKIP 或 AES 作为 Data Encryption (数据加密) 模式。

输入与设定为传输密钥索引的位置的匹配的网络密钥 (重新键入以确认)。

表 B.16 关联设置

<i>Network Authentication</i> (网络身份验证)	WPA-PSK
<i>Data Encryption</i> (数据加密)	TKIP 或 AES，具体取决于在接入点上是如何配置此选项的。 注： 将接入点上的加密套件设为 Both （二者）时，具有有效 TKIP 密钥的 TKIP 客户端和具有有效 CCMP (AES) 密钥的 AES 客户端能够与该接入点进行关联。有关更多信息，请参阅接入点上的联帮助。
<i>Network Key</i> (网络密钥)	提供您在接入点的 Security（安全）设置上为使用的加密套件输入的密钥。 例如，如果将接入点上的密钥设为使用 TKIP 密钥 “012345678”，则 TKIP 客户端指定和网络密钥相同的字符串。
<i>The key is provided for me automatically</i> (自动为我提供密钥)	根据其他设置，应自动禁用此方框。

表 B.17 身份验证设置

<i>Enable IEEE 802.1x authentication for this network</i> (为此网络启用 IEEE 802.1x 身份验证)	确保 禁用 （取消选中）IEEE 802.1x 身份验证。 (将加密模式设置为 WEP，会自动禁用身份验证。)
---	---

在 Wireless Network Properties（无线网络属性）对话框上单击 **OK**（确定），即可将其关闭并保存您的更改。

通过 WPA-PSK 客户端连接至无线网络

WPA-PSK 客户端现应能够与接入点关联并进行身份验证。系统不会提示客户端输入密钥。当您连接时，自动使用在客户端安全性设置上配置的 TKIP 或 AES 密钥。

B.9 配置外部 RADIUS 服务器以识别 9160 G2

在网络上运行的外部远程身份验证拨号用户服务器 (RADIUS) 支持在公钥基础设施 (PKI) 中将 EAP-TLS 智能卡/证书分发至客户端，并进行 EAP-PEAP 用户帐户设置和身份验证。外部 RADIUS 服务器是指接入点外部的身份验证服务器。这是用于区分您在产品名称上使用网络 RADIUS 服务器和内置身份验证服务器的场景。

本小节提供配置外部 RADIUS 服务器的示例，目的是从配置为“WPA/WPA2 Enterprise (RADIUS)”或“IEEE 802.1x”安全模式的特定产品名称的无线客户端验证和授权 TLS-EAP 证书。本小节旨在提供此流程的示例，但由于您使用的 RADIUS 服务器和配置方式的不同，流程会有所区别。在本示例，我们使用 Microsoft Windows 2003 服务器附带的 Internet 身份验证服务。



注释：本文档不介绍如何在 RADIUS 服务器上设置管理用户。在本示例中，我们假设您已配置了 RADIUS 服务器用户帐户。您需要有 RADIUS 服务器用户名和密码，能执行此流程以及说明如何在无线客户端上获取和安装证书的流程。请查阅 RADIUS 服务器的文档，了解有关设置用户帐户的信息。

此流程旨在将产品名称识别为 RADIUS 服务器的“客户端”。RADIUS 服务器可以处理 AP 的无线客户端的身份验证和授权。每个接入点都需要执行此流程。如果您计划将多个接入点用于外部 RADIUS 服务器，需要对各个 AP 执行以下步骤。

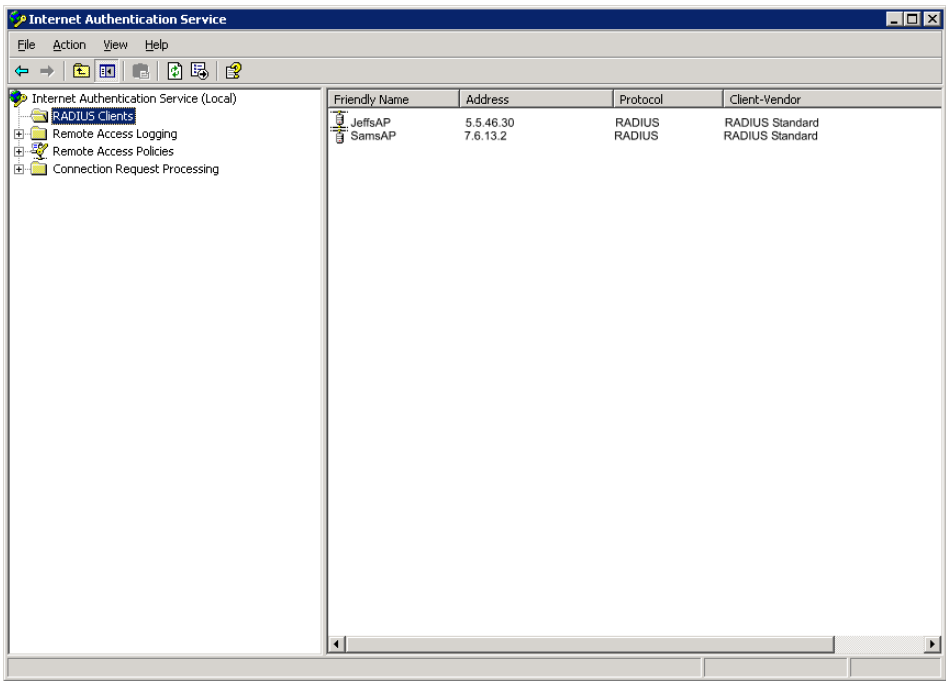
请记住，您需要向 RADIUS 服务器提供的有关接入点的信息与接入点上的设置（安全性）相对应，反之亦然。您应已向 AP 提供了 RADIUS 服务器的 IP 地址，在接下来的步骤中，您将需要向 RADIUS 服务器提供接入点的 IP 地址。在 AP 上提供的 RADIUS 密钥是您需要向 RADIUS 服务器提供的“共享密钥”。

Basic Settings	<h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: IEEE802.1x</p> <p><input type="checkbox"/> Use internal radius server</p> <p>Radius IP: 10.128.14.14</p> <p>Radius Key:</p> <p><input checked="" type="checkbox"/> Enable radius accounting</p> <p>Update</p>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	



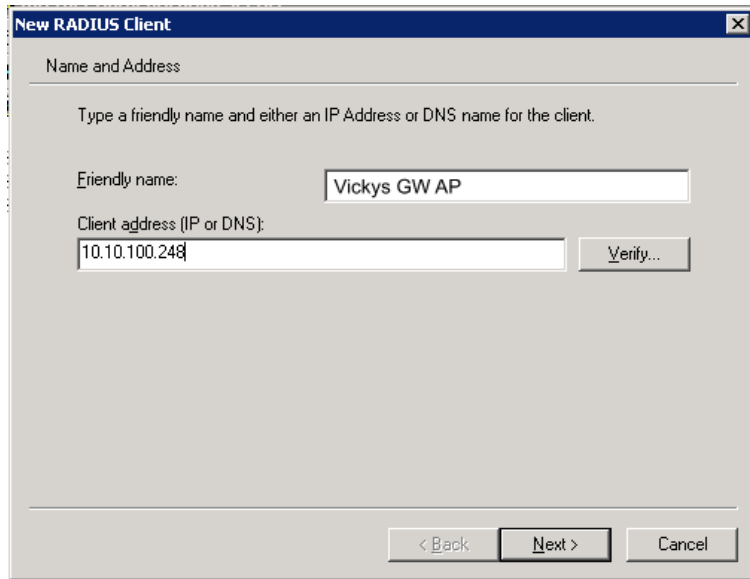
注释： 根据 IP 地址和 UDP 端口号识别 RADIUS 服务器， 以使用它提供的不同的服务。 在当前版本的 9160 G2 无线网关上， 该接入点使用的 RADIUS 服务器用户数据报协议 (UDP) 端口不可配置。（对 9160 G2 无线网关进行硬编码， 以使用 RADIUS 服务器 UDP 端口 1812 进行身份验证， 使用端口 1813 进行计费。）

1. 登录到托管 RADIUS 服务器并显示 Internet 身份验证服务的系统。



2. 在左侧面板中，右键单击 **RADIUS Clients** （RADIUS 客户端）节点， 并从弹出的菜单中选择 **New** （新建） > **Radius Client** （Radius 客户端）。

3. 在 *New RADIUS Client* wizard（新建 RADIUS 客户端）向导的第一个屏幕上，提供您希望客户端连接到的产品名称的相关信息：
 - 接入点的逻辑（友好）名称。（您可能想要使用 DNS 名称或位置。）
 - 接入点的 IP 地址。单击 **Next**（下一步）。



New RADIUS Client

Name and Address

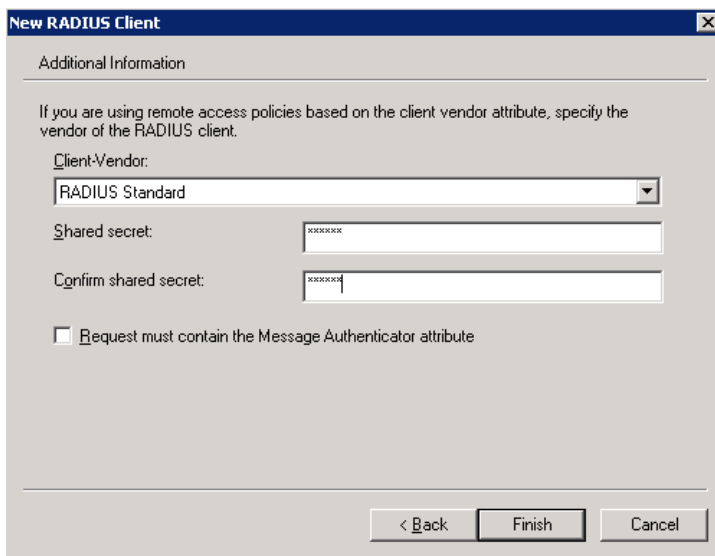
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: Vickys GW AP

Client address (IP or DNS): 10.10.100.248 Verify...

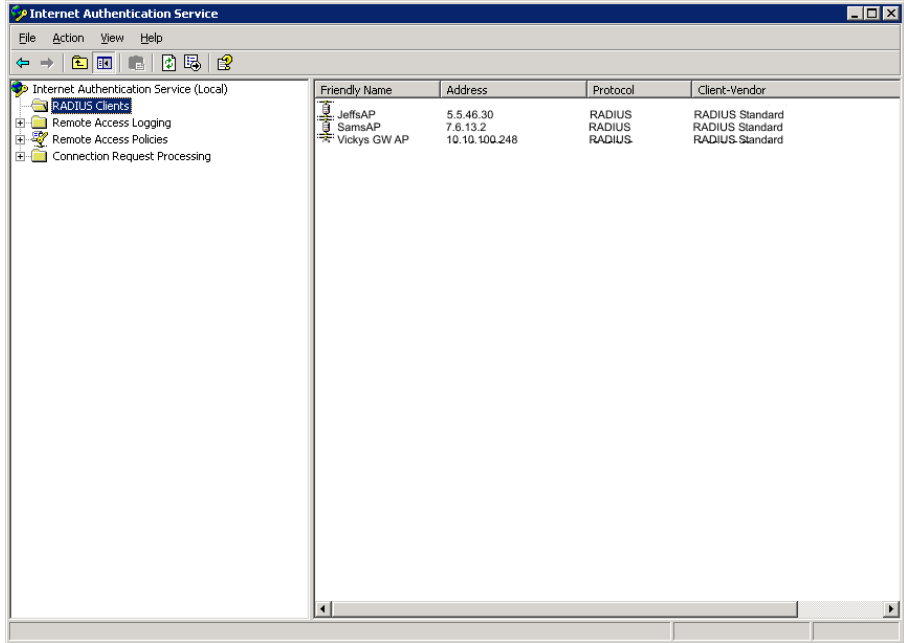
< Back Next > Cancel

4. 在 *Shared secret* （共享密钥）中，输入您提供给接入点的 **RADIUS 密钥**（在 *Security* （安全性）页面上）。重新键入密钥进行确认。



The image shows a Windows-style dialog box titled "New RADIUS Client". It has a close button (X) in the top right corner. The dialog is divided into sections. The first section is titled "Additional Information". Below this, there is a text instruction: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." This is followed by a label "Client-Vendor:" and a dropdown menu currently showing "RADIUS Standard". Below that are two text input fields. The first is labeled "Shared secret:" and contains several "x" characters. The second is labeled "Confirm shared secret:" and also contains "x" characters. At the bottom of the main content area, there is a checkbox labeled "Request must contain the Message Authenticator attribute", which is currently unchecked. At the very bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

5. 单击 **Finish**（完成）。接入点现在显示为身份验证服务器的客户端。



B.10 获取客户端的 TLS-EAP 证书



注释: 如果您想要将 IEEE 802.1x 模式与 EAP-TLS 证书结合使用进行客户端的身份验证和授权, 则必须有一台外部 RADIUS 服务器和一个公钥基础设施 (PKI), 包括在的网络上配置的服务器 — 证书颁发机构 (CA)。RADIUS 服务器、PKI 和 CA 服务器的配置不在此文档的介绍范围内。请参阅这些产品的说明文档。

Microsoft Windows PKI 软件的 Web 上提供一些良好的起点文章, 包括:

“如何安装/卸载 Windows 2000 的公钥证书颁发机构”, 地址:

<http://support.microsoft.com/default.aspx?scid=kb:zh-cn:231881?> 以及

“如何配置证书服务器”, 地址:

<http://support.microsoft.com/default.aspx?scid=kb:zh-cn:318710#3>。

配置为将 “WPA/WPA2 Enterprise (RADIUS)” 或 “IEEE 802.1x” 安全模式” 用于支持 TLS-EAP 证书的外部 RADIUS 服务器的无线客户端必须从 RADIUS 服务器获取 TLS 证书

这是在将上述模式用于证书的各个客户端上必须完成的初始一次性步骤。在此流程中，我们使用 Microsoft 证书服务器为例。

要获取客户端的证书，请执行以下步骤。

1. 在 Web 浏览器中转至以下 URL:

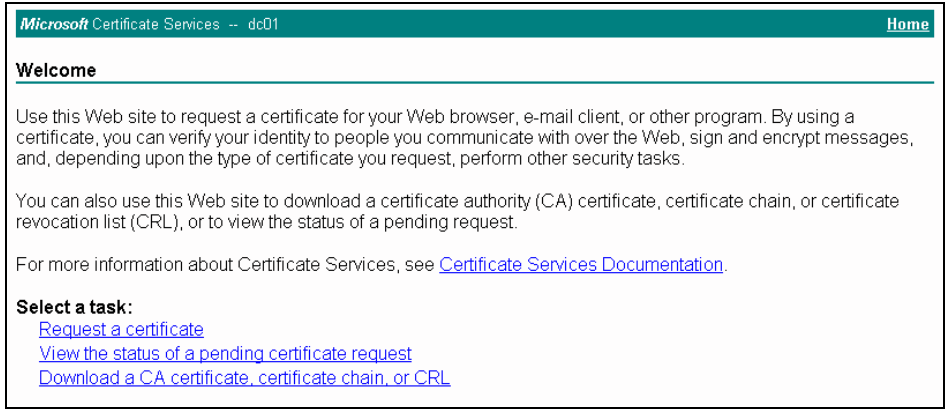
<https://IPAddressOfServer/certsrv/>

其中，*IPAddressOfServer* 是外部 RADIUS 服务器的 IP 地址，或证书颁发机构 (CA) 的 IP 地址，具体取决于基础设施的配置。

2. 单击 **Yes** (是) 继续保护服务器 Web 页面的安全。



浏览器中显示证书服务器的欢迎界面。



3. 单击 **Request a certificate**（请求证书）后，会收到 RADIUS 服务器的登录提示。
4. 提供有效的 **user name**（用户名）和 **password**（密码），以访问 RADIUS 服务器。

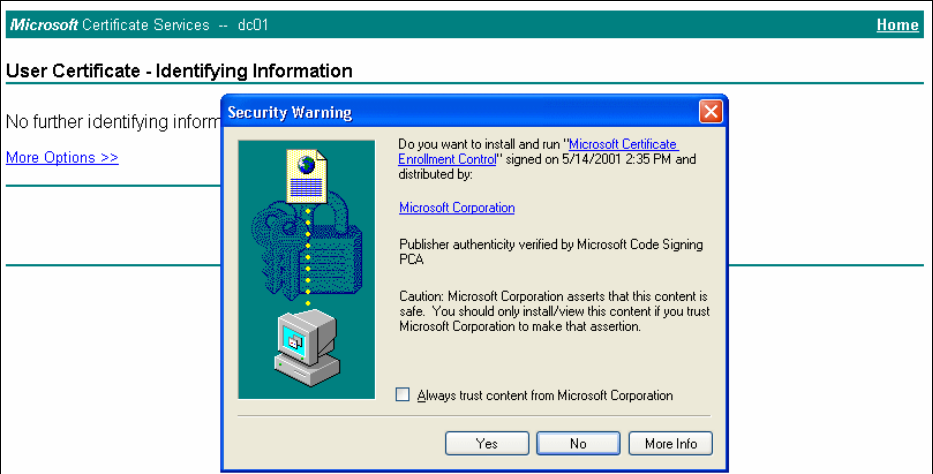


注释: 您在此处需要提供的用户名和密码是用于访问 RADIUS 服务器，且您已经配置了 RADIUS 服务器的用户帐户。本文档不介绍如何在 RADIUS 服务器上设置管理户帐户。请参阅 RADIUS 服务器的文档，了解操作流程。

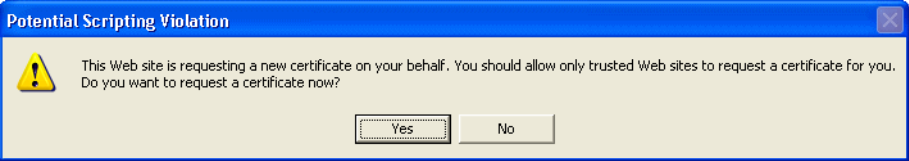
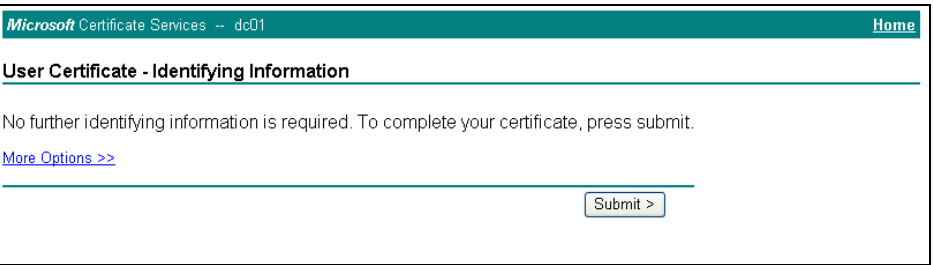
5. 在显示的下一页上单击 **User Certificate**（用户证书）。



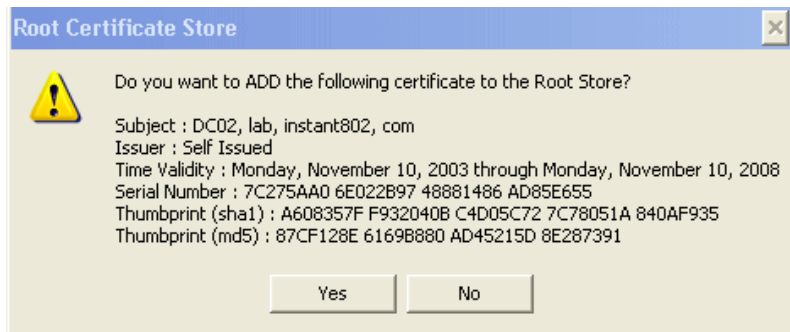
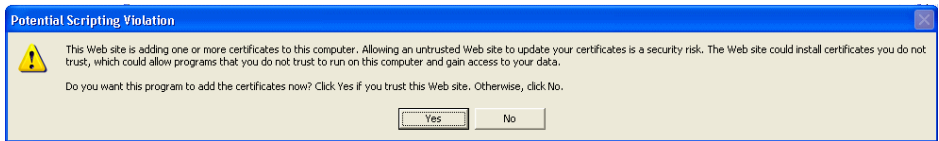
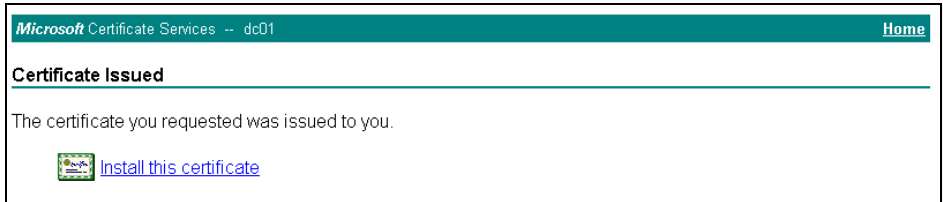
6. 单击对话框上显示的 **Yes**（是）以安装证书。



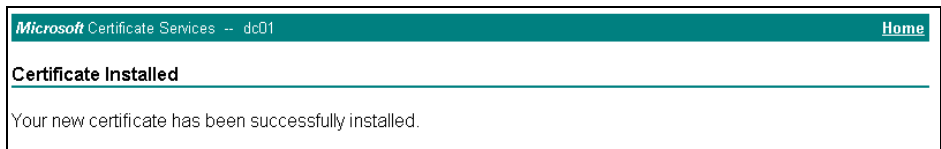
7. 单击 **Submit**（提交）完成并单击 **Yes**（是）在弹出的对话框上确认提交。



- 单击 **Install this certificate**（安装此证书），在客户端工作站上安装新颁发的证书。（此外，在弹出的窗口中单击 **Yes**（是），确认安装并添加证书到根存储。）



此时显示一条成功消息，表明证书现已安装到客户端上。



B.11 配置 RADIUS 服务器用于 VLAN 标记

VLAN 是一台交换机上的一组端口或不同交换机上的一组端口。动态 VLAN 允许您将用户分配至 VLAN，并自动切换，以使用此信息自动配置交换机上的端口。

通常根据用户的身份选择 VLAN。作为身份验证的一部分，RADIUS 服务器会通知 NAS（例如，接入点）选定的 VLAN。使用此设置，动态 VLAN 的用户可以从一位置移动到另一个位置，无需干预也无需对交换机进行任何更改。

使用产品名称时，如果用户选择使用外部 RADIUS 服务器（在 *Security*（安全性）页面上配置），则外部 RADIUS 服务器将尝试验证用户的身份。用户的身份验证凭据传递至 RADIUS 服务器。如果这些凭据有效，则 NAS 将端口置为 RADIUS 身份验证服务器表示的 VLAN。

B.11.1 配置 RADIUS 服务器

需要将 RADIUS 服务器配置为在 Access-Accept（访问接受）消息中使用 Tunnel（隧道）属性，才能通知接入点有关选定的 VLAN。在 RFC 2868 中定义这些属性，RFC 3580 中指定动态 VLAN。

如果使用 FreeRADIUS 服务器，则可以在用户文件中设置以下选项，以添加必要的属性。

```
example-user  Auth-Type :=EAP,  User-Password == "password"  
               Tunnel-Type = 13,  
               Tunnel-Medium-Type = 6,  
               Tunnel-Private-Group-ID = 7
```

Tunnel-Type and Tunnel-Medium-Type 对所有工作站使用相同的值。Tunnel-Private-Group-ID 是选定的 VLAN ID，但该 ID 对每个用户是不同的。

故障排除

C.1 无线分布系统 (WDS) 问题和解决方案 45

C.2 集群恢复 45

 C.2.1 重启或重置接入点 46

本节提供有关如何解决您在多个集群接入点所服务的网络上更新网络配置的过程中可能遇到的常见问题的信息。

C.1 无线分布系统 (WDS) 问题和解决方案

如果您在配置 WDS 链路时遇到问题，请务必阅读第 204 页的“配置 WDS 设置”中的注意事项和警告。为方便起见，在此处重新印刷了这些注意事项。管理员在设置 WDS 时最常见的问题是忘记将链路中的接入点设为相同的无线电道和 IEEE 802.11 模式。以下注意事项中列出了前提条件及其他条件。



注释:

使用 WDS 时，确保在参与 WDS 链路的**两个**接入点上配置 WDS 设置。

任何一对接入点之间只能有一个 WDS 链路。也就是说，在特定接入点的 WDS 页面上，远程 MAC 地址仅显示一次。

参与 WDS 链路的两个接入点必须处在同一个无线电信道上，并使用相同的 IEEE 802.11 模式。（请参阅第 167 页的“配置无线通信设置”，了解有关配置无线通信模式和信道的信息。）有关 IEEE 802.11h 的更多信息，请参阅第 146 页的“802.11h 监管域控制”。

确保启用生成树协议 (STP)，通过 WDS 桥接或有线（以太网）连接和 WDS 桥接组合防止无限循环及路径冗余。如果启用 STP，您可以使用 WDS 创建备份链路。如果禁用 STP，请谨记以下规则：

- 任何两个接入点只能通过一个路径连接，WDS 桥接（无线）或以太网连接（有线），但不能同时使用两个路径。
- 请勿创建“备份”链路。
- 如果您在通过任何以太网或 WDS 链路组合的任何一对 AP 之间跟踪到超过一个路径，则您有一个循环。
- 您只能扩展或桥接内部或访客网络，但不能同时扩展或桥接这两个网络。

C.2 集群恢复

如果集群中的接入点不同步，或其中一个接入点无法加入集群或从集群中删除，则建议使用以下方法恢复集群。

C.2.1 重启或重置接入点

下面按您应该尝试的顺序介绍了这些恢复方法。除最后一个案例（停止集群）外，您只需重置或重启配置与其他集群成员不同步或无法加入集群或从群中删除的接入点即可。

- 通过断电后再打开电源（按下电源按钮 OFF（关闭），再按下 ON（打开）），实际重启接入点。
- 从管理 UI 重置接入点。要执行此操作，请转至 <http://IPAddressOfAccessPoint>，导航至 **Reset Configuration**（重置配置），然后单击 **Reset**（重置）按钮。（AP 的 IP 地址显示在任何集群成员的 Cluster（集群）> Access Points（接入点）页面上。）

术语表

0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0-9

802

IEEE 802 (*IEEE 标准 802-2001*) 是一系列适用于通过 *LAN* 进行点对点通信的标准。这些技术使用共享介质，且广播的信息可供所有站点接收。提供的基本通信功能均基于数据包。基本传输单位是一系列八位字节的数据，根据 *LAN* 类型，可以是范围内的任何长度。

在 802 系列 *IEEE* 标准中，定义了桥接、管理和安全协议。

802.1x

IEEE 802.1x (*IEEE 标准 802.1x-2001*) 标准适用于使用被称为 *EAP Encapsulation Over LAN* (EAPOL) 的协议，通过 **802.11** 无线网络进行的 *EAP* 数据包的传输。它建立起了支持多种身份验证方法的框架。IEEE 802.1x 验证用户的身份而不是机器的身份。

802.2

IEEE 802.2 (*IEEE 标准 802.2.1998*) 定义了用于 **802** 系列标准的 *LLC* 层。

802.3

IEEE 802.3 (*IEEE 标准 802.3-2002*) 定义了使用 *CSMA/CA* 的网络的 *MAC* 层。*以太网* 是此类网络的示例。

802.11

IEEE 802.11 (*IEEE 标准 802.11-1999*) 是媒体访问控制 (*MAC*) 和物理层 (*PHY*) 规格, 适用于本地区域内固定、便携和移动式工作站的无线连接。它使用 2.4 GHz ISM 频段中的直序扩频 (DSSS), 支持 1 和 2 Mbps 的原始数据速率。该标于 1997 年正式采用, 但已逐渐被 *802.11b* 取代。

IEEE 802.11 一般还被用于引用无线局域网的 *IEEE* 标准系列。

802.11a

IEEE 802.11a (*IEEE 标准 802.11a-1999*) 是 *PHY* 标准, 使用正交频分复用技术 (OFDM) 在 5 GHz U-NII 频段内运行。它支持 6 到 54Mbps 的数据速率。

802.11a Turbo

IEEE 802.11a Turbo 是 *Atheros Communications* 提供的 *802.11a* 标准的专有变体。它支持 6 到 108Mbps 的加速数据速率。Atheros Turbo 5 GHz 是 IEEE 802.11a Turbo 模式。Atheros Turbo 2.4 GHz 是 IEEE 802.11g Turbo 模式。

802.11b

IEEE 802.11b (*IEEE 标准 802.11b-1999*) 是初始 *802.11 PHY* 的增强版, 包括 5.5 Mbps 和 11 Mbps 的数据速率。它使用 2.4 GHz ISM 频段中的直序扩频 (DSSS) 或跳频扩频 (FHSS) 及补码键控 (CCK), 以提供更高的数据速率。它支持 1 到 11Mbps 的数据速率。

802.11d

IEEE 802.11d 定义了 IEEE 802.11 无线 LAN 在任何国家/地区运行的标准规则, 且无需重新配置。提供各个国家/地区的 PHY 要求, 例如跳频表、可接受信道和功率级别。在接入点上启用 IEEE 802.11d 支持后, 作为 AP 信标的组成部分, AP 会广播其运行所在的国家/地区。客户端工作站将会使用这些信息。对于在 5GHz IEEE 802.11a 频段运行的 AP, 这一点尤其重要, 因为每个国家/地区使用的频率各不相同。

802.11e

IEEE 802.11e 是正在开发的 *IEEE* 标准，通过增强 *MAC* 来支持 *QoS*。它提供一种优先分配 *802.11* 中的流量的机制。它定义了仲裁帧间间隔允许的更改，最小和最大竞争窗口尺寸，以及大量数据的最大长度（单位：kμsec）。

IEEE 802.11e 仍然是草稿 *IEEE* 标准（最近的版本是 2003 年 6 月推出的 D5.0）。当前可用的 802.11e 子集是 *无线多媒体功能增强 (WMM)* 标准。

802.11f

IEEE 802.11f（*IEEE 标准 802.11f-2003*）标准定义了扩展服务集 (*ESS*) 中的接入点（无线通信中心）的接入点互连协议 (*IAPP*)。该标准定义了接入点传达其移动工作站的关联和重新关联的方式。

802.11g

IEEE 802.11g（*IEEE 标准 802.11g-2003*）在 2.4 GHz 频段运行，是 *802.11b PHY* 更高速度的扩展（高达 54 Mbps）。它使采用正交频分复用技术 (OFDM)。它支持 1 到 54Mbps 的数据速率。

802.11h

IEEE 802.11h 是用于解决 802.11a 经常会出现的干扰问题的标准。使用两个方案最大程度地减少 802.11h 的干扰，分别是发射功率控制 (TPC) 和动态频率选择 (DFS)。DFS 检测到同一频率上存在其他 AP，并将这些 AP 重定向至另一个信道。TCP 降低了该 AP 的网络频率输出功率，因此减少了任何干扰的可能性。欧洲、日本和美国均要求达到此标准。

802.11i

IEEE 802.11i 是针对无线局域网 (*WLAN*) 的安全性的综合性 *IEEE* 标准，引入了 *Wi-Fi 受保护访问 2 (WPA2)*。它定义了 *MAC* 层的增强功能，以克服 *WEP* 的某些弱点。它采用的加密技术比原始 *Wi-Fi 受保护访问 (WPA)* 更强大，例如高级加密标准 (*AES*)。

原始 **WPA** 被视为 802.11i 的子集，使用 *临时密钥完整性协议 (TKIP)* 进行加密。WPA2 提供与支持原始 WPA 的产品的向后兼容性。

IEEE 802.11i / WPA2 于 2004 年 6 月完成制定并通过批准。

802.11j

IEEE 802.11j 实现了使用 4.9 和 5 GHz 无线通信频段的芯片组的标准化，符合日本政府制定的关于将这两个频段面向室内、室外和移动无线 LAN 应用程序的规则。根据法规要求，公司需要调整这些信道的宽度。IEEE 802.11j 允许无线设备通过利用新技术和工作模式，接入一些之前不可用的信道。部分是望缓解电波的拥挤，并与 IEEE 802.11h 有着切向关系。

802.11k

IEEE 802.11k 是针对无线网络 (**WLAN**) 的正在开发的 *IEEE* 标准，可帮助自动管理网络信道选择、客户端漫游和接入点 (AP) 利用率。支持 802.11k 的网络将会自动加载 AP 上的平衡网络流量，以提高网络性能并防止任何一个 AP 出现使用过度或过少的情况。最后，802.11k 通过确保无线链路上的多媒体的 QoS，补充 *802.11e* 服务质量 (**QoS**) 标准。

802.1p

802.1p 是 IEEE 802 标准的扩展，负责 QoS 的配置。802.1p 的主要用途是优先分配数据链路/MAC 层的网络流量。802.1p 具有过滤多播流量的功能，确保它不会第 2 层交换网络增加。它使用标签帧实施优先分配计划。

要符合此标准，第 2 层交换机必须能够将传入的 LAN 数据包分组为不同的流量级别。

802.1Q

IEEE 802.1Q 是针对无线技术的 *虚拟局域网(VLAN)* 的 *IEEE* 标准。

(请参阅 <http://www.ieee802.org/1/pages/802.1Q.html>。)

该标准解决了如何将大型网络分割为较小部分的问题，以防止广播和多播数据流量消耗过多不必要的带宽。802.11Q 还提高了内部网络的各段之间的安性。802.1Q 规格提供将 VLAN 成员信息插入以太网帧的标准方法。

A

AES

高级加密标准(AES) 是对称的 128 位数据块加密技术，可取代 DES 加密。AES 在多个网络层同时工作。

如需更多信息，请访问 [NIST 网站](#)。

Atheros XR (扩展范围)

Atheros 扩展范围 (XR) 是在较长距离内实施低速率流量的专有方法。它对启用 XR 的客户端和接入点是透明的，并可与 802.11g 和 802.11a 模式下的 802.11 标准实现互操作性。不支持 802.11b 模式下的 Atheros XR、Atheros Turbo 5 GHz 或 Atheros Dynamic Turbo 5 GHz。

B

BSS

基本服务集(BSS) 是具有一个接入点的 *基础架构模式无线网络框架*。另请参阅扩展服务集 (*ESS*) 和独立基本服务集 (*IBSS*)。

BSSID

在 *基础架构模式* 中，*基本服务集标识符(BSSID)* 是 *接入点* 的无线接口的 48 位 *MAC* 地址。

包丢失

包丢失描述了通过网络传输却未能到达预期目的地的数据包的百分比。0% 的包丢失表示传输过程中没有丢失任何数据包。QoS 功能旨在最大程度减少包丢失。

C

CCMP

计数器模式/CBC-MAC 协议(CCMP) 是适用于使用 AES 的 802.11h 的加密方法。它采用 CCM 运行模式，将密码区块链计数器模式 (CBC-CTR) 和密码区块链消息身份验证代码 (CBC-MAC) 组合使用，实现了加密和消息的完整性。

AES-CCMP 需要安装硬件协处理器才能运行。

CGI

通用网关接口 (CGI) 是针对在 HTTP 服务器上运行外部程序的标准。它指定了如何将参数传递至现有程序，作为 HTTP 请求的组成部分。它还可定义一组环境变量。

CGI 程序是 HTTP 服务器与用户动态交互的通用方式。例如，包含表单的 HTML 页面可以使用 CGI 程序，来处理提交的表单数据。

CSMA/CA

载波侦听多路访问与冲突避免 (CSMA/CA) 是低级的网络仲裁/争用协议。工作站侦听媒体并尝试在信道安静时传输数据包。工作站检测到信道处于空闲状态时，会传输该数据包。如果检测到信道是忙碌的，工作站会等待随机数量的时间，然后尝试再次访问媒体。

CSMA/CA 是 IEEE 802.11e 分布式控制功能 (DCF) 的基础。另请参阅 RTS 和 CTS。

802.11 网络使用的 CSMA/CA 协议是 CSMA/CD（以太网网络使用）的变体。CSMA/CD 侧重于检测冲突，而 CSMA/CA 侧重于避免冲突。

CTS

清除发送(CTS) 消息是 **IEEE 802.11** 客户端工作站为回复 *请求发送*(RTS) 消息而发送的消息。CTS 消息表示已为 RTS 消息的发送方清除信道，以开始数据传输。其他工作站将会等待，确保不干扰无线电波。此消息是 IEEE 802.11 **CSMA/CA** 协议的组成部分。（另请参阅 **RTS**。）

D

DCF

*分布式控制功能*是 IEEE 802.11e 服务质量 (QoS) 技术标准的组成元素。DCF 通过控制信道访问的等待时间，来协调无线网络上多个工作站的信道访问。等待时间由随机退避计时器确定，而通过定义最小和最大竞争窗口即可配置随机退避计时器。另请参阅 **EDCF**。

DHCP

动态主机配置协议(DHCP) 指定了中央服务器是如何以动态方式向客户端提供网络配置信息的。DHCP 服务器向客户端系统“提供”“租赁”（预先配置的时间—请参阅*租用时间*）。提供的信息包括客户端的 IP 地址和网络掩码，及其 **DNS** 服务器和**网关**的地址。

DNS

域名服务(DNS) 是通用查询服务，用于将*完全限定名称*转换为互联网地址。完全限定名称由系统的主机名及其域名组成。例如，www 是 Web 服务器的主机名，而 *www.psionteklogix.com* 是该服务器的完全限定名称。DNS 将域名 *www.psionteklogix.com* 转换为 IP 地址，例如 66.93.138.219。

*域名*可用于识别一个或多个 IP 地址。反过来，一个 IP 地址可以与多个域名对应。

域名的后缀表示其所属的*顶级域*(TLD)。每个国家/地区都有其自己的顶级域名，例如德国是 .de，法国是 .fr，日本是 .jp，台湾是 .tw，英国是 .uk，美国是 .us 等。此外，.com 表示商业机构，.edu 表示教育机构，.net 表示网络运营商，.org 表示其他组织，.gov 表示美国 政府，而 .mil 表示其军事部队。

DOM

文档对象模型 (DOM) 界面允许程序和脚本动态访问并更新文档的内容、结构和样式。DOM 允许针对 HTML 或 XML 文档中的对象（文本、链接、图像、表格）进行建模，定义各对象的属性以及对其进行操作的方式。

有关 DOM 的更多详情，请参阅 [W3C](#)。

DTIM

传输流量信息图 (DTIM) 消息是某些 *信标* 帧中包含的元素。它指示当前在低功率模式下睡眠的哪个客户端工作站在等待选取的 *接入点* 上缓冲了数据。部分 DTIM 消息表示工作站检查缓冲数据的频率。

单播

单播 发送一条消息至一个指定的接收方。在无线网络中，单播通常是指接入点以 *IEEE 802.1x 帧* 形式直接向网络上的单个客户端工作站 *MAC* 地址发送数据数据流量的交互方式。

有线无线安全模式的不同之处在于单播、多播和广播帧的加密方式或是否对其进行加密。

另请参阅 *多播* 和 *广播*。

端口转发

端口转发 通过防火墙创建“隧道”，允许具有 Internet 接入的用户能够使用在 *LAN* 的其中一台计算机上运行的服务，例如 Web 服务器、FTP 或 SSH 服务器，或其他服务。从外部用户的角度来看，它就好像是在防火墙上运行的服务。

多播

多播发送同一条消息至选中的收件人组。多播的示例之一就是发送电子邮件至邮件列表。在无线网络中，多播通常是指接入点以 **IEEE 802.1x 帧** 形式发送数据流量至网络上一组指定的客户端工作站（**MAC** 地址）的交互方式。

有线无线安全模式的不同之处在于单播、多播和广播帧的加密方式或是否对其进行加密。

另请参阅 **单播** 和 **广播**。

代理

代理是位于客户端应用和真实服务器之间的服务器。它拦截请求，并尝试自行履行请求。如果无法履行请求，会将其转发至真实的服务器。代理服务器有个主要目的：通过多台机器传播请求以提高性能，同时对请求进行筛选，防止使用特定服务器或服务。

点对点模式

点对点模式是**无线网络框架**，在其中工作站可以彼此直接通信。它可用于在不需要正式基础设施时快速建立网络。

点对点模式也被称为**对等模式**或独立基本服务集 (**IBSS**)。

动态 IP 地址

请参阅 **IP 地址**。

抖动

抖动是指从一个接入点传输数据包至网络上另一个接入点时出现的延迟之间的差别。如果不以一致的速率（包括**延迟**）传输数据包，则某些数据类型的 **QoS** 会受到影响。例如，不一致的传输速率会导致 VoIP 和流媒体扭曲。**QoS** 旨在减少抖动以及其他会影响网络性能的因素。

E

EAP

可扩展身份验证协议 (EAP) 是身份验证协议，支持多种方法，例如令牌、Kerberos、一次性密码、证书、公钥身份验证和智能卡。

EAP 的变体包括 EAP Cisco Wireless (LEAP)、受保护的 EAP (PEAP)、EAP-TLS 和 EAP 隧道化 TLS (EAP-TTLS)。

EDCF

增强型分布式控制功能 是 **DCF** 的扩展。EDCF 是 IEEE 无线多媒体 (WMM) 标准的组成元素，提供对无线媒介的优先访问。

ESS

扩展服务集 (ESS) 是具有多个接入点的 **基础架构模式无线网络框架**，形成单个子网，支持的客户端数量比基本服务集 (**BSS**) 更多。各个接入点支持大量无线工作站，为大面积空间（例如，办公室）提供更广泛的无线覆盖范围。

ERP

扩展速率协议 是指与正交频分复用 (OFDM) 组合使用时，**IEEE 802.11g** 工作站使用的协议（2.4GHz 时的传输速率超过 20 Mbps）IEEE **802.11g** 标准内置于 ERP 中，可有效实现 IEEE 802.11g 工作站与同一信道上 IEEE 802.11b 节点的互操作性。

传统的 IEEE 802.11b 设备无法检测到 IEEE 802.11g 工作站使用的 ERP-OFDM 信号，这会导致 IEEE 802.11b 和 IEEE 802.11g 工作站发送的数据帧产生冲突。

如果在同一信道上混用 802.11b 和 802.11g 节点，IEEE 802.11g 工作站通过接入点上的 ERP 标记检测，并在发送数据前启用 *请求发送* (**RTS**) 和 *清除发送* (**CTS**) 保护。

另请参阅 **CSMA/CA** 协议。

G

共享密钥 (Shared Key)

加密和解密都使用一个密钥的传统加密方法使用 *共享密钥*。它也被称为 *秘密密钥* 或 *对称密钥* 加密。

另请参阅 *公钥*。

公钥

在 *公钥密码* 系统中使用公钥，以对仅可使用收件人的私钥或密钥解密的消息进行加密。公钥加密也被称为对称加密，这是因为它使用两个密钥或 Diffie-Hellman 加密。另请参阅 *共享密钥 (Shared Key)*。

广播

广播 同时向所有人发送同一条消息。在无线网络中，广播通常是指接入点以 *IEEE 802.1x 帧* 的形式向网络上的所有客户端工作站发送数据流量这一交互方式。

有线无线安全模式的不同之处在于单播、多播和广播帧的加密方式或是否对其进行加密。

另请参阅 *单播* 和 *多播*。

广播地址

请参阅 *IP 地址*。

H

HTML

超文本标记语言 (HTML) 定义了万维网上的文档结构。它使用标签和属性暗示该文档的布局。

HTML 文档以 <html> 标签开头，以 </html> 标签结束。格式正确的文档还包含 <head> ... </head> 部分（包含定义文档的元数据）以及 <body> ... </body> 部分（包含其内容）。其标记来源于 *标准通用标记语言* (SGML)。

服务器通过 **HTTP** 将 HTML 文档发送至浏览器。另请参阅 **XML**。

HTTP

超文本传输协议 (**HTTP**) 定义了万维网上消息的格式及传输方式。HTTP 消息由 **URL** 和命令（GET、HEAD、POST 等）组成，请求之后是响应。

HTTPS

安全超文本传输协议 (HTTPS) 是 HTTP 的安全版本，也是万维网的通信协议。HTTPS 内置于浏览器中。如果您使用 HTTPS，您会注意到浏览器页面的底部显示个闭锁图标。

通过 HTTPS 发送的所有数据都会加密，从而确保了交易的安全性。

I

IAPP

接入点互连协议 (IAPP) 是 **IEEE** 标准 (**802.11f**)，定义了“分布式系统”中的接入点之间的通信。包括交换移动工作站的相关信息、维护网桥转发表，此外还确保了接入点之间通信的安全性。

IBSS

独立基本服务集 (IBSS) 是 *点对点模式无线网络框架*，在其中工作站可以彼此直接通信。

IEEE

电气电子工程师协会 (IEEE) 是国际标准组织，负责制定和建立针对广泛技术的行业标准（包括 802 系列联网和无线标准）。（请参阅 **802**、**802.1x**、**802.11**、**802.11a**、**802.11b**、**802.11e**、**802.11f**、**802.11g** 和 **802.11h**。）

有关 IEEE 任务组和标准的更多信息，请参阅 <http://standards.ieee.org/>。

IP

互联网协议 (IP) 指定了数据包的格式（也被称为数据包）和寻址方案。IP 是无连接、尽力而为的数据包交换协议。它提供数据包的路由、分段和重新组合。它与高级别的协议组合使用，例如 **TCP** 或 **UDP**，以建立目的地和来源之间的虚拟连接。

当前的 IP 版本是 **IPv4**。新版本（也被称为 **IPv6** 或 **IPng**）正在开发当中。IPv6 尝试解决 IP 地址的短缺问题。

IP 地址

系统由其 **IP 地址** 定义，IP 地址是四字节（八位字节）数字，唯一地定义互联网上的各台主机。它通常以 192.168.2.254 格式显示。也被称为带点的十进制。

一个 IP 地址分为两部分：网络前缀和该网络上的主机编号。**子网掩码** 用于定义该部分。有两个特殊的主机编号：

- **网络地址** 由全是零的主机编号组成（例如，192.168.2.0）。
- **广播地址** 由全是一的主机编号组成（例如，192.168.2.255）。

可以存在的 IP 地址数量是有限的。因此，局域网通常使用 **IANA** 指定的地址范围，应用于专用网络。地址范围如下所示：

10.0.0.0 至 10.255.255.255

172.16.0.0 至 172.31.255.255

192.168.0.0 至 192.168.255.255

动态 IP 地址 是通过 **DHCP** 服务器或类似机制自动分配至主机的 IP 地址。它被称为动态地址，这是因为每次建立连接时会被分配不同的 IP 地址。

静态 IP 地址是用于特定主机的硬接线 IP 地址。对于运行服务器（例如 Web 服务器）的任何主机，通常需要静态地址

IPSec

IP 安全 (IPSec) 是一组支持在 **IP** 层安全交换数据包的协议。它使用共享公钥。有两种加密模式：传输和隧道。

- **传输模式**只加密各包的数据部分（有效负载），但不加密标头。
- **隧道模式**更安全，对标头和有效负载进行加密。

ISP

Internet 服务提供商 (ISP) 是向个人及公司提供 Internet 访问的公司。它可以提供相关服务，例如虚拟主机托管、网络咨询、Web 设计等。

J

基本速率设置

基本速率设置定义了想要加入此无线网络的任何工作站必须达到的传输速率。所有工作站必须能够以本设置中列出的速率接收数据。

基础架构模式

基础架构模式是 **无线网络框架**，在其中无线工作站通过 **接入点**彼此通信。在此模式下，无线工作站能够彼此通信或与有线网络上的主机进行通信。接入点连接至有线网络，并支持一组无线工作站。

单个接入点 (**BSS**) 或多个接入点 (**ESS**) 可提供基础架构模式框架。

接入点

接入点是用于 **WLAN** 上的设备通信中心，提供了无线和有线网络设备之间的连接或桥接。它支持被称为**基础架构模式**的**无线网络框架**。

当某个接入点连接至有线网络并支持一组无线工作站时，被称为基本服务集 (**BSS**)。通过组合两个或更多 BSS 来创建扩展服务集 (**ESS**)。

静态 IP 地址

请参阅 *IP 地址*。

L

LAN

局域网(LAN) 是涵盖区域有限的通信网络，例如，您想要进行联网的家中或建筑物内两个楼层的计算机。一个 LAN 可以连接多台计算机及其它网络设备（例如储器和打印机）。*以太网*是实施 LAN 的最常用技术。

无线以太网 (*802.11*) 是另一个非常热门的 LAN 技术（另请参阅 *WLAN*）。

LDAP

轻量目录访问协议(LDAP) 是用于访问在线目录服务的协议。它用于提供另一种身份验证机制。它以 X.500 标准为基础，但没有那么复杂。

LLC

逻辑链路控制(LLC) 层控制帧同步、流控制和错误检查。它是通过 *PHY* 层的更高级别的协议，与 *MAC* 层一起工作。

路由器

*路由器*是在网络之间转发数据包的网络设备。它至少连接两个网络，通常是在两个局域网 (*LAN*) 或 *LAN* 和广域网 (*WAN*) 之间进行连接，例如 Internet。路由器位于网关上，在那里连接两个或更多网络。

路由器使用标头及其表格内容，确定转发数据包的最佳路径。它使用互联网控制消息协议 (ICMP)、路由信息协议 (RIP) 和互联网路由器发现协议 (IRDP) 等协议，与其他路由器进行通信，以配置任何两台主机之间的最佳路由。路由器不对其传递的数据进行筛选。

M

MAC

媒体访问控制 (MAC) 层处理在共用信道上的 *NIC* 之间移动的数据包。它是通过 *PHY* 层的更高级别的协议。它提供仲裁协议，试图防止信号发生冲突。

它使用唯一地识别网络各节点的硬件地址，也被称为 *MAC 地址*。 *IEEE 802* 网络设备共享一个通用的 48 位 MAC 地址格式，通常显示为使用冒号分隔的 12 位十六进制数字，例如 FE:DC:BA:09:87:65。

MDI 和 MDI-X

媒体专用接口 (MDI) 和 *MDI 交叉电缆* (MDIX) 是适用于硬件设备中的以太网端口的双绞线布线技术。内置双绞线布线和自动感应功能，因此只需使用一根标准的以太网电缆就能连接设备。例如，如果接入点支持 MDI/MDIX，则您只需使用一根以太网电缆就能成功连接 PC 和该接入点，无需使用交叉电缆）。

MIB

管理信息库 (MIB) 是用于网络管理的虚拟对象数据库。 *SNMP* 代理及其他 SNMP 工具可用于监控在 MIB 中定义的任何网络设备。

MSCHAP V2

Microsoft 质询握手身份验证协议第 2 版 (MSCHAP V2) 为基于 Windows 的计算机和 *接入点* 或其他网络访问设备之间的 *PPP* 连接提供身份验证。

MTU

最大传输单元 是指网络可以传输的最大尺寸的物理包，以字节为单位进行测量。大于 MTU 的任何消息将在发送前拆分为较小的数据包。

漫游

在 *IEEE 802.11* 用语中，*漫游客户端* 是指无线网络 (*WLAN*) 上移动的客户端工作站或设备，它们在移出和移进不同的基站服务器区域范围时需要使用多个 *接入点* (AP)。IEEE 802.11f 定义了 AP 为支持漫游客户端而传达客户端关联和取消关联的相关消息所使用的标准。

N

NAT

网络地址转换 是 Internet 标准，生成 *LAN* 中使用的内部 IP 地址的掩码。在网关上运行的 NAT 服务器保留转换表，将传出请求中的所有内部 IP 地址与自己的地址进行对应，并将所有传入请求转换为正确的内部主机。

NAT 有三个主要目的：它隐藏内部 IP 地址，通过隐匿来实现安全性，因此使用广泛的内部 IP 地址时无需再担心与其他组织使用的地址发生冲突，此外还允许使用单个 Internet 连接。

NIC

网络接口卡 是插入计算机以提供与网络的物理连接的适配器或扩展板。大多数 NIC 专为特定类型的网络、协议和媒体而设计，例如 *以太网* 或无线。

NTP

网络时间协议 确保了计算机网络中系统时钟的准确同步。NTP 服务器传输 *协调世界时* (UTC，也被称为 *格林威治标准时间*) 至其客户端系统。NTP 客户端发送定期的时间请求至服务器，使用返回的时间戳调整其始终。

O

OSI

开放系统互连 (OSI) 参考模型是用于网络设计的框架。OSI 模型由七层组成：

- 第 1 层——物理层，确定用于节点之间的通信的物理媒体。如果使用无线网络，则物理媒体是无线，且无线电波是物理层的组成部分。
- 第 2 层——数据链路层，定义了如何构建和格式化用于传输的数据，以及用于通信和寻址的低级协议。例如，**CSMA/CA** 等协议和 **MAC** 地址等组件，以及 **帧** 均已定义，并作为数据链路层的组成部分进行处理。
- 第 3 层——网络层，定义了如何确定通过网络的信息的最佳路径。**数据包** 和逻辑 **IP 地址** 在网络层上运行。
- 第 4 层——传输层，定义了 **TCP** 和 **UDP** 等面向连接的协议。
- 第 5 层——会话层，定义了用于发起、保留和结束网络上的通信及事务的协议。在此层上运行的协议的一些常见示例包括网络文件系统 (NFS) 和结构化查询语言 (SQL)。通信流也是该层的组成部分，例如单一模式（设备批量发送信息）、半双工模式（设备轮流传输批量信息）和全双工模式（交互，设同时收发信息）。
- 第 6 层——表示层，定义了向应用显示信息的方式。它包括关于如何加密/解密和压缩/解压缩数据的元信息。**JPEG** 和 **TIFF** 文件格式是此层协议的示例。
- 第 7 层——应用层，包括超文本传输协议 (**HTTP**)、简单邮件传输协议 (**SMTP**) 和文件传输协议 (**FTP**) 等协议。

P

PHY

物理层 (PHY) 是网络层模型中的最低层（请参阅 **OSI**）。物理层在电气和机械级别通过网络传输位流（电脉冲、光或无线通信信号）。它提供在介质上收发数据的硬件方式，包括定义电缆、**NIC** 和物理方面。

以太网 和 **802.11** 协议是具有物理层组件的协议。

PID

进程标识符(PID) 是 Linux 用来唯一地识别某个进程的整数。通过 `fork()` 系统调用返回 PID。`wait()` 或 `kill()` 使用它在指定进程上执行操作。

PPP

*点到点协议*是针对通过串行点到点链路传输网络层数据报 (*IP* 数据包) 的标准。PPP 可通过异步连接和面向位的同步系统工作。

PPPoE

以太网上的点到点协议(PPPoE) 是针对通过常见带宽介质 (例如一根 DSL 或电缆调制解调器线) 连接 *LAN* 的用户和 *Internet* 的规范。

PPtP

点对点隧道协议(PPtP) 是针对在 *点到点协议*(*PPP*) 中创建 *虚拟专用网络*(*VPN*) 的技术。它用于确保从一个 VPN 节点传输至另一个节点是数据是安全的。

PSK

预共享密钥(PSK), 请参阅 *共享密钥*(*Shared Key*)。

Q

QoS

服务质量 (QoS) 定义了网络服务的性能属性, 包括保证的吞吐量、传输延迟和优先发送队列。QoS 旨在最大程度减少 *延迟*、*抖动*、*包丢失* 和网络拥塞, 并提供分配高优先级网络流量的专用带宽的方式。

IEEE 标准用于在无线网络上实施 QoS, 目前被 *802.11e* 任务组使用。*802.11e* 功能的子集如 *WMM* 规范中所述。

桥接

使用相同协议的两个局域网 (*LAN*) 之间的连接, 例如局域网 *IEEE 802.1x*。

R

RADIUS

远程身份验证拨号用户服务 (RADIUS) 提供身份验证和计费系统。它是适用于许多 *ISP* 最常见的身份验证机制。

RC4

RSA Security 提供的对称的流密码。它是密钥大小的可变流密码，可进行面向字节的操作。密钥的长度不得超过 204 位。

RSSI

接收信号强度指示 (RSSI) 是计算相对于接收信号强度的电压的 *802.1x* 值。测量和指示 *射频 (RF)* 信号强度有多种方式，RSSI 是其中之一。还可以采用 mW（毫瓦特）、dBms（分贝毫瓦）和百分比值为单位测量信号强度。

RTP

实时传输协议 (RTP) 是用于传输音频和视频灯实时数据的互联网协议。它不保证交付，但提供发送和接收应用程序以实现流数据的支持机制。RTP 通常在 *UDP* 协议之上运行，但也支持其他传输协议。

RTS

请求发送 (RTS) 消息时客户端工作站发送至接入点的信号，要求获得权限来发送数据包并阻止其他无线客户端工作站争用无线电波。此消息是 IEEE 802.11 *CSMA/CA* 协议的组成部分。（另请参阅 *RTS 阈值* 和 *CTS*。）

RTS 阈值

RTS 阈值 指定了发送 (*RTS*) 传输请求的数据包大小。这可帮助控制通过接入点的流量，对提高具有多个客户端的接入点的性能尤其有用。

入侵检测

入侵检测系统(IDS)检测所有传入的网络活动，并报告可疑的模式，表示网络或系统收到其他试图进入系统的人员的攻击。它使用不受支持或已知不安全的协议报告访问尝试。

S

SNMP

简单网络管理协议(SNMP)为管理和监控网络上的节点而制定。它是 *TCP/IP* 协议组的组成部分。

SNMP 由管理的设备及其代理，以及管理系统组成。代理将其设备相关数据存储在管理信息库(MIB)中，并在请求时将这些数据返回至 SNMP 管理系统。

SNMP 陷阱

SNMP 陷阱实现了从网络设备到管理代理的异步通信。设置 SNMP 陷阱可以节约网络资源，并消除冗余 SNMP 请求。

SSID

服务集标识符(SSID)是 32 个字符的字母数字密钥，唯一地标识无线局域网。它也被称为网络名称。对于在 SSID 中使用的字符没有任何限制。

STP

生成树协议(STP)是 IEEE 802.1 标准协议（与网络管理相关），适用于 *MAC* 网桥，以管理冗余路径并防止客户端工作站之间的多个活动路径创建的网络中存在不需要的循环。当接入点之间有多个路由时，会发生循环。STP 创跨越扩展网络中所有交换机的树，迫使冗余路径进入备用或阻塞状态。STP 只允许一次在任何两个网络设备之间使用一个活动路径（以阻止回路），如果初始链路出现故障，它会建立冗余链路作为备份。如果 STP 成本发生变化，或 STP 中的一个网络段不可达，则生成树算法会重新配置生成树的拓结构，并通过启用备用路径来重新建立链路。如果不实施 STP，有可能同时使用两个连接，这会导致 LAN 上流量的无限循环。

SVP

SpectraLink 语音优先级 (SVP) 是用于部署 Wi-Fi 的 QoS 方法。SVP 是开放式规范，与 IEEE 802.11b 兼容。SVP 最大限度地减少了延迟，并优先于数据包安排无线 LAN 上的语音包，因此增加了提高网络性能的可能性。

数据包

以*数据包*的形式，在网络上的节点之间传输数据和媒体。对数据和多媒体内容进行划分并打包进*数据包*。数据包包括一小块要发送的内容，及其目标地址和发送人地址。将数据包推送到网络，并接受各节点的检查。将数据包发送至的节点就是最终接收。

T

TCP

传输控制协议 (TCP) 基于互联网协议 (*IP*) 建立。它增添了可靠的通信（确保数据交付）、流控制、时分复用（多个同时连接）以及面向连接的传输（要求数据包接收方向发送方确认已收到。它还确保了数据包的交付顺序与其发送顺序相同。

TCP/IP

互联网及大多数局域网是由一组协议定义的。其中最重要的协议就是*通过互联网协议的传输控制协议* (TCP/IP) 这一实际的标准协议。TCP/IP 最初是由国防部高级研究计划局（DARPA，也被称为 ARPA，是美国国防部机构）开发的。

尽管 *TCP* 和 *IP* 是两个特定协议，TCP/IP 通常用于引用基于这两个协议的整体协议组，包括 ICMP、ARP、*UDP* 及其它，以及在这些协议之上运行的应用程序，例如 Telnet、FTP 等。

TKIP

临时密钥完整性协议 (TKIP) 提供扩展的 48 位初始化向量、每包密钥构建和分配、消息完整性代码（MIC，有时被称为“Michael”），以及密钥更新机制。传输前，它使用 *RC4* 流密码来加密帧主体以及各 *802.11* 帧的 CRC。它是 *WPA* 和 *802.11h* 安全机制的重要组成部分。

ToS

TCP/IP 包头包括由应用开发人员设置的 3 到 5 位 *服务类型 (ToS)* 字段，用于表示该包数据相应的服务类型。设置位元的方式确定了是将该包加入队列来进行延迟最小、吞吐量最大、成本低的发送，还是进行中路“尽力而为”设置，具体视数据要求而定。产品名称 使用 ToS 字段来为从 AP 传输至客户端工作站的数据提供通过 *服务质量 (QoS)* 队列的配置控制。

U

UDP

用户数据报协议 (UDP) 是传输层协议，提供的数据报服务虽简单却不可靠。它向 **IP** 包添加了端口地址信息和校验和。

UDP 不保证交付，也不需要连接，既轻便又有效。必须由应用程序来执行所有错误处理和重新传输。

URL

统一资源定位符 (URL) 是用于指定互联网上对象（例如文件或新闻组）的位置的标准。URL 在 HTML 文档中广泛使用，以指定超链接目标，而该超链接通常表示另一个文（可能存储在另一台计算机上）。URL 的第一部分表示使用哪个协议，第二部分指定了资源所在的域名的 IP 地址。

例如，<ftp://ftp.devicescape.com/downloads/myfile.tar.gz> 指定了应使用 FTP 协议提取的文件，<http://www.devicescape.com/index.html> 指定了应使用 **HTTP** 协议提取的网页。

UTC

协调世界时 (UTC) 也被称为格林威治标准时间。

V

VLAN

虚拟 LAN (VLAN) 是对网络上的设备进行基于软件的逻辑分段，允许这些设备就像连接至一个物理网络那样运行，尽管实际上它们并未连接网络。VLAN 中的节点共享资源和带宽，在该网络上独立的。产品名称支持配置无线 VLAN。在用于“虚拟”访客网络功能的接入点上使用此技术。

VPN

虚拟专用网络 (VPN) 是使用 Internet 连接其节点的网络。它使用的加密和其他机制确保仅授权用户能够访问其节点，且不会拦截数据。

W

WAN

广域网 (WAN) 是跨越的地理范围相对较大的通信网络，延伸距离超过一公里。通常通过公共网络（例如电话系统）连接 WAN。还可通过租用线路或卫星来连接

从本质上来说，互联网就是一个很大的 WAN。

WDS

无线分布式系统 (WDS) 允许创建完全无线的基础设施。通常，*接入点* 连接至有线 LAN。WDS 允许以无线方式连接接入点。接入点可用作无线中继器或桥接。

WEP

有线等效加密 (WEP) 是用于 **802.11** 无线网络的数据加密协议。通过静态 64 位（40 位密钥 + 24 位初始化向量 (IV)）或用于数据加密的 128 位（104 位密钥 + 24 位 IV）*共享密钥 (Shared Key)*，配置网络上的所有无线站点和接入点。传输前，它使用 **RC4** 流密码来加密帧主体以及各 **802.11** 帧的 CRC。

Wi-Fi

根据非盈利性行业组织 Wi-Fi 联盟 所推广的 *IEEE 802.11* 标准, 来进行 *WLAN* 产品的互操作性测试和认证。

WINS

Windows Internet 命名服务 (WINS) 是将基于 Windows 的计算机名称解析为 IP 地址的服务器进程。它提供的信息允许这些系统使用 *网上邻居* 来浏览远程网络。

WLAN

无线局域网 (WLAN) 是 *LAN*, 使用高频无线电波而不是连接线进行节点之间的通信。

WMM

无线多媒体 (WMM) 是 *IEEE* 技术标准, 旨在提高无线网络上的音频、视频和多媒体应用的质量。接入点和无线客户端 (便携式计算机、消费类电子产品) 均支持 WMM。WMM 功能基 *WLAN IEEE 802.11e* 草案规范的子集。符合标准并通过一系列质量测试的无线产品可以贴上 “通过 WMM 的 Wi-Fi 认证” 标签, 确保与其他此类产品的互操作性。有关更多信息, 请参阅 Wi-Fi 联盟网站上的 WMM 页面:
<http://www.wi-fi.org/OpenSection/wmm.asp>。

WPA

Wi-Fi 受保护访问 (WPA) 是草案 *IEEE 802.11h* 标准的 *Wi-Fi* 联盟版本。它提供比 *WEP* 更高级的数据加密, 此外还提供用户身份验证。WPA 包括 *TKIP* 和 *802.1x* 机制。

WPA2

Wi-Fi 受保护访问 (WPA2) 是增强的安全标准, 如 *IEEE 802.11h* 中所述, 使用高级加密标准 (*AES*) 进行数据加密。

原始的 *WPA* 使用临时密钥完整性协议 (*TKIP*) 进行数据加密。WPA2 提供与支持原始 *WPA* 的产品的向后兼容性。

和原始 **WPA** 一样，WPA2 支持 *企业* 和 *个人* 版本。企业版需要使用 IEEE **802.1x** 安全功能和 *可扩展身份验证协议 (EAP)* 验证 **RADIUS** 服务器的身份。

个人版本无需 IEEE **802.1x** 或 **EAP**。它使用 *预共享密钥 (PSK)* 密码生成进行身份验证所需的密钥。

WRAP

无线健壮身份验证协议 (WRAP) 加密方法适用于使用 **AES** 却采用另一种加密方法 (**OCB**) 实现加密和完整性的 **802.11h**。

网络地址

请参阅 *IP 地址*。

网关

网关是用作另一网络的入口的网络节点。通常，网关还提供代理服务器和防火墙。它与路由器（使用标头和转发表确定发送数据包的位置）和交换机或网（提供网关发送或接收的数据包的 *实际路径*）关联。

在 **LAN** 上的主机接入互联网前，它需要知道其 *默认网关* 的地址。

无线网络框架

组织无线网络有两种方式：

- 直接与 *点对点模式* 网络中的其他工作站彼此通信的工作站，也被称为独立基本服务集 (**IBSS**)。

通过 *基础架构模式* 网络中的 *接入点* 通信的工作站。单个接入点创建基础架构基本服务集 (**BSS**)，而在扩展服务集 (**ESS**) 中组织多个接入点。

X

XML

可扩展标记语言 (XML) 是 **W3C** 制定的规范。XML 是简单、灵活的文本格式，来源于 *标准通用标记语言 (SGML)*，专为电子出版而设计。

信标

信标帧提供 **WLAN** 的“心跳”，表示存在网络，并使得工作站能够有序地建立和保持通信。它提供以下信息（其中一些信息是可选的）：

- 工作站使用 *时间戳* 来更新本地时钟，实现所有关联工作站的同步。
- *信标间隔* 定义了两次信标帧的传输之间的时间量。进入省电模式前，工作站需要信标帧来确定何时唤醒以接收信标。
- *功能信息* 列出了想要加入 **WLAN** 的工作站的要求。例如，它指出所有工作站必须使用 **WEP**。
- *服务集标识符 (SSID)*。
- *基本速率设置* 是列出 **WLAN** 支持的速率的位图。
- 可选的 *参数设置* 表示使用的特定通信方式的特性（例如跳频扩频、直序扩频等）。

可选的 *流量指示图 (TIM)* 识别了使用省电模式使数据帧加入队列的工作站。

信道

信道 定义了用于收发射频的射频频谱部分。所有 **802.11** 标准均提供大量信道，具体取决于国家和跨国机构（例如，联邦通信委员会 (FCC)、欧洲电信标准协会 (ETSI)、韩国通信委员会 或 电信工程中心 (TELEC)）许可频谱的方式。

Y

延迟

延迟 是指发送器向接收器传输 **数据包** 所需的时间。接入点向客户端传输数据（反之亦然）时，会发生延迟。接入点向 **Internet** 传输数据（反之亦然）时，也会发生延迟。延迟是由 *固定网络* 因素导致的，例如编码和解码数据包所需的时间；此外还受到 *变量网络* 因素的影响，例如网络繁忙或过载。**QoS** 功能旨在最大程度减少高优先级网络流量的延迟。

以太网

以太网是支持 10 Mbps 到 1 Gbps 的数据传输速率的局域网 (*LAN*) 架构。以太网规范是 **IEEE 802.3** 标准的基础，指定物理或较低的软件层。它使用 **CSMA/CA** 访问方法处理同时要求。

以太网支持的数据速率为 10 Mbps，快速以太网支持 100 Mbps，千兆位以太网支持 1 Gbps。其电缆被归类为 “*XbaseY*”，其中 *X* 表示以 Mbps 为单位的数据速率，而 *Y* 表示布线类别。原始电缆是 *10base5*（粗缆或“黄色电缆”）。其他电缆包括 *10base2*（细缆）、*10baseT*（双绞线）和 *100baseT*（快速以太网）。通常提供后两种电缆，使用具有 *RJ-45* 连接器的 *CAT5* 布线。此外，还有 *1000baseT*（千兆位以太网）。

Z

帧

一个帧由离散部分的数据以及一些为在无线网络上传输而打包的描述性元信息组成。每个帧包括一个来源 **MAC** 地址和目标 **MAC** 地址、协议版本的控制字段、帧类别、帧序号、帧主体（和要传输的实际信息）以及用于检测错误的帧检验序列。帧与数据包的概念类似，不同之处在于数据包在网络层（**OSI** 模型中的第 3 层）运行，而帧在数据链接层（**OSI** 模型中的第 2 层）运行。

支持的速率设置

支持的速率设置定义了此无线网络上可用的传输速率。工作站必须能以此设置中列出的任何速率来接收数据。所有工作站必须能够以基本速率设置中列出的速率接收数据。

子网掩码

子网掩码是一个数字，用于定义 IP 地址的哪些数字表示网络地址，而哪些数字表示网络上的主机地址。它以带点的十进制表示（例如，24 位掩码显示为 255.255.255.0），或显示为 IP 地址附加的数字（例如，192.168.2.0/24）。

子网掩码允许路由器快速确定某个 IP 地址是本地地址还是需要通过在掩码和 IP 地址上执行按位“与”运算来进行转发。例如，如果 IP 地址为 192.168.2.128 而网络掩码为 255.255.255.0，则生成的网络地址为 192.168.2.0。

按位“与”运算符比较两个位元，并仅在两个位元都为 1 的情况下向结果分配 1。下表列出了网络掩码的详细信息：

IP 地址	192.168.2.128	11000000 10101000 00000010 10000000
网络掩码	255.255.255.0	11111111 11111111 11111111 00000000
生成的网络地址	192.168.2.0	11000000 10101000 00000010 00000000

租用时间

租用时间指定了 DHCP 服务器向其客户端提供 IP 地址及其他所需信息使用的时间。租用到期时，客户端必须请求新的租用。如果租用设为短时间跨度，您可以更新您的网络信息，并及时传播提供给客户端的信息。

索引

英文字母

AIAG

3274 仿真 259

5250 仿真 274

ANSI, 连接终端 22

ANSI 仿真 284-292

Atheros Turbo 模式 7, 165

客户端

另请参阅 站点 167

DCF

随机退避计时器 188

与 QoS 相关 187

DEC VT220, 连接 22

DHCP, 了解与自我管理 AP 的关系 30

DNS 主机名, 以太网设置 136

DSCP

标签 189

优先级 191

DTIM 周期, 配置 167

EAP-PEAP

在 IEEE 802.1x 客户端上配置 C-15

在 WPA/WPA2 企业版 (RADIUS) 客户端上配置 C-23

Firefox 22

Flash ROM 316

IEEE 802.1x

安全模式

何时使用 94

客户端配置 C-15

配置 106

IEEE 802.11

速率设置, 配置 167

无线通信模式, 配置 167

支持标准 9

IEEE 802.11a

配置 167

IEEE 802.11b

配置 167

IEEE 802.11g

配置 167

Internet Explorer 22

IP 地址

查看接入点 53, 60, 83

导航至 59

了解自我管理 AP 的政策 30

9160 G2 20

IP 地址 (基站) 230

IP 语音

通过 QoS 改进服务 183

LAN 安装 20

LED 指示灯 21

LU 名称前缀

3274 Telnet 协议 267

MAC 过滤, 配置 176

mapRF

802.IQv2 295

MIBs 参见 管理信息库 211

Microsoft Internet Explorer 22

NTP 服务器

配置接入点以使用 304

Orchestrator 功能概述 12

PEAP

在 IEEE 802.1x 客户端上配置 C-15

在 WPA/WPA2 企业版 (RADIUS) 客户端上配置 C-23

QoS 参见 服务质量 183

RADIUS 服务器

还可参阅 身份验证服务器

配置以确认接入点 C-33

RA1001A 无线通信参数 222

RA1001A 窄带无线通信

规格 317

配置 220

RJ-45 连接器引脚分配 (10BaseT 以太网) B-3

RLE, ANSI 仿真 286

RRM 模式 228

RRM 组

RRM 组编号 233

冲突大小 235

共用信道 234

呼叫信号周期 235

呼叫信号字符串 235

- 活动信道 236
- 轮询窗口的大小 234
- 轮询窗口的数量 234
- 轮询协议参数 234
- 同步延迟 236
- 消息模式限值 235
- 远程传输开启时间 236
- 重试次数 235
- 自动启动 233
- 自由窗口外形尺寸 235
- 组合 236
- 最大消息段大小 234
- RRM 组配置设置** 231
- RTS 阈值, 配置 167
- SDRAM 316
- SNMP 参见简单网络管理协议 211
- 站点
 - 另请参阅 客户端
- TCP 会话请求密钥, ANSI Telnet 协议** 288
- TekTerm, 无线通信链路功能 240
- TekTerm 的直接 TCP 连接**, 无线通信链路功能 240
- TLS-EAP
 - 获取客户端证书 C-37
 - 在 IEEE 802.1x 客户端上配置 C-19
 - 在 WPA/WPA2 企业版 (RADIUS) 客户端上配置 C-27
- Turbo 广播模式, 不建议 7, 165
- UI 上的图标 48
- UI 颜色和样式 48
- VLAN
 - 适用于内部和访客接口 154
 - 优先级 191
- VWN (虚拟无线网络), 以太网设置 138
- WDS
 - 规则 204
 - 配置 204
 - 说明 201
- WDS 示例 206
- Web 浏览器 22
- WEP 安全模式
 - 何时使用 93
 - 客户端配置 C-12
 - 配置 101
- Wi-Fi 规定 9
- WPA/WPA2 个人版 (PSK) 安全模式
 - 客户端配置 C-30

- WPA/WPA2 企业版 (RADIUS) 安全模式
 - 客户端配置 C-23
- WPA 个人版安全模式
 - 何时使用 95
 - 配置 109
- WPA 企业版安全模式
 - 何时使用 96
 - 配置 112

A

- 安全
 - 批准 xv
 - 说明 xvii
- 安全模式的身份验证 92
- 安全性
 - IEEE 802.1x 106
 - WPA/WPA2 个人版 (PSK) 109
 - WPA/WPA2 企业版 (RADIUS) 112
 - 比较模式 92
 - 不同模式的优缺点 91
 - 纯文本 (配置为无) 100
 - 访客网络 100
 - 功能概述 11
 - 静态 WEP 101
 - 客户端证书 C-37
 - 配置 89-116
 - 身份验证服务器 C-33
 - 在接入点上配置 98
 - 在无线客户端上配置 C-5
- 安装
 - LAN 20
 - 安全 xvii
 - 电源线 20
 - 环境要求 17, 315
 - 天线 20

B

- 包突发
 - 与 QoS 相关 189
- 备份
 - 链路, WDS 202
 - 用户帐户数据库 69
- 本地**
 - 5250 仿真 272
- 本机**
 - 3274 仿真 257
- 标准 9
- 不联机/脱机**, 9010/TCP/IP 仿真 245
- 不同安全模式下的加密 92

C

参数

使用 Web 浏览器更改 22

常规参数, 窄带无线通信 223

冲突

大小

RRM 组 235

窄带无线通信 226

初始 RTT, 802.IQv1 298

处理器 316

传输行

3274 仿真 259

5250 仿真 274

串行

串行 I/O

3274 仿真 263

5250 仿真 277

数据速率 22

状态指示灯 LED 21

纯文本安全模式

何时使用 92

客户端配置 C-11

配置 100

D

打印表单长度

3274 仿真 263

5250 仿真 278

打印行

3274 仿真 263

5250 仿真 278

大写字符集 (GL), ANSI 仿真 287

登录管理 Web 页面 38

第一个本地终端端口

ANSI Telnet 协议 288

3274 Telnet 协议 265

5250 Telnet 协议 280

第一个终端 244, 252

第一个终端监听端口

ANSI Telnet 协议 288

3274 Telnet 协议 266

5250 Telnet 协议 280

电缆

串行描述 B-1

控制台端口编号 B-2

同轴 19

电气安全批准 xv

电压, 输入 18, 316

电源

连接 36

要求 18, 316

调制级别, 窄带无线通信 227

定向天线 18

端口

位置 20

引脚分配

RJ-45 连接器 (10BaseT) B-3

控制台端口 B-1

硬件 35

端口, RA1001A 参数 228

队列, 为 QoS 配置 192

F

发射/接收信息 125

发射功率, 配置 167

仿真

ANSI 284-292

概述 249

3274/Telnet 254-268

5250 269-283

9010/TCP/IP 245

仿真

微型控制器配置 253

访客访问, 以太网设置 136

访客接口

VLAN 154

功能概述 11

配置 153

说明 153

访客接口设置, 以太网设置 141

访客网络安全性 100

非法接入点 128

分段阈值, 配置 167

蜂窝

基站 220, 239

切换 219

辐射信息, 加拿大 xv

服务类型 参见 ToS 186

服务质量 183

负载平衡, 配置 180

G

工作

温度 315

相对湿度 315

工作模式, 基站 224

功能概述 9

功能键 n

功能键映射屏幕

ANSI 292

3274 268

5250 283

功能键重映射, ANSI 仿真 285

共用信道

RRM 组 234

共用信道, 基站 225

关联的无线客户端 127

管理信息库 (MIB) 211

管理员

密码

基本设置 47

平台 28

光纤以太网端口 21

广播 SSID 98

规格

RA1001A 窄带无线通信 317

物理 315

802.11A/G 无线通信 316

802.11G 无线通信 316

H**呼叫信号**

周期

RRM 组 235

周期, 窄带无线通信 227

字符串

RRM 组 235

字符串, 窄带无线通信 227

环境要求 17

储存温度 315

概述 17

工作温度 315

工作相对湿度 315

回路, WDS 202

回音, ANSI 仿真 285

会话 60

会话监控

查看会话信息 62

导航至 60

关于 60

刷新信息 62

会话循环密钥, ANSI Telnet 协议 288

活动信道

RA1001A 参数 228

RRM 组 236

J**集群**

安全性 56

大小 54

大小和成员资格 56

定义 53

故障排除 D-45

了解 53

邻居 81, 84

添加接入点 58

停止形成集群 58

信道管理 71

形成 56

支持的接入点类型 54

自动同步 56

集群 AP 的信道管理

查看/设置锁定 76

导航至 73

高级设置 77

建议的信道分配 77

了解 73

示例 74

基本设置, 查看 39

基站

IP 地址 230

不联机/脱机, 9010/TCP/IP 主机 245

第一个终端 252

第一个终端, 9010/TCP/IP 主机 244

概述 219

工作模式 224

共用信道 225

基站编号 230

监测轮询, 9010/TCP/IP 主机 245

连接菜单 228-245

名称 230

配置 217-245

消息大小 231

窄带无线通信菜单 220-228

主机 242-245

主机编号 244, 252

自动启动 224, 231

最后一个终端, 9010/TCP/IP 主机

244

最后一个终端主机 252

9010/TCP/IP 主机 244, 252

基站配置 245

集群同步 56

集群自动同步的等待时间 56

集群自动同步的进度条 56

监测轮询, 9010/TCP/IP 仿真 245
 简单网络管理协议 (SNMP) 211
 箭头键重映射, *ANSI 仿真* 286
 将 IAC 中断流程作为系统请求发送 267

将 IAC 中断作为注意键发送, 3274
Telnet 协议 267

将 7 位转换为 8 位
ANSI 仿真 287

接口, 网络 316

接入点

MAC 过滤 173
 QoS 183

WDS 桥接 199

安全性 89

访客网络 151

负载平衡 177

集群 53

监控 117

无线设置 143

无线通信 163

以太网 (有线) 设置 133

用户管理 63

解决启动问题 40

仅转发 802.IQ 包, 802.IQ 298

警报

3274 仿真 255

5250 仿真 270

静态 WEP 安全模式

WDS 链路 203

何时使用 93

配置 101

K

可见匹配字符

3274 仿真 261

5250 仿真 276

客户端

安全性 C-5

关联 127

会话 59

会话, 定义 60

链路完整性监控 127

平台 29

控制台

端口

电缆编号 19387 B-2

引脚分配 B-1

连接至 22

L

联机/脱机消息 245

联网, 功能概述 12

连接

ANSI 兼容终端 22

控制台 22

以太网 20

连接菜单 242, 245

连接器

RJ-45 B-3

连接选项

RRM 模式 228

基站模式 223

链路完整性监控 127

邻居 83

流程

3274 仿真 257

5250 仿真 272

轮询 ID, 无线通信链路功能 239

轮询窗口的

数量

RRM 组 234

数量, 窄带无线通信 225

轮询窗口的大小

RRM 组 234

窄带无线通信 226

轮询协议参数

RA1001A 225

RRM 组 234

轮询协议终端超时, 无线通信链路功能 239

轮询协议终端超时百分比, 无线通信链路功能 239

M

密码

管理员的网络设置 47

基本设置 47

密钥管理, 安全性 92

命令区域

3274 仿真 264

5250 仿真 279

默认配置, 还原 244, 253

默认设置, 适用于 9160 G2 无线网关 25

N

内部接口设置, 以太网设置 138

内存 316

内核消息的日志中继主机, 事件日志
122

P

配置

微型控制器 247–292

配置 LU 名称

3274 *Telnet* 协议 266

配置设备名称

3274 *Telnet* 协议 282

批准 xv

平台

管理员要求 28

客户端要求 29

Q

启动网络 48

启用或禁用持久性, 事件日志 121

启用虚拟设备名称, 5250 *Telnet* 协议
281

强制网络门户 154

桥接, WDS 201

清除

3274 *仿真* 256

5250 *仿真* 271

渠道, 配置无线通信 167

全向天线 18

R

软件升级

802.1Qv2 295

S

上个主动会话密钥

ANSI Telnet 协议 289

设备名称前缀

5250 *Telnet* 协议 282

身份验证服务器

适用于 IEEE 802.1x 安全模式 106

适用于 WPA 企业版安全模式 112

深度, 事件日志 122

升级固件 8

时分复用 219

时间, 配置 AP 为使用 NTP 服务器 304

时间设置 303

时区 304

使用国际 EBCDIC

3274 *仿真* 254

5250 *仿真* 269

使用期限, 无线通信链路功能 241

事件

监控 120

日志 120

事件 120

视频显示终端, 连接 22

输入电压 (电源要求) 18, 316

输入行

3274 *仿真* 263

5250 *仿真* 278

数据速率, 串行 22

说明的出厂默认值 25

T

天线要求 18, 19

条码

3274 *仿真* 263

5250 *仿真* 278

通过 WDS 桥接扩展服务集 201

通过视频显示终端连接 22

通路

3274 *仿真* 256

5250 *仿真* 271

同步延迟

RRM 组 236

窄带无线通信 227

W

外部设备 19

网络接口 316

微型控制器

仿真 249

配置 247–292

网络 249

维护要求 18

位置, 描述 58

文本转换 6

无线

AP 功能概述 7

邻居 81

无线设置 143

无线通信

DTIM 周期 167

IEEE 802.11 模式 167

RA1001A 窄带 317

RTS 阈值 167

SuperAG 167

Turbo 广播模式, 不建议 7, 165

安装和天线 18

- 打开或关闭 167
 - 发射功率 167
 - 分段阈值 167
 - 规格 316
 - 集群 AP 的信道管理 71
 - 轮询 ID** 239
 - 轮询协议终端超时** 239
 - 轮询协议终端超时百分比** 239
 - 配置设置 167
 - 配置一个或两个无线通信 AP 167
 - 使用期限** 241
 - 速率设置 167
 - 协议 (自适应轮询, IEEE 802.11) 220
 - 信标间隔 167
 - 已安装配置 8
 - 状态指示灯 LED 21
 - 自动无线通信地址分配范围** 240
 - 自动终端号** 241
 - 最大工作站数量 167
 - 802.11A/G 无线通信 316
 - 802.11G 无线通信 316
 - 无线通信参数**
 - RA1001A 227
 - RRM 组 235
 - 无线通信卡的状态**
 - 窄带无线通信配置菜单 222
 - 无线通信链路功能**, 配置设置 237-242
 - 物理
 - 规格 315
 - 描述 315
- ## X
- 相邻接入点 128
 - 消息**
 - 大小 (基站) 231
 - 模式限值**
 - RRM 组 235
 - 模式限值**, 窄带无线通信 226
 - 小型可插拔模块 21
 - 协议
 - 无线通信
 - 蜂窝切换 219
 - 时分复用 219
 - 自适应轮询/争用 220
 - 自适应轮询/争用 220
 - 协议**
 - 类型 ID**, 802.IQv1 298
 - 写入错误代码**, 5250 仿真 269
- ## 信标
- UDP 端口**, 802.IQv2 299
 - 接口**, 802.IQv1 298
 - 周期**
 - 802.IQ 296
 - 信标间隔, 配置 167
- ## Y
- 严重性, 事件日志 121
 - 要绑定的本地 IP 地址**
 - ANSI Telnet 协议 288
 - 3274 Telnet 协议 266
 - 5250 Telnet 协议 280
 - 页面**
 - 3274 仿真 259
 - 5250 仿真 273
 - 页面保存**
 - ANSI 仿真 286
 - 页面保存考虑双字节字符**, ANSI 仿真 286
 - 以蜂窝模式运行**, 无线通信链路功能 239
 - 以太网
 - 电缆长度 21
 - 基站 230
 - 连接 20
 - 设置 133, 157
 - 适配器卡 316
 - 状态指示灯 LED 21
 - 10BaseT 20
 - 引脚分配 B-3
 - 100Base-FX 光纤 21
 - 100BaseT 20
 - 引脚分配 B-3
 - 以太网供电规格 316
 - 以太网连接 20, 36
 - 引脚分配 参阅**端口引脚分配**
 - 隐藏匹配字符**
 - 3274 仿真 262
 - 5250 仿真 277
 - 硬件连接 36
 - 用户
 - 身份验证
 - 在 IEEE 802.1x 客户端上配置 C-15
 - 在 WPA/WPA2 企业版 (RADIUS) 客户端上配置 C-23

- 帐户
 - 备份和还原 69
 - 适用于内置身份验证服务器 63
- 有线设置 133, 157
- 与 QoS 相关的 ToS 186
- 与 QoS 相关的帧间间隔 187
- 远程传输开启时间
 - RRM 组 236
 - 窄带无线通信 228
- 远程打印
 - 3274 仿真 258
 - 5250 仿真 273
- 允许
 - TCP 会话, ANSI Telnet 291
- 允许 Null 字符
 - 3274 仿真 254
 - 5250 仿真 269
- 阈值
 - ANSI 仿真 285

Z

- 在没有用户操作定时延迟的情况下自动 Telnet
 - ANSI Telnet 协议 291
- 在用户不操作的情况下自动 Telnet
 - ANSI Telnet 协议 291
 - 3274 Telnet 协议 268
 - 5250 Telnet 协议 281
- 窄带无线通信
 - 端口参数 228
 - 活动信道参数 228
 - 连接选项, RRM 模式 228
 - 连接选项, 基站模式 223
 - 轮询协议参数 225
 - 配置设置 220, 228
 - 无线通信参数 227
 - 2 级调制 227
 - 4 级调制 227
- 站点
 - 配置最大允许数量 167
- 站点隔离 98
- 证书
 - IEEE 802.1x 客户端的安全性 C-19
 - WPA/WPA2 企业版 (RADIUS) 客户端的安全性 C-27
 - 获取客户端 TLS-EAP 证书 C-37
- 支持的平台
 - 管理员 28
 - 客户端 29

- 直接 TCP 检查重复终端号, 无线通信链路功能 240
- 终端
 - 连接视频显示器 22
- 终端类型
 - ANSI Telnet 协议 288
 - 3274 Telnet 协议 265
 - 5250 Telnet 协议 279
- 离线超时
 - 802.1Q 296
- 终端初始化数据, ANSI 仿真 287
- 终端范围, 主机菜单 252
- 终端范围, 主机菜单 252
- 终端范围, 主机菜单 (9010 仿真) 244
- 终端范围, 主机菜单 (9010 仿真) 244
- 终端重置时关闭主机会话
 - ANSI Telnet 协议 288
- 重试
 - 次数
 - RRM 组 235
 - 次数, 窄带无线通信 226
- 重试, 次数 226
- 主动与主机协商
 - 3274 Telnet 协议 266
 - 5250 Telnet 协议 280
- 主机
 - 超时
 - ANSI 仿真 284
 - 打印
 - 3274 仿真 257
 - 5250 仿真 272
 - 端口
 - ANSI Telnet 协议 288
 - 3274 Telnet 协议 265
 - 5250 Telnet 协议 280
 - 微型控制器配置 250
 - 主机 (基站配置) 242–245
 - 主机编号, 基站配置 244, 252
- 主机菜单
 - 微型控制器 253
- 主机初始化数据, ANSI 仿真 287
- 主机是否为 Fujitsu
 - 3274 仿真 254
- 转义超时, ANSI 仿真 285
- 状态指示灯 (LED) 21
- 自动 Telnet
 - 3274 Telnet 协议 267
 - 5250 Telnet 协议 280

自动 Telnet, ANSI Telnet

密码 290

终端提示 290

主机 290

自动 Telnet/登录启用 289

自动 Telnet 主机

3274 Telnet 协议 267

5250 Telnet 协议 281

自动 Telnet 最多尝试次数

ANSI Telnet 协议 291

自动登录, ANSI Telnet

登录失败 291

密码 291

用户 ID 290

自动 Telnet/登录启用 289

自动启动

(基站) 231

RRM 组 233

802.IQ 295

自动启动, 基站模式 224**自动无线通信地址分配范围, 无线通信**

链路功能 240

自动终端号, 无线通信链路功能 241**自适应轮询/争用协议 220****自由**

窗口外形尺寸

RRM 组 235

窗口外形尺寸, 窄带无线通信 226

字段开销

3274 仿真 264

5250 仿真 278

字段下划线重新映射

5250 仿真 270

组参数, RRM 组 236**组合, RRM 组 236****最大**

消息段大小

RRM 组 234

消息段大小, 窄带无线通信 226

最大值

每个终端的会话数量

ANSI Telnet 协议 288

3274 Telnet 协议 265

5250 Telnet 协议 280

屏幕尺寸, ANSI 仿真 284

数字

10BaseT 以太网 20, B-3

100Base-FX 光纤端口 21

100BaseT 以太网 20, B-3

3274/Telnet 254-268

协议 267

5250 仿真 269-283

802.IQ

协议概述 295

信标周期 296

终端离线超时 296

自动启动 295

802.IQv1

初始 RTT 298

功能菜单 298

仅转发 802.IQ 包 298

描述 295

协议类型 ID 298

信标接口 298

802.IQv2

功能菜单 299

描述 295

信标 UDP 端口 299

802.1p 标签 189

802.11A/G 无线通信 316

802.11G 无线通信 316

802.11 高级设置 (无线通信设置

页面) 165, 171

802.11 设置 (无线设置页面) 145, 150

9010 / TCP/IP, 基站配置 244, 252

9010 仿真 245

9010 配置 245

9500 通信服务器, 蜂窝模式 239

