注：此页为封一。
阅后删除此文本框。

注：居中，宋体，小一号，加黑，统招、单考硕士、高校教师在职申请硕士学位、同等学历硕士填写内容为“硕士学位”；工程硕士、MBA、EMBA、MPA 填写内容为“专业学位硕士学位”。阅后删除此文本框。

小区无线监控解决方案









MOTOROLA

名目

一．工程概述 2

1.1

1.2

1.3

2.1

2.2

2.2.1

2.2.2

4.1

4.1.1

4.1.2

4.1.3

4.2

4.2.1

4.3

4.3.1

4.3.2

4.3.3

4.4

4.5

4.5.1

4.5.2

4.6

5.2 AP-5181 32

一．工程概述

1.1　用户介绍

南京玉兰山庄小区需要用无线来掩盖整个小区，监控和网络中心在第 6 栋别墅。打算实现整个小区的室外无线监控数据传输功能。

1.2　需求分析

- **机动性**

驱策无线通讯与行动运算最根本的创意原动力，可以说是机动性。过去几年来手机与家用手提式无绳　的普及，就是个最好的说明。轻薄短小而携带便利的笔记本电脑，也已经渐渐开头取代笨重的桌上型计算机。

然而，光是只有笔记本电脑、甚至个人数字助理PDA 是不够的，走到哪、用到哪，仅只为根本的需求，保持信息的传递与无时无刻的网络连结，让个人计算机不再只是个能够移动的孤儿，但是网络线所带来的不便与限制难以抑制，这就是非得靠无线通讯不行了。因此，无线局域网络 WLAN 为计算机带来了相当的机动性，已彻底颠覆传统的生活与工作状态。

- **安全性**

无线局域网 WLAN 的好处之一，还包括其弹性与便利性。由于不需要大量布线，架设上较传统网络便利，也极少需要管路来架设网络线缆，对网管人员而言，不仅可以大幅度缩减建构网络的时间，将来假设网络拓扑需要更动时，也不用太过大费周章的进展重拉线。譬如说传统的以太网络应用在办公室的环境下，或许遇到部门间间或人事上的调动、组织的重编，那么网络的架构很可能就得需要修改，即使只是增加一两个员工，都有可能让额外的网络线铺设大费周章。在这种状况下，WLAN 由于以无线电波连接取代铜线或光纤电缆，调整上就便利多了！就算办公桌挪来挪去，也不需要为了网络线插孔的移动而伤脑筋，信息就有如空气一般顺手可得，适合网管人员弹性规划运用，对商业上的应用极具吸引力。

- **扩大性**

无线局域网 WLAN 还有另一个优点，那就是良好的扩大性。传统有线网络的铺设下，一般网管往往为了预防以后额外的架设需要，造成初次架设时非必要的铺张。以一个 2.4GHZ 下的 WLAN 而言，假设当有更多使用者参加该网络时，可以在同个定点扩大至三个互不干扰的无线网络，显着扩大了其带宽负荷量。因此，WLAN 可大可小，扩大与升级都较传统有线网络来得便利。只要增加无线接入点AP 就可以拓展整个网络的涵盖范围与容量，也因此安装 WLAN 对网管人员而言，确定是项明智之举。

- **投资酬劳**

无线局域网 WLAN 广受重用的最大因素，莫过于其投资酬劳 ROI。或许一开头的网络设备较为昂贵，然而安装本钱低廉，加上无线网络的检修较为便利，不怕虫蛀鼠咬，牢靠度高，长期维护本钱亦相对下降。重点是 WLAN 提升了效率与机动性，甚至无形中助长了生产力，使得投资酬劳率上升，也让企业对 WLAN 的应用与进展寄予厚望。美国波音公司就是个很好的例子，他们善用 WLAN 于制造飞机的厂房，不仅网络铺设上更具弹性，更增加了工作生产力，可谓一举数得。而且随着网络语音VOIP 在商业上应用的进展，WLAN 可与之建构于办公室的信息语音网络，特别用在大区域、低密度的连网。WLAN 的用途 ，凭借着随之而来的高度投资酬劳率，前景一片光明。

1.3 摩托罗拉

Motorola 是全球移动计算技术的先驱，也是最早参与制定无线网络标准的厂商之一。在无线网络技术领域拥有格外高的权威和声誉。Motorola 公司是 IEEE802.11 组织的五大缔造者和核心成员之一；是 WiFi 组织的主要发起人和召集人； 2023 年度，IEEE802.11 组织的轮值主席为 Motorola 公司员工。

Motorola 的企业移动解决方案集成了先进的无线系统 Wi-NG、高度冗余的无线 Mesh 网络，结实强大的移动计算系统、移动软件和世界级的Motorola 企业移动效劳。Motorola 所供给的端到端、实时的企业移动解决方案可以提高员工生产力、降低运营本钱、改进运营效率并增加竞争优。Motorola 是全球领先的零售商、运输和物流公司、制造商、公共部门和政府、教育机构以及医疗保健、医院和安全机构供给商最可信任的参谋。

Motorola 公司是一家布满创的公司，拥有大量无线网络的专利。例如 Motorola的无线交换技术、无线网络的 VoIP 技术，无线网络的 MESH　POE 技术，智能漫游、抢先漫游、无线终端的节电技术、三层无缝漫游。另外还有像PoE 以太网供电技术大大简化了网络的实施和安装过程。

Motorola　依托于强大的企业移动解决方案，将无线网络成功地推入到各个行业。我们的大客户有：美国国防部DOD，沃尔玛集团，家乐福集团，UPS，FedEx，DHL，波音飞机制造公司，通用汽车公司，奔驰汽车公司，纽约华尔街证券交易所，纽约肯尼迪国际机场，英国伦敦希斯罗国际机场，法国巴黎戴高乐国际机场等等。Motorola 公司供给的先进的技术，品质优异的产品以及完善的售后效劳使之成为全球移动解决方案业界确实定领先者。

摩托罗拉公司力求将每一细节问题阐述清楚，供给完整的无线网络建议，期望通过我们专业的精神，领先的技术和完善的客户至上的效劳理念为客户供给一个牢靠、安全、稳定和高效的无线网络。

二． 无线网络设计方案

2.1 总体方案

整个工程承受全无线，分层次，分区域的设计理念，依据网络系统中不同网络设备的地位和作用，可以将无线网络系统分为以下几个层次：

骨干层

将整个小区分为 8 个区域，分别架设 8 个室外 AP 基站，其中 1 个室外 AP 基站在监控中心所在的 6 栋。其他 7 个室外 AP 基站和监控中心之间承受光纤来支撑基站的流量，如有特别室外 AP 基站没有光纤资源，可以使用 AP 的无线回传力量。

接入层

在室外 AP 基站承受 1 台 Motorola AP5181 产品作无线掩盖和无线回传。

应用层

主要承载在网络应用的无线网络终端。无线网路终端的种类很多，所承载的应用也丰富多样。例如：用于无线定位的 AeroScout 定位标签，用户语音通信的 WiFi 无线、TEAM 手机，带有 WiFi 功能的笔记本电脑、数字助理 PDA 和无线监控摄像机，以及其他无线设备均可通过 AP5181 进展接入。

2.2 设备配置

本次工程总计掩盖整个小区，实现无线监控数据传输功能。设备主要安装于几个根本位置：

2.2.1 监控中心

监控中心配置 RFS6000 设备用于 WLAN 的治理，治理全部在接入点安装的 AP5181。全部 AP5181 收集到的无线监控流量都通过光纤集合到核心无线交换机 RFS6000 进展统一的过滤和治理。

以上全部设备均通过网线连接到治理中心的有线网络中。共同组成整个网络的核心。

2.2.2 室外 AP 基站

配置 AP5181，用于无线掩盖和无线回传。

掩盖主要承受 Motorola AP 无线接入点设备，负责无线终端用户的接入和网络传输。方案中承受的主要无线接入点产品是 Motorola AP5181，承受专用的 2.4G 进展掩盖和 5.8G 进展回传。供给电源供电即可工作。

AP 点位图如下：红色圆点为 AP



三． Motorola WLAN 无线掩盖方案

4.1 设备选型

结合保护区 WLAN 网络的特点/要求以及 Motorola 设备的技术特点，我们建议在核心网中使用 Motorola 的 RFS6000 无线掌握交换机。

摩托罗拉 RFS6000 无线交换机具备实时的 RF 治理功能，可以利用动态算法，创立一个高带宽、高可用性的完全自行配置、优化、冗余、自愈和安全的网络环境。RFS6000 无线掌握交换机具有以下功能：

1) 动态信道安排
2) 自动放射功率调整
3) 网络负载均衡
4) 无线流量优先处理
5) 高安全性
6) 易治理性

4.1.1 网络动态信道安排

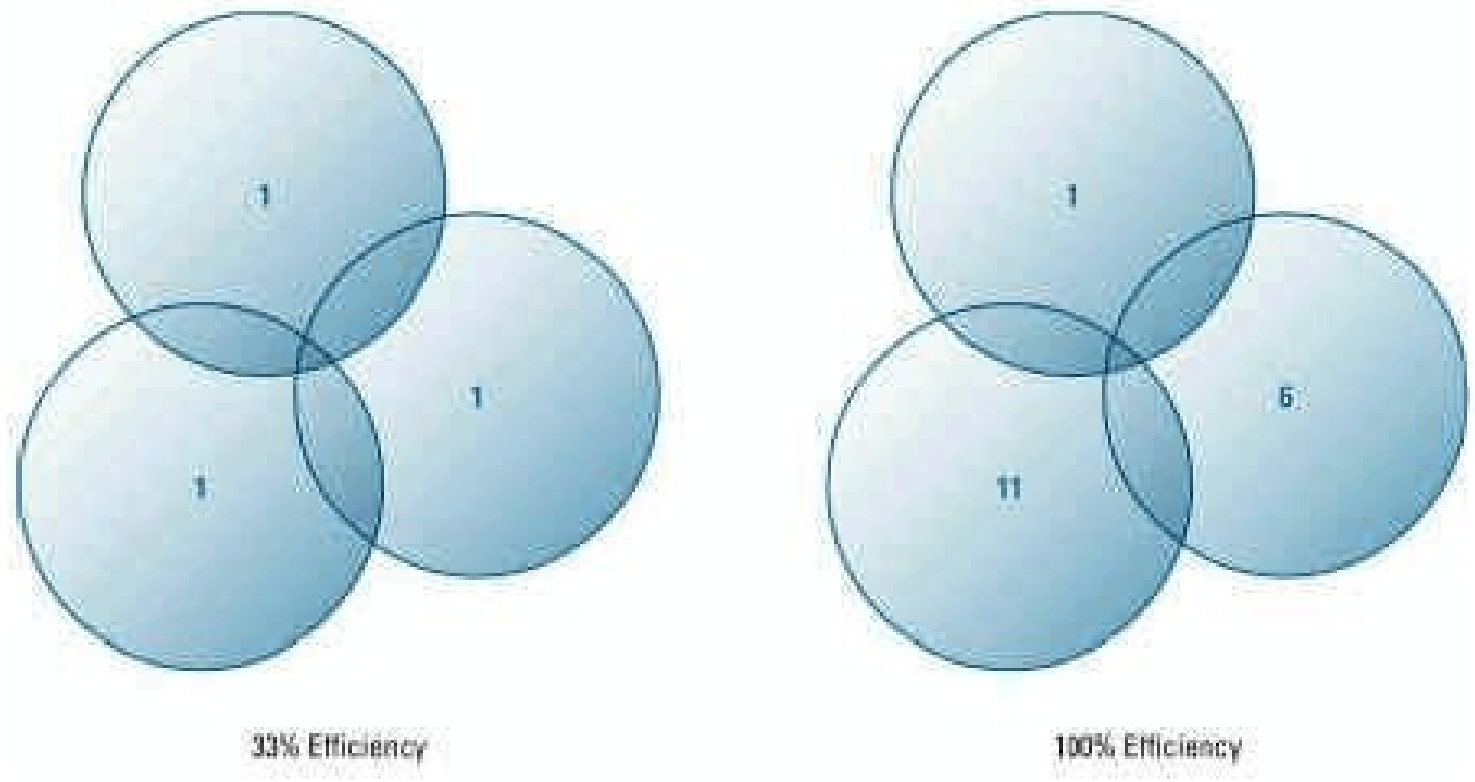
802.11 MAC 功能需要承受一种基于二进制指数退避的冲突避开机制，即带有冲突检测的载波侦听多路存取〔CSMA/CA〕。

当某个终端需要发送信息时，它会将其供给应介质。假设介质是闲置的，接入点将会允许该终端发送它的数据。否则，终端将被告知等到其他正在使用介质的基站完成任务之后再发送数据。这可以防止两个客户端同时在同一个信道上发送数据，导致数据帧受损。

在使用 CSMA/CA 时，同一个信道上的两个接入点〔位于同一个区域〕与两个不同信道上的两个接入点相比，将获得其一半的容量。这可能会导致问题。摩托罗拉的 AP 可以通过动态安排接入点信道，避开冲突，从而提高系统容量。

摩托罗拉 AP 的动态信道安排功能还有助于最大限度地削减 WLAN 解决方案中的

相邻接入点之间的同频干扰。通过安排信道，可以隔离一样信道，从而避开这个问题〔如以下图所示〕。



33%效率　　100%效率

摩托罗拉无线交换机可以通过分析 AP 供给的多种实时 RF 特性，有效地处理信道安排。这些特性包括：

无线信道中的 AP 数量。摩托罗拉无线交换机通过分析由 AP 收集的 beacon 信息，计算出不同信道中的 AP 数量，选择 AP 数量少的信道承受 AP。

信道的平均接收信号的强度。摩托罗拉无线交换机通过分析每个信道的平均信号接收强度，选择平均信号接收强度低的信道承受 AP。

噪声——这个因素会限制客户端和接入点的信号质量。噪声的增大会导致有效网格的减小。通过优化信道和避开噪声源，摩托罗拉无线交换机可以在优化网络掩盖范围的同时，保持系统容量不变。假设某个信道由于噪声过高而无法使用，该信道将会被避开。

802.11　干扰——假设存在其他无线网络，摩托罗拉无线交换机将会自动转变信道的使用方式，以避开与其他网络的干扰。例如，假设一个网络使用的是信道　6，另一个相邻 WLAN 将被安排信道 1 或者 11。这可以通过限制频率重叠，提高网络容量。假设

由于某个信道的使用量过高而导致没有可用容量，摩托罗拉无线交换机将会选择避开这个信道。

摩托罗拉无线交换机可以将 RF 特性信息与智能算法相结合，执行针对整个系统的决策。利用软决策机制，可以满足相互冲突的需求，为最大限度地削减网络干扰确保最正确的选择。

4.1.2 Smart RF:网络自愈/自动放射功率调整

正确的接入点放射功率设置对于保证 WLAN 的平稳运行具有重要的意义。这对于实现网络冗余也格外重要，有助于确保在接入点失去连接时进展实时的故障切换。

摩托罗拉无线交换机的SmartRF 功能可依据实时的WLAN 状况动态地掌握接入点的放射功率。在正常状况下，功率可以保持在较低的水平，以获得额外的容量和削减干扰。

假设检测到某个发生故障的接入点，四周接入点的功率将会自动提高，以填补掩盖范围受损所导致的漏洞。只允许对放射功率进展静态设置的 WLAN 解决方案在支持动态网络需求方面的力量极为有限。

4.1.3 网络负载均衡

只有在客户端能够通过负载均衡，有效地利用容量的状况下，WLAN 容量才具有实际意义。不幸的是，客户端并没有足够的智能来自行制定均衡决策，即使这可以带来更好的性能。例如，的全部用户可能都会与某个距离最近的接入点建立关联，而无视某个距离较远、但是利用率较低的接入点。

摩托罗拉无线交换机为全部接入点的客户端负载供给了一个集中视图。通过两种方式来确定在哪里将的客户端参加网络。分别为基于用户数量的负载分担和基于流量的负载分担。当启用上述负载分担方式时，摩托罗拉无线交换机可以主动地 "驱使 "现有客户端关联到的接入点，以提高 WLAN 的性能。这样，容量可以更加平均地安排到整个无线网络之中。

Motorola 的负载分担方式支持在 2.4G 和 5.8G 之间进展负载分担，为防止负载分担只对 AP 掩盖重叠区域启用。

4.2 无线网络高牢靠冗余方案

4.2.1 牢靠的室外型 AP 5181

AP-5181 是为室外应用环境而设计的，它不怕风吹、雨淋以及通常的室外气候。它具有天馈浪涌保护器，安全牢靠。该设备可分别供给 POE 或 220V AC 两种电源系统供用户选择。它包括多个室外双频天线以及精彩的技术特性支持。



AP-5181 室外型金属外壳和工业级组件结实耐用，工作温度范围大〔-30℃至 55℃〕，放水防尘等级为 IP56。因而能满足工厂、仓库、大型零售环境和类似设施的要求。该产品接收灵敏度高，而且延迟低，因而掩盖距离长、范围大，能够满足这些应用的需要。

4.3 无线网络安全方案

由于无线局域网承受公共的电磁波作为载体，因此与线缆网络不同，任何人都有条件窃听或干扰信息，因此在无线局域网中，网络安全很重要。常见的无线网络安全问题如下：

效劳区标示符(SSID)：

无线工作站必需出示正确的 SSID 才能访问 AP，因此可以认为 SSID 是一个简洁的口令，从而供给肯定的安全。假设配置AP 向外播送其 SSID，那末安全程度将下降；由于一般状况下，用户自己配置客户端系统，所以很多人都知道该 SSID，很简洁共享给非法用户。在消费类产品中，例如在机场，很多人通过使用一般的迅驰 PC 就能实现对区域内 AP 的扫描，从而非法使用该 AP 的网络资源。有的厂家支持“任何”SSID 方式， 只要无线工作站在任何 AP 范围内，客户端都会自动连接到 AP，这将跳过 SSID 安全功能。

在 SSID 安全的保证中，一项根本的设置要求就是必需关闭SSID 的播送，这样至少可以杜绝简洁的扫描攻击。

物理地址〔MAC〕过滤：

每个无线工作站网卡都由唯一的物理地址标示，因此可以在 AP 中手工维护一组允许访问的 MAC 地址列表，实现物理地址过滤。物理地址过滤属于硬件认证，而不是用户认证。这种方式要求 AP 中的 MAC 地址列表必需随时更，目前都是手工操作通常列表数目不超过 40 个；假设用户增加，则扩展力量很差，因此只适合于小型网络规模。对于二代无线架构，MAC 过滤是一种比较简洁使用的方式。

由于无线信号的空间泄漏特性，以及 802.11 技术的普及，随之而来的无线网络安全问题也被宽阔用户普遍关注。如何在保证 802.11WLAN 的高带宽，便利访问的同时， 增加强有力的安全特性？业界的厂商纷纷争论进展了 802.11 技术，增加了无线局域网安全的各个方面，并促成了诸如 802.1x/EAP，802.11i，WPA/WPA2 等标准的诞生，以及后续标准〔如 802.11w〕的制定。

摩托罗拉在无线局域网安全技术和标准制定方面，扮演了极为重要的角色，是 802.1x/EAP 无线环境应用的最早支持厂商，并在无线安全标准工作组中占据领导地位。

与其他网络一样， WLAN 的安全性主要集中于访问掌握和隐私保护。健全的 WLAN 访问掌握〔也被称为身份验证〕可以防止未经授权的用户通过接入点收发信息。

严格的 WLAN 访问掌握措施有助于确保合法的客户端基站只与牢靠的接入点〔而不是恶意的或者未经授权的接入点〕建立联系。

WLAN 隐私保护有助于确保只有预定的接收者才能了解所传输的数据。在数据通过一个只供数据的预定接收者使用的密钥进展加密时，所传输的 WLAN 数据的隐私才视为得到了妥当保护。数据加密有助于确保数据在收发传输过程中不会遭到破坏。

但是，无线局域网的安全并不仅仅局限于接入认证和数据加密。无线接入设备 AP 的物理安全性，AP 连接到有线网络交换机的安全认证，基于无线访问位置的物理防护手段，如何避开攻击，如何快速觉察非法/假冒 AP，对一个网络系统来讲也是格外重要的。

下面我们就结合保护区 WLAN 信息系统工程的无线网络构造，以及无线网络传输特点，进展具体说明。

4.3.1 无线通讯安全加密

在无线通讯传输过程中，全部数据包经过加密后在无线链路上进展传输。在现有的无线网络数据加密技术中，除了要考虑加密算法外，还应当考虑传输密钥的治理。摩托罗拉已经在产品方案上实施了 TKIP/AES 加密技术，可以有效改善无线链路的通讯安全。

TKIP〔动态密钥完整性协议〕加密机制

TKIP〔动态密钥完整性协议〕主要包括两个关键的对 WEP〔连线对等保护〕的增加局部：

1、在全部WEP〔连线对等保护〕加密的数据包上承受报文完整性检测 (MIC) 功能，以更有效的保证数据帧的完整性；

2、针对全部的 WEP〔连线对等保护〕加密的包实行 基于每个数据包密匙的方式。

MIC 主要是用来改善 802.11 低效率的 Integrity check function (ICV)，主要解决两个主要的缺乏：MIC 对每个无线数据帧增加序列号，而 AP 将丢弃挨次错误的帧；另外

在无线帧上增加 MIC 段，MIC 段则供给了更高量级的帧的完整性检查。

有很多报告显示 WEP〔连线对等保护〕密匙方式的弱点，报告了 WEP 在数据私密和加密上的很低成效性。在 802.1X 的重认证中承受 WEP〔连线对等保护〕密匙旋转的方法可以减轻可能经受的网络攻击，但没有根本解决这些问题。802.11i 的标准中 WEP〔连线对等保护〕增加机制已经承受了针对每个分组的 WEP 密匙。并且这些技术已经在摩托罗拉的 WLAN 设备中得以实施。

***AES(*高级加密标准*)*加密机制**

AES(高级加密标准)是一种旨在替代 TKIP〔动态密钥完整性协议〕和 WEP 中使用的 RC4 加密的加密机制。AES(高级加密标准)不存在任何攻击，而且加密强度远远高于 TKIP 和 WEP〔连线对等保护〕。AES(高级加密标准)是一种极为安全的密码算法， 目前的分析说明，需要 2 的 120 次方次计算才能破解一个 AES(高级加密标准)密钥－－ 还没有人真正做到这一点。

AES(高级加密标准)是一种区块加密法。这是一种对称性加密方法，加密和解密都使用同一个密钥，而且使用一组固定长度的比特－－即所谓的“区块”。与使用一个密钥流对一个文本数据输入流进展加密的 WEP〔连线对等保护〕不同，AES 会独立地加密文本数据中的各个区块。AES(高级加密标准)标准规定了三种可选的密码长度〔128、192 和 256 比特〕，每个 AES(高级加密标准)区块的大小为 128 比特。WPA2/802.11i 使用 128 比特密钥长度。一轮 WAP2/802.11i AES 加密包括四个阶段。对于 WPA2/802.11i，每轮会重复 10 次。

为了保护数据的保密性和真实性，AES 承受了一种名为 Counter-Mode/CBC-Mac (CCM)的型构造模式。CCM 会在 Counter 模式〔CTR〕下使用 AES，以保护数据保密性，而AES 承受 CBC-MAC 来供给数据完整性。这种对两种模式〔CTR 和 CBC-MAC〕使用同一个密钥的型构造模式已经被 NIST〔特别声明 800-38C〕和标准化组织〔IETF RFC-3610〕所承受。

CCM 承受了一种 48 比特的 IV。与 TKIP 一样，AES(高级加密标准)使用 IV 的方式与 WEP 加密模式有所不同。在 CCM 中，IV 被用作用于制止重复攻击的加密和解密流程的输入信息。而且，由于 IV 空间被扩展到 48 比特，发生一次 IV 冲突所需的时间会以指数形式增长。这可以供给进一步的数据保护。

建议承受基于硬件的 AES 加密〔和解密〕，由于 AES 需要进展大量的计算。摩托罗拉无线设备产品为 AES 供给了硬件支持。

4.3.2 防范潜在的无线网络攻击

WLAN 可能会患病多种类型的攻击。在使用 802.1X-EAP、TKIP 或 AES(高级加密标准)时，可以防止网络患病多种网络攻击的影响。如下表所示：

的安全技术有助于制止网络攻击

攻击类型	安全改进		
	身份验证： 开放 加密： 静态 WEP	身份验证： EAP-FAST，EAP-TLS 或者 PEAP 加密： 动态 WEP	身份验证： EAP-FAST， EAP-TLS 或者 PEAP 加密： TKIP MIC，AES
中间人	担忧全	担忧全	安全
身份伪装	担忧全	安全	安全
薄弱 IV 攻击〔AirSnort〕	担忧全	担忧全	安全
分组伪装〔重复攻击〕	担忧全	担忧全	安全
暴力攻击	担忧全	安全	安全
字典攻击	担忧全	安全	安全

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
https://d.book118.com/577055161146006130