服务器知识手册（二）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

企业 E 化方案.....1
社区网络技术选型方案分析 1
金融防火墙配置方案 11
小企业共享 ADSL 方案 18
如何设置一个企业级的 LinuxPOP3 服务器 25
中小企业 Reahat7.2+PoPtoP 实现 VPN 一例.....28
运行 HylaFAX 传真服务器 31
无线局域网络在公共场所覆盖解决方案 59
泛微销售自动化管理软件系统 65
管理会计在银行业的深入应用 78
面向金融行业电子商务软件的未来 84
高密度机架优化式服务器技术剖析 88
苹果电脑的电子化人力资源系统 93
Sun 公司金融行业解决方案 101
村务公开解决方案 107
惠普金手指制造企业 ERP 解决方案 114
路由器的应用 117
Linux 下路由器的配置 117

企业 E 化方案

社区网络技术选型方案分析

由于信息技术的发展和人们生活水平的提高，房地产开发商提供具有宽带信息化能力的智能小区已经成为必然。本文通过对智能化社区网络建设过程中所涉及到的关键技术以及典型案例的介绍，为智能化社区的建设者提供一个有力参考。

一、社区网络建设的主要技术

智能化社区的核心是智能化社区网络的建设，通过社区网络，社区管理员不但可以对社区进行现代化的物业管理，还可以为社区用户提供一些增值服务，比如高速 Internet 访问、网上社区、网上超市、网络图书馆、远程医疗、网上学校、股票网上实时交易和视频点播等社区服务。

智能化社区网络属于园区网络，与传统园区网络相比最大不同点是，智能化社区网络是一个公用的运营网络，其设计应包括以下 5 个方面:

1.社区网络控制中心的设计，包括宽带 Internet 接入方式、网管技术选择和核心交换路由设备的选择等；

2.基础物理传输网络设计，包括物理线路和传输协议等；

3.网络逻辑设计，包括路由服务和网络流量控制等；

4.网络运营管理平台设计，包括基于用户的认证、

计费、网络安全和服务质量等；

5.Internet 服务网络平台设计，包括防火墙、WebCache 和服务器负载均衡等。

除了社区网络控制中心的建立之外，智能化社区网络的建设重点就是物理网络传输技术即社区用户接入技术的选择，目前主要有 4 种接入技术：以太网技术、无线局域网技术、有线电视网数据传输技术和数字电话线路传输技术。由于智能化社区网络的建设是围绕着社区用户接入方式这一核心开展的，下面我们就这 4 种方式衍生的智能化社区网络建设方案进行分析与比较。

（一）以太网技术

采用以太网技术建设的智能化社区网络，实际上就是建设智能化社区以太园区网。具体方法是，在社区用户的家中添加 RJ45 接口信息插座作为接入社区网络的接口，可提供 10/100Mbps 自适应的网络连接速率。

由于采用的以太网技术较为成熟，因此基础网络设计方案和技术实现比较简单，主要包括 2 方面：即园区内网络结构化布线和以太网设计与实现。园区内网络结构化布线通常采用光纤到楼、双绞线到户的方案，即楼宇之间采用光纤形成网络骨干线路，在单栋建筑物内采用五类双绞线到每户。以太网设计与实现包括网络管理控制中心和社区楼内子网的设计与实现。网络管理控制中心一般采用核心级骨干交换机，社区子网一般采用工作组级交换机。设计者可以根据每栋楼内住户数量确定交换机端口数量，从而决定采用交换机的数量。

虽然采用以太网技术建设智能化社区网络技术成熟、方法简单，但设计者还是应当注意以下几个问题。

1．适用对象此方案最适用于新开发的小区，通常布

线工作是与房屋的建设施工一同进行，以降低建设成本。

2. 注意规范由于此方案采用以太网技术，所以网络布线结构和线缆的选择设计应参照以太网设计要求而制定。比如，不同的以太网技术对线缆的类型及传输距离的要求是不同的。

3. 以太网技术的选择目前可采用的以太网技术主要有千兆以太网、快速以太网和普通以太网技术。根据目前的技术现状，采用千兆交换到楼、百兆到户的以太网技术较为普遍。

4. 网络设备的选择核心网络骨干交换机作为网络的核心，应具备高性能、可扩展性、高可靠性，并具备丰富和强有力的网络控制能力和良好的可管理特性。网络边缘交换机是建筑物内用户直接接入网络的连接设备，应具备灵活性、使用方便和一定的网络服务质量和控制能力，并且要求价格便宜。

5. 网络服务运营管理平台实现社区网络作为一个公用的提供接入服务的运营网络，其运营服务管理应特别考虑用户认证、计费和网络安全，其中网络安全更是重中之重。网络安全包括 2 方面问题:一方面，由于以太网技术本身的一些弱点，如广播风暴等，对整网的服务可靠性造成威胁；另一方面，如果不采取措施，以太网内的用户，将面临本地黑客从网络第二层（即数据链路层）的直接窃听甚至攻击。对于以上问题，一般采用虚拟局域网技术（VLAN），即从用户端口到网络出口建立专用逻辑通路。但由于社区网络一般将承载数以百计的用户，网络管理员通过静态设置，管理同样数量的虚拟网和路由，其繁杂度和不灵活性可想而知。与此同时还要考虑此种设置方案下，网络设备的承载能力。由此可见，社

需要全本请访问 www.ertongbook.com

区网络设计中网络运营管理平台的设计与接入网相配套是非常关键的。

6．Internet 多功能服务平台设计实现除了基础物理网络和网络运营管理平台的设计，围绕 Internet 的应用服务实现，也应该是网络设计者需要考虑的重点，如 DHCP 服务器、DNS 服务器、防火墙系统、Web 服务器、电子邮件系统和文件访问服务器等。面对以上诸多的 Internet 服务，对于不同应用、不同规模的网络环境将有不同的解决方案。

7．其他设计实现包括网络骨干线路的冗余设计、网络地址的分配与管理以及服务质量的实现等。

（二）无线局域网技术

采用无线局域网技术建设社区网络，是采用以太网技术建设社区网络的有益补充，实际上也是建设社区以太网。无线局域网设备由无线客户端和访问单元（AccessPoint 简称 AP）组成，有时为了增加无线网络的传输（连接）距离，还包括高增益定向天线，现有的无线局域网设备可以提供 2Mbps～10Mbps 的传输速率。AP 通常还提供以太网接口，以方便超出传统传输介质连接范围的多个局域网互联，因此 AP 也被称为无线网桥，并且一些厂商生产的 AP 还可以互联，以增加无线局域网的覆盖范围。

采用无线局域网技术建设社区网络与前面所介绍的以太网技术基本相同，都是先在社区网络中心及单栋建筑物中建设以太网，然后在各楼交换机与网络管理中心骨干交换机之间，利用无线 AP 及高增益天线配合使用充当网桥互联，解决了传统以太网建设过程中，社区楼外布线成本高及利用率低等弊端，特别适合楼栋分布范

围广和用户群分散的社区采用。同时社区用户，只要拥有无线网卡及可移动计算机，可以在社区随时随地上网，实现住户与社区网络的无缝链接。

（三）有线电视网络数据传输技术

此技术类似于广电的宽带接入技术，比较适用于已经建成并使用的社区。为了不破坏建筑物室内外的装修，利用已有的有线电视线路，在用户端增加线缆调制解调器，就可以实现不重新布线接入社区网络管理控制中心。利用有线电视数据网络建设智能化社区网络主要注意以下问题。

1．有线电视网的传统业务是传输电视模拟信号，要在它的网络上开展数据传输业务，需要增加相应的设备，以便将数字信号调制到电视电缆相应的频带上。其中，在用户端需要安装线缆调制解调器（CableModem），在社区的有线电视网络中心需要添置线缆调制解调头端设备（CMTS）。

2．传统的有线电视网是广播式的单向传输网络，而为了传输双向的数据业务，需要有线电视传输网络支持双向传输。如果原有有线电视网络是单向的，则可采取2 种解决方式，其一是进行双向网改造，其二是利用现有的电话网作为数据上行通道。从服务于用户的角度来说（如带宽和使用方便等），以采用第一种方式为好。

3．此外，在选择头端设备和用户端的线缆调制解调器时，应注意设备要符合工业标准，这样才能保证不同厂家设备的互操作性、可升级能力和对用户设备投资的保护。目前，业界主流的工业标准为MCNS 的DOCSIS1.0 和 DOCSIS1.1。

（四）数字电话线路传输技术

对于已经建成的社区，为了避免重新布线破坏室内外装修，除了可以采用上述有线电视网络数据传输技术外，还可以利用数字电话线路传输技术来解决。

采用数字电话线路传输技术建设智能化社区就是用户利用电话线和调制解调器接入社区网络管理控制中心，为了实现数据传输的高速性，通常利用比较成熟的xDSL（如 ADSL）技术。

该方式利用现有的电话线路，为社区住户同时提供语音和高速数据传输服务，因此，它的适用范围很广泛，特别是适合于不便于进行结构布线的社区。系统的组成很简单，主要包括用户端的网络存取单元（NAU）、中心的网络集中单元（NCU）、网络交换机和电话布线系统。

这种组网方式不需要重新布线，在传输网络数据的同时，仍可提供电话业务服务。例如利用 3Com 公司的 EthernetOverVDSL 技术，可以在 1 类到 5 类双绞线上同时传输传统的语音业务和标准的以太网数据，即全双工 10Mbps 的数据业务。

二、社区网络建设技术的选择

以上介绍了 4 种智能化社区网络设计技术。那么，针对不同的社区，设计者采用何种接入技术建设社区网络呢？应该主要从以下几个方面考虑。

1．从布线的角度考虑:如果是新建社区或老区改造用户接受重新布线，则可以采用以太网技术或无线局域网技术。否则，就选择有线电视数据传输技术或数字电话线路传输技术。同时如果小区范围广，光纤铺设相对较为昂贵，同时需要住户计算机能无缝接入社区网络，则可以优先考虑无线局域网技术。

2．从社区用户接入的带宽需求角度考虑:以太网技术、无线局域网技术和数字电话线路传输技术都可以向用户提供 10Mbps 的网络接入速率，对于高带宽的网络应用（如视频点播等）支持较好，而有线电视数据传输则相对带宽较小。

3．从网络安全的角度考虑:由于以太网技术原本是为局域网而开发的技术，将它用于公共接入运营网络，将存在相对较为严重的安全问题。无线局域网和数字电话线路传输技术由于也采用了以太网技术，所以也有相同的问题。而有线电视数据传输技术本身就是为宽带接入运营网络而设计，比如 DOCSIS 标准中就定义了基于网络链路层的安全措施，所以安全性较好。

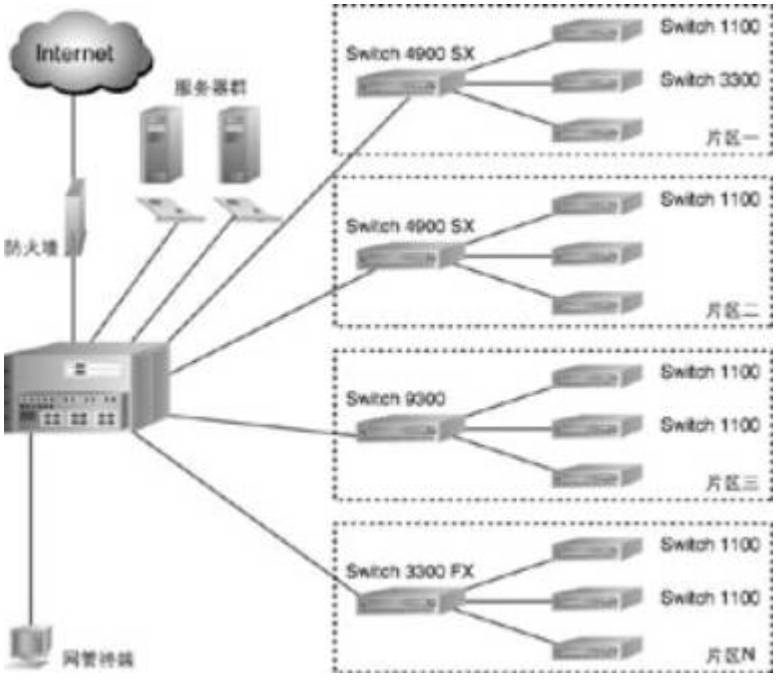
4．从网络设备管理的角度考虑:采用以太网技术和无线局域网技术的网络设备可能分别放置在各个建筑物内，网络设备需要分布管理，并且需要考虑网络设备运行环境。而采用有线电视数据传输技术和采用数字电话线路传输技术则不存在这类问题，其所有网络设备均集中放置在网络中心室内，管理和维护方便。

三、社区网络建设实例分析

广州某花园小区自 1991 年开始开发，在 1996 年就开始进行智能住宅建设的尝试，在一些新建楼宇进行了智能住宅的基础设计及施工（规划为综合布线系统），建立了小区光纤宽带网信息平台，构筑了周边防卫系统、楼宇指模门禁系统、每户的三表远传系统、可视门铃系统和消防自动报警系统，基本实现了小区的社会信息化沟通和起居安全化。现在，该小区已铺设光纤 25km，覆盖 231 栋住宅楼，购置安装了 1030 台交换路由网络设备。小区已完成了安全防范、信息管理和信息传输网络

3 个系统的建设，达到了家居安全化阶段。该小区是国内第 1 批开始住宅智能化建设的小区，于 2000 年 12 月 25 日正式通过了国家建设部智能化示范小区的验收。

该智能化小区网络采用以太网技术建设，实现千兆交换到楼，百兆交换到用户。全面采用了 3Com 公司的网络产品，其拓扑结构如附图所示。



（一）网络连接设备的选择

社区网络管理中心核心交换机 3ComSwitch4007 骨干交换机，支持多达 54 个 1000Mbps（千兆以太网）端口。Switch4007 的二层转发率超过 100Mpps，第三层的交换率高达 48Mpps。

楼栋汇聚交换机采用 3ComSS34900SX、SS•9300、SS•3900 和 SS•3300FX。其中 SS34900SX 是第三层交

换机，其前面板有 12 个 1000MbpsBase-Sx 端口，后面板的扩展槽能扩展 4 端口的各种千兆模块；SS·9300 是二层交换机，其前面板有 12 个 1000MbpsBase-Sx 端口;SS·3900 是 3Com 公司的线速二层交换机，支持 10/100/1000Mbps 技术;SS·3300FX 是二层交换机，其前面板有 8 个 100MbpsBase-Fx 端口，2 个 10/100MbpsRJ45 端口，后面板的扩展槽能扩展各种千兆模块。

楼层交换机采用 3ComSwitch3300 系列及 Switch1100 系列交换机。Switch3300 和 Switch1100 系列交换机都支持 10/100/1000Mbps 技术，采用 3Com 公司第 2 代 ASIC 集成电路技术，提供线速交换能力。

（二）网络服务运营管理平台实现方案

利用 3ComVBNServer 服务运营管理服务器实现网络服务运营管理，实现了以下服务及功能。

1．基于 PCMAC 地址和交换机端口的用户管理。

2．提供 IP 地址管理，DHCP 用户动态地址分配和 NAT 地址转换功能。用户 PC 无论其原有 IP 地址设置如何(动态/静态地址)，均能即插即用，无需任何设置改变。方便用户上网、简化网络维护。

3.提供强制性用户认证功能和社区门户网址自动转接功能。用户接入网络，可立即被要求进行注册认证，并自动连接社区门户网址。用户可以方便地浏览社区管理信息发布和其他社区服务。

4.提供用户计费功能。可提供详细的用户计费信息，运营商可自由定制计费管理界面。

（三）Internet 服务网络系统设计

提供 Internet 访问和内容服务是智能化社区网络的重要功能之一。如何保证社区网络服务的安全性和提高

需要全本请访问 www.ertongbook.com

网络响应速度是网络运营商要考虑的重要问题，因此选用了以下产品，以实现各种环境的网络需求。

1．采用 3Com 公司的 OfficeConnectFirewall 和 SuperStack•Firewall 防火墙产品，提供数据流状态跟踪和监控级别的防火墙功能，以实现社区网络的安全。

2．用 3ComSuperStack•WebCache 产品，以缓存经常被本地用户访问的网络信息，提高响应速度，降低运营商的 Internet 接入成本。

3．采用了 3ComSuperStack•loadBalanceServer 产品，实现服务器负载均衡。

（四）网络应用

经过上述建设，该社区网络主要实现了以下应用。

1．通过小区内部的多功能智能化网站及与 Internet 的高速连接，网上影院、网上图书馆、网上炒股、网上购物、在线游戏、网上直播、网上订餐、自动抄表、网上医疗和网上可视语音聊天等应用已全面开展。

2．通过 Internet，社区向住户提供国内外新闻、社区内新闻以及住户自己感兴趣的新闻，另外还有交通信息、天气信息、地区性活动和商业区地图等。

3．小区住户还可以利用网络实现防火防盗、煤气泄漏、自动报警、小区监控、可视门铃门禁、紧急呼叫、信息查询、视频点播和多媒体通信等，满足了住户在小区生活中的多种需求。

四、点燃未来生活的动力

在智能化社区内，房地产开发商通过计算机及网络设备为用户提供社区内的信息和服务，不仅缩短了人们物理上的距离，而且给用户带来了许多方便，因此，智能化的生活成为点燃未来生活的新动力。可以说，智能

化社区的建设代表了未来几年内建筑业的发展方向，必将成为开发商吸引住户的一大卖点。智能化社区建设的核心是智能化社区网络的建设，对于该网络接入技术的选择又成为其中的关键，并且，接入技术一旦选择就不易更改，故此需要慎重考虑。

金融防火墙配置方案

依据金融机构的职能在防火墙中正确定义符合安全策略和规则的组合，控制进出金融网的双向数据流，可达到金融网安全的目的。但如果防火墙规则配置错误，甚至可能使内网暴露在公众下！因此，正确设立防火墙安全策略、有效进行规则组合并实施方案比防火墙本身更重要。

一、制定防火墙策略

1、基本安全策略

金融网的两条基本安全策略：一是没有允许的服务都是禁止的，二是没有禁止的服务都是允许的。即对一切没有被禁止的服务，防火墙可转发其信息；对一切被禁止的服务，防火墙要逐项删除。人民银行防火墙的设置按安全级别由高到低排序为:内部局域网、人行系统内联网、金融区域网（城市网）；各商业银行防火墙的设置按安全级别由高到低排序为:内部局域网、工行、农行、中行、建行系统内联网、金融区域网（城市网）以及Internet。

2、内容安全检查

金融机构提供的服务内容有以下几点。

一是金融信息类（www 服务、电子邮件的支持、FTP

等）。允许存取 Internet 特定网页，确保员工能下传和存取某些网页，保护网络带宽，控制流量；通过 SMTP 的连接提供高度控制。可在一个标准应用程序地址之后，隐藏外出的邮件地址，或可隐藏内部的网络结构与真正的内部使用者。

二是电子银行类（结算、承兑、信用卡、借贷、储蓄、同城清算、电子联行、清算服务等）。其主要策略是网络地址转译，可隐藏内部网络地址，并克服 IP 地址数量的限制，维护内部地址的完整性。按照人行总行审定的地址规范，设置内部的网络地址，将内部注册 IP 地址以一个合法有效的 IP 地址对外。金融机构防火墙常用的两种操作模式有：动态模式，将内部所有 IP 地址经过防火墙用单一合法的 IP 地址对外；静态模式，提供一个对外公开的 IP 地址和内部真正的 IP 地址之间的映射。

3、冗余设计

金融机构的防火墙必须考虑冗余设计，当主防火墙发生故障时，备用防火墙可及时被激活工作。银行业务的时间性极强，通常是 24 小时营业，所以要求网络必须保障 24 小时安全，冗余设计的目的是在尽可能短的时间内，用较小的代价将突发事件对业务的影响降到最低。

4、安全认证

因为大多数金融业务采用的是通用的、流行的 TCP/IP 协议，由于该协议的开放性，使一些重要的信息（如客户资料等）在 Internet 传输过程中，容易被截取、破译，因此，任何进入内部网络的通话必须经过安全认证。防火墙认证的应用是当使用者与目的主机联机时，在通信被允许之前，安全地确认他们的身份，所有的认证过程都能经由防火墙日志浏览器来监视和追踪。认证

机制分使用者认证、端口认证、特定 IP 地址的存取认证；认证的机制包括固定密码和随机产生的动态密码。

网络防病毒系统是防火墙的捆绑产品，由于较显著地影响网络速度，目前，视各金融机构的具体情况，防病毒系统已经作为一个独立的子系统依附于安全系统中。

5、人员策略

无论金融机构防火墙系统提供了如何完善的安全保障，安全系统最终需要人来执行。这部分的安全检测属于人员的管理，主要目的在于降低人员使用信息或操作信息设备时可能发生的错误，如滥用、窃取、过失等。

二、规则设计原则

防火墙规则集是安全策略的技术实现，规则设计应遵循以下思路和原则。

1、建立规则文件。防火墙的配置文件可对允许进出的流量作出规定。它非常重要，因为网络的重大错误往往是防火墙配置的错误。

2、策略核心很微妙。金融机构一般具有 Web 和 E-mail 服务，由于任何人都能访问 Web 和 E-mail 服务器，所以不能信任它们。可把它们放入 DMZ（中立区），DMZ 是一个孤立的不信任网络，DMZ 中的系统不能连接内部网。

3、网络地址转换要谨慎。地址转换配置（NAT）分为源地址转换和目的地址转换。在源地址转换的配置中，需要配置源地址到伪装源地址（转换后的源地址）的转换规则，要为源地址设置一个伪装的合法地址，在源地址转换时，使内部子网的地址能够通过网络地址转换后利用一个伪装的合法地址达到访问外部网的目的。这样

就省去了占用多个合法 IP 的资源浪费。在目的地址转换的配置中，需要配置目标地址到真实目标地址之间的转换规则。在目的地址转换时，系统必须把目标地址和端口转换成真实的内部子网或 DMZ 区的地址，端口才能进行数据传送。这样系统可以指定某一子网或 DMZ 区的 IP 地址和相关端口接收外部网的数据。

4、路由设置必须合理。防火墙一般提供静态路由，静态路由是由网络管理员在启动网络路由功能之前预先建立起一个路由映射表。要访问某一子网的用户必须经过路由表中配置的网关地址，才能到达该子网。有时，不但要防止来自外部的黑客攻击，还要防止来自银行内部人员盗用别人的主机 IP 进行非法活动。采用内部网段的 IP 地址与网卡 MAC 地址绑定的方式，可防止内部主机盗用其他主机的 IP 进行未授权的活动。

5、规则力求简单。一个简单的规则集是建立一个安全的防火墙的关键所在。尽量保持规则集简洁和简短，因为规则越多，就越可能犯错误。一个好的规则最好不超过 30 条。规则少还意味着只分析少数的规则，这样，防火墙的 CPU 周期就短，效率可大大提高。当要从很多规则入手时，就要认真检查一下整个安全体系结构，而不仅是防火墙的。

6、规则次序很关键。同样的规则，以不同的次序放置，可能会完全改变防火墙的运转情况。一些防火墙具有自动给规则排序的特性，很多防火墙以顺序方式检查信息包。一般来说，应该将较特殊的规则放在前，较普通的规则在后，这可防止防火墙配置错误。

7、注意更改控制。恰当地组织好规则之后，写上注释并经常更新它们。注释可以帮助管理员明白哪条规则

做什么，对规则理解得越好，错误配置的可能性就越小。对那些有多个管理员的大型金融机构，建议当规则被修改时，把规则更改者的名字、变更的日期和时间、变更的原因加入注释中，这可以帮助管理员跟踪谁修改了哪条规则以及修改的原因。

8、做好审计工作。在安全审计中，经常能看到某个防火墙由于某个规则配置的错误而将机构暴露于巨大的危险之中。因此，不仅要对防火墙的操作进行审计，还要对审计内容本身进行审计，同时审计中要有明确的权限，充分保证审计内容的完全性。

综上，只有对所需保护的金融网的安全级别作出定性、定量评估，从整个系统的安全策略、安全规则实现等方面进行考虑，才能创建一个由防火墙隔离出的安全网络环境。

三、应用实例

图 1 是典型地市级金融机构防火墙的配置。在城市中心支行金融网络防火墙的应用中，人民银行防火墙的设置应将人民银行内部的局域网联接在防火墙一的内口（Insider 接口）上，安全级别最高，为 100；而将安全级别最低的防火墙一的外口（Outsider 接口）接入金融区域网（商业银行网）中；人行系统内联网的安全级别介于两者的中间，可定义为 80。商业银行防火墙的设置应将商业银行内部的局域网联接在防火墙二的内口（Insider 接口）上，安全级别最高，为 100；而将安全级别最低的防火墙二的外口（Outsider 接口）接入 Internet，金融机构（工、农、中、建行）内联网、金融区域网（城市网）的安全级别介于两者中间，可分别定义为 80 和 60。

需要全本请访问 www.ertongbook.com