“十三五”职业教育国家规划教材

无线短距离通信技术开发项目教程（第2版）

主　编　张玲丽　虞　沧


课件


微课


教学大纲

西南交通大学出版社
·成　都·

第 2 版前言

物联网是一场技术重塑的革命，一方面由技术自上而下驱动，另一方面由需求自下而上驱动。传输方式分为有线和无线两种，在无线传输系统中，短距离无线传输技术成为物联网技术中的一个重要分支，从生活、生产、公共领域等重构城市建设，为城市治理提供了新的发展模式。物联网行业的迅猛发展，对电子信息领域的人才培养提出了更高要求，需要大量网络建设和维护人员，本书以真实案例为主线，紧跟技术发展的脚步，在第 1 版的基础上进行了更新改进。

为了满足市场需求，本书在编写和安排上突出以市场需求和岗位需求为导向，以岗位技能和职业素质培养为目标，旨在实现“知识、技能、态度、素质”人才四要素融合。

全书重点分析了当前无线短距离通信技术典型的应用开发实例：从广为人知的 WiFi 技术的应用出发，对比多种无线通信技术，最后以在物联网技术中肩负重任的 ZigBee 技术为基于协议栈项目开发的蓝本，向读者展示基于协议栈编程的一般流程和方法。学生学习后能动手实现单播、组播、广播等多种数据传输方式，完成温度、湿度、光照度等采集数据的成功传送或控制。

本教材已用于武汉职业技术学院现代通信技术专业和潍坊工程职业技术学院物联网技术专业等高职院校，使用教材的老师和同学们均反馈教材结构合理，知识体系上循序渐进，实用操作性强，对入门和提高者尤其适用。2021 年，该书被教育部评选为“十三五”职业教育国家规划教材，为促进人才培养与产业需求紧密衔接，有效支撑我国产业结构深度调整、新旧动能接续转换，进一步深入推进产教研融合，本书通过校企联合制定培养目标和培养方案，共同建设课程与开发教材，该书此次修订主要包括以下方面：

第一，项目设计无痕地植入“课程思政”。结合学生的兴趣点融入职业规范和素养，采用教、学、做一体化模式，使学生熟练掌握短距离通信中 ZigBee 技术开发的基础知识，让学生既要对基于协议栈开发的思路架构有一个整体认知，又能在现有网络的基础上设计扩容或完成新建，覆盖规划和容量计算，还能对特定网络设备的工作特性、应用方式、配置、设计等有所掌握，面对运维、营销与服务等工作展现出综合应用能力和职业素质能力；对各项操作均能遵守严格的操作规范，具有认真负责、一丝不苟的工作态度。

第二，全面更新、整合教材内容，由原教材的 20 个实训项目调整为此版的 21 个实训项目。调整了项目五～十的顺序，同时增加了项目九——无线点灯实验，使得各个项目以及任务安排更符合学生的学习、认知规律；将每个任务的教学重、难点进行了分解和逐个击破，对每个项目实施的具体网络环境、开发工具等都有详细的图文操作步骤。ZigBee 功能强大，组网方式灵活，官方标准协议栈的代码定义多，函数调用复杂。本书在内容编排上按基本概念和原理、实际应用、技能训练的顺序展开，并附有习题。通过网络搭建、节点功能、数据传输、有效控制等实验，突出重点，各个击破，争取从实践的角度找到与理论的吻合点。同时注重培养学习者规范化编程的习惯，能够看懂协议栈进行二次开发，具备程序调试的能力。

第三，教材配套的数字化资源更加丰富。所有项目涉及的编程任务都配有源代码和详细的注解，可操作性和通用性强。同时，在教材中穿插了很多在线视频二维码，读者通过扫描二维码可在线观看相关视频，帮助消化吸收。本课程在编写及授课过程中积累了大量的教辅材料，课程已在职教云平台上线：https://zjy2.icve.com.cn/teacher/mainCourse/mainClass.html?courseOpenId=zp6rabgp2ytmaejuad5u3w，读者可以在平台上下载书籍资料及相关软件工具、练习文件和程序源代码，也可以通过平台对数据内容、质量等进行反馈。后期计划在慕课平台等同步上线，吸引更多的技术爱好者，共同促进技术的发展与进步。

本书由张玲丽和虞沧担任主编，王金龙、王碧芳、廖骏杰、张帆参与编写。其中项目一到项目四由潍坊工程职业学院的王金龙老师编写，项目五到项目七由武汉职业技术学院的王碧芳老师编写，项目八到项目十由武汉职业技术学院的虞沧老师编写，项目十一和项目十二由武汉职业技术学院的廖骏杰老师编写，项目十三到项目十四由武汉职业技术学院的张帆老师编写，项目十五到项目二十一由武汉职业技术学院的张玲丽老师编写。由于编者水平有限，难免有不当之处，恳请广大读者批评指正！

编　者

2022 年 2 月

第 1 版前言

当前，带有物联网元素的智能手表、智能手环，以及智能家居等产品已经越来越多地渗透到我们的生活当中，这些设备都是物联网中的联网设备。从技术上来说，物联网可以分为三层：传感层、通信层和应用层。在通信层中，需要将这些数据和信息进行安全可靠的通信和传输。传输方式分为有线和无线两种，在无线传输系统中，短距离无线传输技术成为物联网技术中的一个重要分支。

为了满足市场需求，本书在编写和安排上突出以市场需求和岗位需求为导向，以岗位技能和职业素质培养为目标，旨在实现“知识、技能、态度、素质”人才四要素融合。全书重点分析了当前无线短距离通信技术典型的应用开发实例，其主线是：从广为人知的 WiFi 技术的应用出发，对比多种无线通信技术，最后以在物联网技术中肩负重任的 ZigBee 技术为基于协议栈项目开发的蓝本，向读者展示基于协议栈编程的一般流程和方法。学生学习后能动手实现单播、组播、广播等多种数据传输方式，完成温度、湿度、光照度等采集数据的成功传送或控制。

本书内容编排上循序渐进，先阐述基本概念和原理，接着介绍应用，然后提供实验示例供操作、练习，并附有习题。通过网络搭建、节点功能、数据传输、有效控制等实验，突出重点，各个击破，争取从实践的角度去找到与理论的吻合点。本书采用项目式的编排方式，便于教学安排，也可以作为课程设计、毕业设计、技术开发等的参考用书。

本书由张玲丽和虞沧担任主编，王金龙、王碧芳、廖骏杰、张帆参与编写。其中项目一到项目四由潍坊工程职业学院的王金龙老师编写，项目五到项目七由武汉职业技术学院的王碧芳老师编写，项目八到项目十由武汉职业技术学院的虞沧老师编写，项目十一和项目十二由武汉职业技术学院的廖骏杰老师编写，项目十三到项目十四由武汉职业技术学院的张帆老师编写，项目十五到项目二十由武汉职业技术学院的张玲丽老师编写。由于编者水平有限，难免有不当之处，恳请广大读者批评指正！

编　者

2018 年 10 月

数字资源列表

序号	资源名称	资源类型	资源位置	资源页码
1	认识 ZigBee 技术	PPT	项目三	023
2	ZigBee 技术基础	视频	项目三	024
3	ZigBee 无线传感网入门	PPT	项目四	037
4	ZigBee 协议和协议栈	PPT	项目五	044
5	ZStack 协议栈的安装、功能及使用介绍	视频	项目五	053
6	实验系统硬件介绍	PPT	项目六	057
7	CC2530 硬件资源介绍	视频	项目六	058
8	感知 RF2 试验箱	视频	项目六	059
9	实验开发套件介绍	视频	项目六	061
10	IAR 基础习题讲解	视频	项目六	067
11	IAR 工程的编辑与修改	PPT	项目七	069
12	基于 CC2530 的按键控制 LED 灯	PPT	项目八	079
13	按键控制 LED 灯的实验原理	视频	项目八	080
14	按键控制 LED 灯的编程	视频	项目八	082
15	如何新建及配置功能	视频	项目八	083
16	按键控制 LED 灯重点代码解析	视频	项目八	085
17	按键控制 LED 灯习题讲解	视频	项目八	088
18	基于 Basic RF 无线点灯实验	PPT	项目九	090
19	无线点灯实验原理	视频	项目九	091
20	无线点灯实验目标及关键步骤	视频	项目九	095
21	无线点灯代码实现	视频	项目九	095
22	无线点灯习题讲解	视频	项目九	100
23	精简 OS 实验	PPT	项目十一	116
24	OSAL 运行机理	视频	项目十一	118

25	协议栈寻找 OSAL 的踪迹	视频	项目十一	120
26	OSAL 如何进行任务初始化	视频	项目十一	126
27	OSAL 如何进行事件处理	视频	项目十一	132
28	精简 OSAL 习题讲解	视频	项目十一	134
29	点对点数据传输实验	PPT	项目十二	135
30	点到点数据传输实验原理介绍	视频	项目十二	136
31	点到点数据传输的代码实现	视频	项目十二	137
32	如何修改信道、PAN ID 及正确地配置工程	视频	项目十二	145
33	片内温度检测实验	PPT	项目十三	156
34	无线温度检测实验原理	视频	项目十三	157
35	无线温度检测实验代码实现	视频	项目十三	159
36	无线温度检测故障工程解决	视频	项目十三	163
37	单播与广播实验	PPT	项目十七	212
38	单播与广播实验原理	视频	项目十七	215
39	单播与广播代码实现	视频	项目十七	217
40	组播实验	PPT	项目十八	226
41	组播原理及实现流程	视频	项目十八	227
42	组播的代码实现	视频	项目十八	230
43	书中实验源代码			

目 录

项目一

WiFi 标准及基本 WLAN 网络组建 ……1

第一部分　教学要求 ……1
第二部分　教学内容 ……2
一、WLAN 基础 ……2
二、WLAN 结构 ……6
第三部分　技能训练 ……7
一、Ad-Hoc 对等无线网络组建 ……7
二、Ad-Hoc 对等无线网络接入 Internet 7
三、Infrastructure 无线网络组建 ……8
四、Infrastructure 无线网络接入 Internet 9
五、知识点考核 ……10

项目二

利用无线路由器组建 WLAN 网络 ……11

第一部分　教学要求 ……11
第二部分　教学内容 ……12
一、路由器的特点 ……12
二、路由器的功能 ……12
三、路由器级别 ……13
四、不同型号路由器的重要参数对比 ··16
第三部分　技能训练 ……17
一、无线路由器的基本配置 ……17
二、路由器+路由器级联模式 ……20
三、路由器+AP 模式 ……21
四、知识点考核 ……22

项目三

认识 ZigBee 技术 ……23

第一部分　教学要求 ……23
第二部分　教学内容 ……24
一、无线网络数据传输协议对比 ……24
二、ZigBee 技术的定义及特点 ……25
三、ZigBee 设备类型 ……25
四、ZigBee 网络的拓扑结构和路由 ····26
五、高可靠性的无线网络 ……28
六、安全和加密 ……31
第三部分　技能训练 ……33
一、ZigBee 容量计算与网络结构规划 ·33
二、知识点考核 ……35

项目四

ZigBee 无线传感网入门 ……37

第一部分　教学要求 ……37
第二部分　教学内容 ……38
一、ZigBee 信道 ……38
二、网络 PAN ID ……39
三、IEEE 物理地址 ……40
四、网络地址 ……40
五、ZigBee 无线传感器网络 ……40
第三部分　技能训练 ……41
一、物理地址烧写工具的使用 ……41
二、知识点考核 ……43

项目五
ZigBee 协议和协议栈 ……44
第一部分　教学要求 ……44
第二部分　教学内容 ……45
一、ZigBee 体系结构 ……45
二、ZigBee 协议栈软件层次 ……47
三、ZigBee 2007/PRO 协议栈 ……50
第三部分　技能训练 ……52
一、熟悉 ZigBee 协议栈开发基本思路 ·52
二、如何使用 ZigBee 协议栈 ……52
三、ZigBee 协议栈的安装和目录结构 ·53
四、ZStack 在项目中的目录结构 ……54
五、知识点考核 ……55
项目六
实验系统硬件介绍 ……57
第一部分　教学要求 ……57
第二部分　教学内容 ……58
一、ZigBee 芯片方案 ……58
二、CC2530 简介 ……58
三、感知 RF2 实验箱
——WSN 系统结构 ……59
四、感知 RF2 实验箱——WSN 系统工作
流程 ……59
五、感知 RF2 实验箱——WSN 硬件介绍
……61
第三部分　技能训练 ……65
一、仿真调试与下载 ……65
二、知识点考核 ……67
项目七
IAR 工程的编辑与修改 ……69
第一部分　教学要求 ……69
第二部分　教学内容 ……70
一、IAR 集成开发环境简介 ……70
二、模块化编程技巧 ……70
第三部分　技能训练 ……71
一、工程的编辑与修改 ……71
二、知识点考核 ……78
项目八
基于 CC2530 实现按键控制 LED 灯 ……79
第一部分　教学要求 ……79
第二部分　教学内容 ……80
一、实验原理 ……80
二、硬件电路 ……81
第三部分　技能训练 ……82
一、编写代码 ……82
二、实验关键步骤 ……83
三、验证实验结果 ……87
四、知识点考核 ……88
项目九
基于 Basic RF 无线点灯实验 ……90
第一部分　教学要求 ……90
第二部分　教学内容 ……91
一、实验原理 ……91
二、Basic RF layer 介绍及其工作过程 ·92
三、硬件电路 ……94
第三部分　技能训练 ……95
一、编写代码 ……95
二、验证实验结果 ……97
三、拓展实验 ……97
四、知识点考核 ……100
项目十
串口收发的实现 ……101
第一部分　教学要求 ……101
第二部分　教学内容 ……102
一、实验原理 ……102
二、硬件电路 ……105
三、代码分析 ……106
第三部分　技能训练 ……110

一、编写代码 ……110
二、实例测试 ……113
三、知识点考核 ……115

项目十一
精简 OS 实验 ……116

第一部分　教学要求 ……116
第二部分　教学内容 ……117
一、操作系统（OS）基本术语 ……117
二、操作系统表象层（OSAL）运行机理 ……118
三、代码分析 ……119
第三部分　技能训练 ……125
一、编写代码 ……125
二、验证实验结果 ……131
三、知识点考核 ……134

项目十二
点对点数据传输实验 ……135

第一部分　教学要求 ……135
第二部分　教学内容 ……136
一、实验效果要求 ……136
二、实验原理 ……136
第三部分　技能训练 ……137
一、协调器编程 ……137
二、终端节点编程 ……148
三、实例测试 ……154
四、知识点考核 ……154

项目十三
片内温度检测实验 ……156

第一部分　教学要求 ……156
第二部分　教学内容 ……157
一、实验原理及流程图 ……157
二、重点代码解析 ……158
第三部分　技能训练 ……159
一、协调器编程 ……159
二、终端节点编程 ……163
三、实例测试 ……168
四、知识点考核 ……169

项目十四
加入网络实验 ……170

第一部分　教学要求 ……170
第二部分　教学内容 ……171
一、协调器初始化网络 ……171
二、节点加入网络 ……173
第三部分　技能训练 ……177
一、编写代码 ……177
二、验证实验结果 ……184
三、知识点考核 ……187

项目十五
简单绑定实验 ……188

第一部分　教学要求 ……188
第二部分　教学内容 ……189
一、绑定原理 ……189
二、重要的数据结构 ……189
三、ZStack 绑定流程分析 ……190
第三部分　技能训练 ……197
一、验证实验结果 ……197
二、知识点考核 ……199

项目十六
自动匹配实验 ……200

第一部分　教学要求 ……200
第二部分　教学内容 ……201
一、自动匹配分析 ……201
二、代码分析 ……206
第三部分　技能训练 ……208
一、验证实验结果 ……208
二、知识点考核 ……211

项目十七
单播与广播实验 ……212
第一部分　教学要求 ……212
第二部分　教学内容 ……213
一、单播、组播、广播 ……213
二、实验原理 ……215
第三部分　技能训练 ……217
一、协调器程序设计 ……217
二、终端节点程序设计 ……221
三、实例测试 ……224
四、知识点考核 ……225
项目十八
组播实验 ……226
第一部分　教学要求 ……226
第二部分　教学内容 ……227
一、ZigBee 网络通信方式 ……227
二、代码分析 ……230
第三部分　技能训练 ……234
一、验证实验结果 ……234
二、知识点考核 ……236
项目十九
传感器采集 SensorDemo 实验 ……237
第一部分　教学要求 ……237
第二部分　教学内容 ……238
一、在应用层启动网络 ……238
二、启动传感节点网关 ……241
三、采集节点和传感节点的绑定 ……244
第三部分　技能训练 ……248
一、验证实验结果 ……248
二、知识点考核 ……253
项目二十
温度传感器实验 ……254
第一部分　教学要求 ……254
第二部分　教学内容 ……255
一、温度传感器 TC77 特性 ……255
二、硬件电路 ……256
三、代码分析 ……256
四、数据格式解析 ……258
第三部分　技能训练 ……259
一、验证实验结果 ……259
二、知识点考核 ……263
项目二十一
光照传感器实验 ……264
第一部分　教学要求 ……264
第二部分　教学内容 ……265
一、CDS 光敏电阻特性 ……265
二、硬件电路 ……266
三、代码分析 ……267
四、数据格式解析 ……271
第三部分　技能训练 ……272
一、验证实验结果 ……272
二、知识点考核 ……278
参考文献 ……279

项目一　WiFi 标准及基本 WLAN 网络组建

第一部分　教学要求

<table>
<tr><td>一、目的要求</td><td colspan="3">1. 了解 WLAN 基础；
2. 掌握多种 WLAN 的结构及相应的配置</td></tr>
<tr><td rowspan="6">二、工具、器材</td><td>实 验 设 备</td><td>数 量</td><td>备　　注</td></tr>
<tr><td>TP-Link 无线 AP</td><td>1</td><td>创建无线网络</td></tr>
<tr><td>PC 机</td><td>3</td><td>配置无线设备</td></tr>
<tr><td>无线网卡</td><td>3</td><td>无线接入</td></tr>
<tr><td>有线网卡</td><td>1</td><td>有线接入</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td>三、重难点分析</td><td colspan="3">重点：
1. 802.11 协议不同版本之间的差别及工作频段划分；
2. 思路清晰地设置相关基本结构的 WiFi 网络连接
难点：
1. WLAN 和 WiFi 的区别；
2. WiFi 的频段布局，不同版本 802.11 协议在调制手段、速率和兼容性上的区别；
3. WiFi 加密的原理和手段</td></tr>
<tr><td colspan="4">四、教学过程</td></tr>
<tr><td>教学步骤/知识或单元结构</td><td colspan="2">教学方式/方法/策略</td><td>学生活动安排/过程</td></tr>
<tr><td>1. WLAN 基础</td><td colspan="2">讲授 WLAN 相关基础知识</td><td>查询资料了解 WLAN 和 WiFi 的联系和差别</td></tr>
<tr><td>2. WLAN 结构</td><td colspan="2">初步讲解两种基本的 WLAN 网络拓扑结构</td><td>查询资料了解新结构，如 Mesh 结构</td></tr>
<tr><td>3. Ad-Hoc 对等无线网络组建</td><td colspan="2">引导学生思考此处对等网络中的 PC 机的 IP 地址属性该如何设置，以及如何创建无线网络</td><td>组网并完成无线网卡的软硬件安装及测试，连接网络后测试连通性</td></tr>
<tr><td>4. Ad Hoc 网络接入 Internet</td><td colspan="2">创设情境，让学生自主完成将 Ad-Hoc 对等无线网络接入 Internet</td><td>理解实验要求，完成相应功能</td></tr>
<tr><td>5. Infrastructure 无线网络组建</td><td colspan="2">演示 AP 的配置方法</td><td>组网完成相应功能，并和 Ad-Hoc 对等无线网络组建比较</td></tr>
<tr><td>6. Infrastructure 网络接入 Internet</td><td colspan="2">引导学生思考如何修改 AP 及终端的设置使其接入 Internet</td><td>完成相应功能并思考借助其他无线设备如何接入 Internet</td></tr>
<tr><td>7. 布置作业</td><td colspan="2">练习</td><td>强化课堂认知技能</td></tr>
<tr><td colspan="4">五、成绩评定</td></tr>
<tr><td>评定等级</td><td colspan="2"></td><td>教师签名</td></tr>
</table>

第二部分　教学内容

一、WLAN 基础

无线技术让网络使用更自由，使任何自由空间均可连接网络，不受限于线缆和端口位置，尤其适用于特殊地理环境下的网络架设，如隧道、港口码头、高速公路。无线网相对于有线网具有安装便捷、使用灵活、易于扩展等优点，但也存在设备价格昂贵、覆盖范围小、网络速度较慢等不足，因此，通常应用于局域网的范围，即无线局域网（Wireless Local Area Network，WLAN）。广义的 WLAN 是指通过无线通信技术将计算机设备互联起来，构成通信网络；狭义的 WLAN 是指采用 IEEE 802.11 无线技术进行互联的通信网络。目前的 WLAN 一般指 802.11 无线网络，802.11 是处于 2.4 G/5.8 G 频段，以电磁波传播的无线网络。在 802.11 标准发展历程中的多个版本中，表 1-1 为比较有代表性的版本。

表 1-1　典型 802.11 协议对比

版本号	802.11	802.11b	802.11a	802.11g	802.11n
标准发布时间	1997	1999	1999	2003	2007
合法频宽/MHz	83.5	83.5	325	83.5	83.5
频率范围/GHz	2.400 ~ 2.483	2.400 ~ 2.483	5.725 ~ 5.850	2.400 ~ 2.483	2.402 ~ 2.483
非重叠信道	3	3	5	3	3
调制技术	FHSS/DSSS	CCK/ DSSS	OFDM	CCK/OFDM	QAM
物理发送速率/（Mb/s）	1, 2	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54	2
兼容性	N/A	与 11 g 产品可互通	与 11 b/g 不能互通	与 11 b 产品可互通	与 11 g 产品可互通

802.11 标准的发展一直没有停下脚步，802.11ac、802.11ad、802.11e、802.11f 等仍然在致力于传输距离和速率应用等方面的发展和提升。

802.11 协议在 2.4 GHz 频段定义了 14 个信道，每个频道的频宽为 22 MHz。两个信道中心频率之间为 5 MHz。信道 1 的中心频率为 2.412 GHz，信道 2 的中心频率为 2.417 GHz，依此类推至位于 2.472 GHz 的信道 13。信道 14 是特别针对日本所定义的，其中心频率与信道 13 的中心频率相差 12 MHz。在北美地区（美国、加拿大）开放 1 ~ 11 信道，在欧洲开放 1 ~ 13 信道，我国与欧洲一样。802.11 b/g 工作频段划分如图 1-1 所示。

从图 1-1 可以看到，信道 1 在频谱上和信道 2、3、4、5 都有交叠的地方，这就意味着：如果有两个无线设备同时工作，且它们工作的信道分别为 1 和 3，则它们发送出来的信号会互相干扰。为了最大限度地利用频段资源，可以使用 1、6、11；2、7、12；3、8，13；4、

9、14 这四组互相不干扰的信道来进行无线覆盖。由于只有部分国家开放了 12～14 信道频段，所以一般情况下，使用 1、6、11 这 3 个信道。为了达到上述目的，我们采用蜂窝式覆盖原则，如图 1-2 所示。

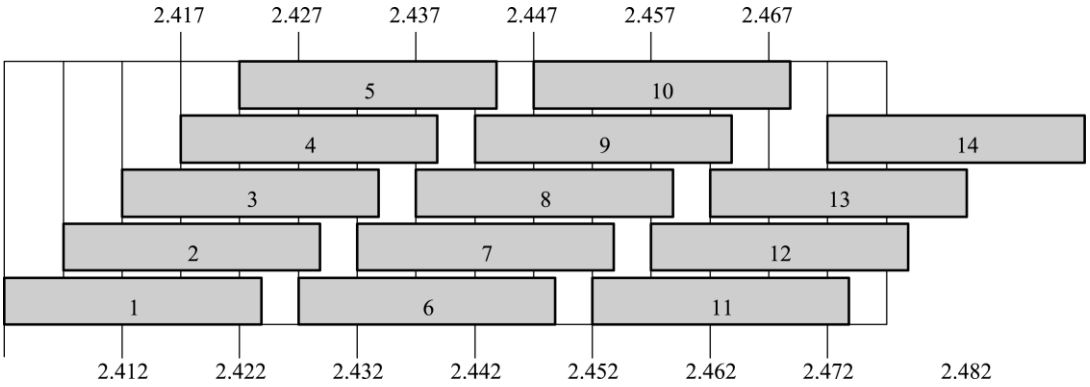

图 1-1　802.11b/g 工作频段划分

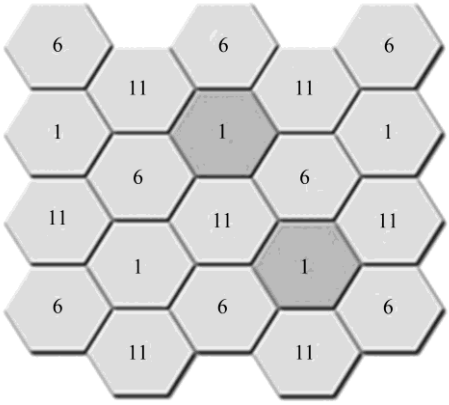

图 1-2　蜂窝式无线覆盖原则示意图

所谓的蜂窝式覆盖原则可以简单地概括为：任意相邻区域使用无频率交叉的频道，如：1、6、11 频道；适当调整发射功率，避免跨区域同频干扰；蜂窝式无线覆盖实现无交叉频率重复使用。

WiFi 联盟（WiFi Alliance）是一家全球非营利性的行业协会，拥有 300 多家成员企业，共同致力于推动 WLAN 产业的发展。以增强移动无线、便携、移动和家用设备的用户体验为目标，WiFi 联盟一直致力于通过其测试和认证方案确保基于 IEEE 802.11 标准的无线局域网产品的可互操作性。自 2000 年 3 月 WiFi 联盟开展此项认证以来，已经有超过 4 000 种产品获得了 WiFi CERTIFIED™指定认证标志，有力地推动了 WiFi 产品和服务在消费者市场和企业市场两方面的全面开展。

如今很多电商平台在推销自家产品的时候都会提到 WiFi 6 这个词，作为新一代的无线通信技术，WiFi 6 和 WiFi 5、WiFi 4 究竟有什么区别呢?

WiFi 6 是由 WiFi 联盟提出的命名规则，它将 802.11ax 改为 WiFi 6，这个 WiFi 标准彻底改变了传统的命名方式，它放弃了 802.11 命名的方案，使用了数字序号，相当于 WiFi 6.0

的版本。与此同时，802.11b 被称为 WiFi 1，从表 1-1 可以看出其速率非常不尽人意，无法和现在的主流技术 WiFi 5、WiFi 6 媲美，但在当时的确解决了有线局域网的局限。802.11a 即 WiFi 2, 802.11g 即 WiFi 3, 802.11n 即 WiFi 4，而 802.11ac 即 WiFi 5, 802.11ax 即 WiFi 6（见表 1-2）。

表 1-2　WiFi 4~WiFi 6 主要参数对比

参数	WiFi 4	WiFi 5	WiFi 6
信道带宽/MHz	20,40	20,40,80+80,160	20,40,80+80,160
频段	2.4 G & 5 G	5 G	2.4 G & 5 G
最大传输速率	150 Mb/s	3.5 Gb/s	9.6 Gb/s
最大子载波调制	64-QAM	256-QAM	1024-QAM
空间流	1	4	8
底层技术	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

WiFi 6 包含一系列新技术，这些技术结合在一起使 WiFi 更加高效。虽然其速度也有所提升，从 WiFi 5 的 3.5 Gb/s 提升到 9.6 Gb/s，但这两个速度都是理论上的最大值，在现实世界中是不可能达到的。WiFi 6 最大的作用不是提升单个设备的速度，而是在大量设备连接时改善网络。WiFi 6 引入了一些新技术，帮助缓解将数十台 WiFi 设备放在一个网络内所带来的问题。它允许路由器与更多的设备通信，允许路由器在同一次广播中向多个设备发送数据，并允许 WiFi 设备自己安排与路由器的签入动作。总之，即使越来越多的设备需要数据，这些功能也能保持强大的连接。通俗地讲，之前的 WiFi 5 的方案（OFDM）就好比按订单发车，不管货物大小，来一单发一趟，哪怕是一小件货物，也发一辆车，这就导致车厢经常是空荡荡的，效率低下，浪费了资源。新方案（OFDMA）则会将多个订单聚合起来，尽量让卡车满载上路，使得运输效率大大提升。WiFi 6 厉害的另一个体现是其抗干扰能力。我们说，WiFi 信号无处不在，这使得无线信号之间的干扰也是无处不在的，总的来说，干扰主要来自相邻频段的无线电波叠加和同频干扰，而 WiFi 6 提出了一种信道空间复用技术（spatial reuse technique），极大地解决了此前由于信号的交叉覆盖而引起的干扰，理论上能彻底解决普通家庭的信号覆盖问题。无线相比较于有线通信方式在保密性等方面是有缺陷的，因此 WiFi 这种技术要得到应用，认证、加密、完整性校验等就是不容忽视的功能。网络的安全机制都有自己的协议标准，就如同我们的社会需要法律约束以确保社会的安定。无线局域网（WLAN）安全标准大致有 3 种，分别是 WEP、WPA 和 WAPI。

1. WEP

WEP（Wired Equivalent Privacy）是 802.11b 采用的安全标准，用于提供一种加密机制，保护数据链路层的安全，使无线网络 WLAN 的数据传输安全达到与有线 LAN 相同的级别。WEP 采用 RC4 算法实现对称加密。通过预置在 AP（Access Point，无线接入点）和无线网卡间共享密钥，在通信时，WEP 标准要求传输程序创建一个特定于数据包的初始化向量（IV），将其与预置密钥相组合，生成用于数据包加密的加密密钥。接收程序接收此初始化向量，并将其与本地预置密钥相结合，恢复出加密密钥。

WEP 允许 40 bit 长的密钥，这对于大部分应用而言都太短。同时，WEP 不支持自动更

换密钥，所有密钥必须手动重设，这导致了相同密钥的长期重复使用。另外，尽管使用了初始化向量，但初始化向量被明文传递，并且允许在 5 h 内重复使用，对加强密钥强度并无作用。此外，WEP 中采用的 RC4 算法被证明是存在漏洞的。综上，密钥设置的局限性和算法本身的不足使得 WEP 存在较明显的安全缺陷，WEP 提供的安全保护效果，只能被定义为“聊胜于无”。

2. WPA

WPA（WiFi Protected Access）是保护 WiFi 登录安全的装置。早期有 WPA 和 WPA2 两个版本，是 WEP 的升级版本，针对 WEP 的几个缺点进行了弥补。WPA 是 802.11i 的组成部分，在 802.11i 没有完备之前，是 802.11i 的临时替代版本。

不同于 WEP，WPA 同时提供加密和认证。它保证了数据链路层的安全，同时保证了只有授权用户才可以访问无线网络 WLAN。WPA 采用 TKIP（Temporal Key Integrity Protocol）作为加密协议，该协议提供密钥重置机制，并且增强了密钥的有效长度，通过这些方法弥补了 WEP 协议的不足。认证可采取两种方法：一种采用 802.11x 协议方式，一种采用预置密钥 PSK 方式。

2018 年 WiFi 联盟正式推出了新的 WiFi 安全标准 WPA3，该标准将解决现有安全标准下已知的所有安全问题,并且将缓解诸如 KRACK 攻击和 DEAUTH 等无线攻击带来的影响。WPA3 为支持 WiFi 的设备进行了重点改动，大大增强了配置、身份验证和加密功能。

WPA3 标准包括个人、企业两种模式，同时还可以应用于物联网领域。

新标准带来的改进包括：

1）针对暴力破解攻击的防护功能

WPA3 针对离线字典暴力破解提供安全防护，即使用户没有使用较复杂的密码。

2）正向加密功能

WPA3 具有强大的正向加密功能，即使攻击者成功破解密码也能够为用户提供通信隐私。

3）增强了公共/开放区域的 WiFi 网络下对用户隐私的保护

WPA3 通过个性化数据加密增强了开放网络环境下对用户隐私的保护。任何设备和 WiFi 接入点之间的通信都是加密的，能够有效阻止 MitM 攻击。

通过使用 OWE（Opportunistic Wireless Encryption）来防止用户被第三方窃听，同时为每位用户提供单独的加密方式，以保证设备与 WiFi 接入点之间的网络信道安全。

4）增强关键网络的防护性

为类似于政府、金融机构使用的关键网络提供 192 位加密。

除此之外，WiFi 联盟还发布了 WiFi Easy Connect，这项新功能简化了物联网设备与无线网络之间的连接。该功能替代了此前的 WiFi 保护设置（WPS），后者在使用过程中已经屡遭质疑。新功能允许用户仅通过扫描二维码便可以将新的 WiFi 证书发送到新的设备中。

3. WAPI

WAPI（WLAN Authentication and Privacy Infrastructure）是我国自主研发并大力推行的无线网络 WLAN 安全标准，它通过了 IEEE（注意，不是 WiFi）认证和授权，是一种认证和私密性保护协议，其作用类似于 802.11b 中的 WEP，但是能提供更加完善的安全保护。

WAPI 采用非对称（椭圆曲线密码）和对称密码体制（分组密码）相结合的方法实现安全保护，实现了设备的身份鉴别、链路验证、访问控制和用户信息在无线传输状态下的加密保护。

WAPI 除实现移动终端和 AP 之间的相互认证之外，还可以实现移动网络对移动终端及 AP 的认证。同时，AP 和移动终端证书的验证交给 AS（Authentication Server，认证服务器）完成，一方面减少了 MT（Mobile Terminal，移动终端）和 AP 的电量消耗，另一方面为 MT 和 AP 使用不同颁发者颁发的公钥证书提供了可能。

二、WLAN 结构

WLAN 不论采用哪一种传输技术，其拓扑结构有两种基本类型：有中心拓扑、无中心拓扑。最基本的就是 Ad-Hoc 结构（无中心拓扑结构）和 Infrastructure 结构（有中心拓扑结构）。

1. 点对点 Ad-Hoc 结构

点对点 Ad-Hoc 对等结构就相当于有线网络中的多机（一般最多为 3 台机）直接通过网卡互联，中间没有集中接入设备[没有无线接入点（AP）]，信号是直接在两个通信端点对点传输的。

在有线网络中，因为每个连接都需要专门的传输介质，所以在多机互联中，一台计算机中可能要安装多块网卡。而在 WLAN 中，没有物理传输介质，信号不是通过固定的传输线路作为信道传输的，而是以电磁波的形式发散传播的，所以在 WLAN 的对等连接模式中，各用户无须安装多块 WLAN 网卡，相比有线网络来说，组网方式要简单许多。

Ad-Hoc 对等结构网络通信中没有一个信号交换设备，网络通信效率较低，所以仅适用于较少数量的计算机无线互联（通常是在 5 台主机以内）。同时由于这一模式没有中心管理单元，所以这种网络在可管理性和扩展性方面受到一定的限制，连接性能也不是很好。而且，各无线节点之间只能单点通信，不能实现交换连接，就像有线网络中的对等网一样。这种无线网络模式通常只适用于临时的无线应用环境，如小型会议室、SOHO 家庭无线网络等。

由于这种网络模式的连接性能有限，所以此种方案的实际效果可能会差一些。况且现在的无线局域网设备价格已大幅下降，一般的 108 Mb/s 无线 AP 价格也可以在 500 元以内买到，54 Mb/s 的更是在 200 元左右，这样的价格根本没必要采用这种连接性能受到诸多限制的对等无线局域网模式。

为了达到无线连接的最佳性能，所有主机最好都适用同一品牌、同一型号的无线网卡；并且要详细了解相应型号的网卡是否支持 Ad-Hoc 网络连接模式，因为有些无线网卡只支持下面将要介绍的基础结构模式，当然绝大多数无线网卡是同时支持两种网络结构模式的。

2. Infrastructure 结构

Infrastructure 结构模式由 AP、无线工作站以及分布式系统（Distribution System Services，DSS）构成，覆盖的区域成为基本服务集（Basic Service Set，BSS）。无线工作站与 AP 关联采用 AP 的基本服务区标识符（Basic Service Set Identifier，BSSID）。在 802.11 中，BSSID 是 AP 的 MAC 地址。从应用角度出发，绝大多数无线局域网都属于有中心网络拓扑结构。基础结构网络也使用非集中式 MAC 协议。但有中心网络拓扑的抗摧毁性差，AP 的故障容

易导致整个网络瘫痪。

第三部分　技能训练

一、Ad-Hoc 对等无线网络组建

实验拓扑如图 1-3 所示，要求正确安装无线网卡后，分别设置两台计算机的 IP 属性。在任意一台 PC 机上创建无线局域网，设置其 SSID（Service Set Identity），即无线网络的名称，用来区分不同的无线网络，最多可以有 32 个字符。同时，SSID 通常由 AP 广播出来，通过无线客户端自带的扫描功能可以查看当前区域内的 SSID。另一台 PC 加入该网络。

图 1-3　Ad-Hoc 对等无线网络组建拓扑

配置过程中请完成表 1-3。

表 1-3　Ad-Hoc 对等无线网络组建配置记录

设备	IP 地址	子网掩码	SSID	认证方式	WEP 密码
PC1					
PC2					

同时用“ping”命令等方式测试两台 PC 的连通性，并记录分析。

二、Ad-Hoc 对等无线网络接入 Internet

Ad-Hoc 对等无线网络接入 Internet 实验拓扑如图 1-4 所示。

图 1-4　Ad-Hoc 对等无线网络接入 Internet 实验拓扑

按拓扑图连接网络设备后，设置 PC1 有线网卡的 IP 地址并设为共享，观察无线网卡地址的变化，再设置 PC2 的 IP 地址、子网掩码、默认网关、DNS 服务器。记录配置数据于表 1-4 中。

表 1-4　Ad-Hoc 对等无线网络接入 Internet 记录

设备	IP 地址	子网掩码	默认网关	DNS 服务器
PC1 有线网卡				
PC1 无线网卡				
PC2 无线网卡				

保障 PC1 有线网卡能上网,重点在于设置 PC1 的无线网卡和 PC2 无线网卡的相关参数，使得正确设置后 PC2 能上网，并测试分析结果。

三、Infrastructure 无线网络组建

Infrastructure（基础结构）模式属于集中式结构，其中无线 AP 相当于有线网络中的集线器，起着集中连接无线节点和数据交换的作用。通常无线 AP 都提供了一个有线以太网接口，用于与有线网络设备的连接，如以太网交换机。无线接入点 AP 就相当于有线网络的集线器，它能够把各个无线终端连接起来，无线终端所使用的网卡是无线网卡，传输介质是空气。

利用 AP 组建如图 1-5 所示的网络拓扑。

首先复位 TP-Link 无线 AP，重置为出厂设置，记录表 1-5 中所需内容。

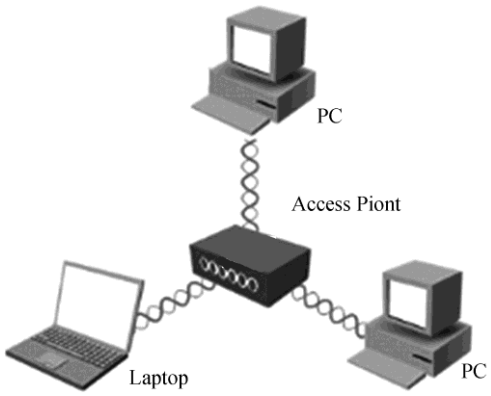

图 1-5　Infrastructure 无线网络组建拓扑

表 1-5　复位 TP-Link 无线 AP 后记录

参数	MAC 地址	管理 IP 地址	子网掩码	用户名	密码
AP					

无线 AP 加电放置后记录表 1-6 中所需内容。

表 1-6　复位后加电 TP-Link 无线 AP 后记录

参数	默认的 SSID	MAC 地址	IP 地址	子网掩码	用户名	密码
AP						

对 PC 机的无线网卡属性进行设置，PC 机通过无线网卡连接无线 AP，在 PC 机上登录无线 AP 管理界面，对无线 AP 的 IP 地址、子网掩码、用户名、密码进行设置，同时对无线参数进行设置，记录在表 1-7 中。

表 1-7　登录无线 AP 对参数的设置记录

参数	地址及用户名、密码参数					无线参数				
	MAC 地址	IP 地址	子网掩码	用户名	密码	工作模式	SSID	信道	模式	WPA-PSK
AP										

启用无线 AP 的 DHCP 服务器地址池，PC 机使用自动获取 IP 地址，接入无线网络，支持 WiFi 的智能手机也能接入该无线网络，记录其 IP 地址属性于表 1-8 中。

表 1-8　PC 机及其他支持 WiFi 的智能手机 IP 地址属性记录表

设备	IP 地址	子网掩码
PC1		
PC2		
PC3		
手机 1		
手机 2		

测试以上终端之间的连通性。

四、Infrastructure 无线网络接入 Internet

Infrastructure 无线网络接入 Internet 实验拓扑如图 1-6 所示。

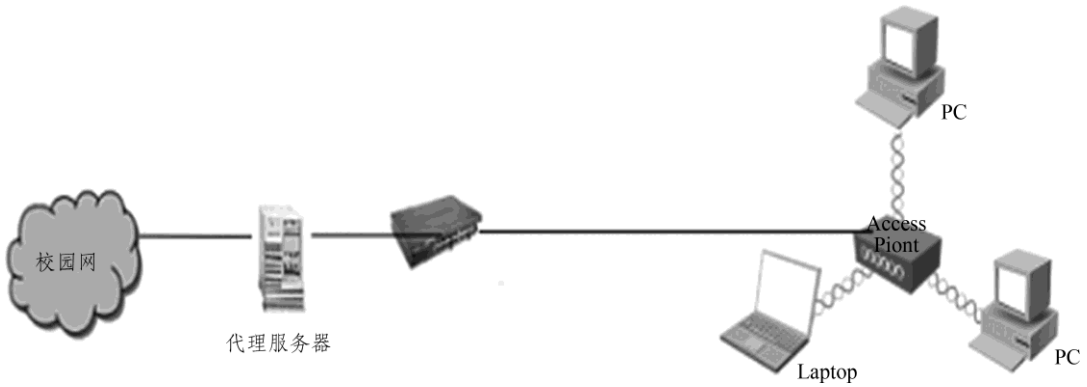

图 1-6　Infrastructure 无线网络接入 Internet 实验拓扑

按拓扑图来连接网络设备，在 PC 机上登录无线 AP 管理界面，对 IP 地址进行设置，使 AP 接入 Internet，启用无线 AP 的 DHCP 服务器，记录数据于表 1-9 中。

表 1-9　AP 的 IP 参数及 DHCP 参数

参数	IP 参数			DHCP 参数		
	IP 地址	子网掩码	网关	地址池	网关	DNS server
AP						

PC 机使用自动或手动获取 IP 地址，接入无线网络，支持 WiFi 的智能手机也接入无线网络，记录数据于表 1-10 中。

表 1-10　终端的 IP 参数

设备	IP 地址	子网掩码	默认网关	DNS 服务器
PC1				
PC1				
手机 1				
手机 2				

测试 PC 机、手机能否访问校园网。

五、知识点考核

1. 无线局域网 WLAN 的传输介质是（　　）。

A. 红外线　　B. 载波电流　　C. 无线电波　　D. 卫星通信

2. 以下可以工作在 2.4 GHz 频段的无线协议是（　　）。（多选）

A. 802.11　　B. 802.11a　　C. 802.11b　　D. 802.11g

3. 在中国，802.11b 2.4 GHz 的频段存在多少个非重叠信道（　　）。

A. 6　　B. 3　　C. 12　　D. 8

4. 根据欧洲标准，ISM 频段被分为（　　）个信道。

A. 11　　B. 13　　C. 14　　D. 3

5. ISM 中 802.11g 2.4 GHz 频段中每个信道所占用的频宽为（　　）。

A. 5.22 MHz　　B. 16.6 MHz　　C. 22 MHz　　D. 44 MHz

6. 如果第一个 AP 已经被设置为信道 6，那么需要在该区域中再增加一台 AP 时，该 AP 的信道应该设置为（　　）。

A. 4　　B. 1　　C. 9　　D. 10

7 IEEE 802.11 标准在 OSI 模型中的（　　）提供进程间的逻辑通信。

A. 数据链路层　　B. 网络层　　C. 传输层　　D. 应用层

8. IEEE 802.11 规定 MAC 层采用（　　）协议来实现网络系统的集中控制。

A. CSMA/CA　　B. CSMA/CD

9. 在下面信道组合中，三个非重叠信道的组合为（　　）。

A. 信道 1　信道 6　信道 10　　B. 信道 2　信道 7　信道 12

C. 信道 3　信道 4　信道 5　　D. 信道 4　信道 6　信道 8

10. 目前国际标准规定的无线产品最大发射功率为 100 mW，相当于（　　）。

A. 1 dBm　　B. 10 dBm　　C. 20 dBm　　D. 30 dBm

11. 1 mW=____dBm　　100 mW=____dBm　　____uW=−10dB m

12. 以下说法不正确的是（　　）。

A. 无线局域网（WLAN）协议用来定义无线网络通信的规则

B. 我们通常讲的无线局域网主要指的是采用 IEEE 定义的 802.11 协议

C. WiFi 是无线网络产品的一个兼容性认证，并不是强制的

D. 802.11ac 适用于 2.4 GHz 和 5 GHz