计算机网络管理与安全技术研究

◎ 赵 睿 康 哲 张伟龙 著

吉林大学出版社

计算机网络管理与安全技术研究

◎ 赵 睿 康 哲 张伟龙 著

吉林大学出版社

图书在版编目（CIP）数据

计算机网络管理与安全技术研究 / 赵睿，康哲，张伟龙著. -- 长春：吉林大学出版社，2018.10

ISBN 978-7-5692-3608-8

Ⅰ. ①计… Ⅱ. ①赵… ②康… ③张… Ⅲ. ①计算机网络管理－研究②计算机网络－安全技术－研究 Ⅳ. ①TP393

中国版本图书馆CIP数据核字（2018）第243193号

书　　名　计算机网络管理与安全技术研究

作　　者　赵睿 康哲 张伟龙 著
策划编辑　魏丹丹
责任编辑　徐佳
责任校对　王婷
装帧设计　凯祥文化
出版发行　吉林大学出版社
社　　址　长春市人民大街4059号
邮政编码　130021
发行电话　0431-89580028/29/21
网　　址　http://www.jlup.com.cn
电子邮箱　jdcbs@jlu.edu.cn
印　　刷　河北纪元数字印刷有限公司
开　　本　787mm×1092mm　1/16
印　　张　19.5
字　　数　364千字
版　　次　2018年10月　第1版
印　　次　2018年10月　第1次
书　　号　ISBN 978-7-5692-3608-8
定　　价　78.00元

前　言

信息、物资、能源已经成为人类社会赖以生存与发展的三大支柱和重要保障，信息技术的快速发展为人类社会带来了深刻的变革。随着计算机网络技术的快速发展，我国在网络化建设方面取得了令人瞩目的成就。电子银行、电子商务和电子政务的广泛应用，使计算机网络已经深入国家政治、经济、文化和国防建设的各个领域，遍布现代信息化社会工作和生活的每个层面，“数字化经济”和全球电子交易一体化正在形成。计算机网络安全不仅关系到国计民生，还与国家安全密切相关，不仅涉及国家政治、军事和经济各个方面，而且影响国家的安全和主权。随着计算机网络的广泛应用，网络技术中最关键也最容易被忽视的安全问题，正在危及网络系统的健康发展和应用，网络安全技术及应用越来越受到世界的关注。

在日常活动与商业活动日益依赖互联网的情况下，人们对网络工作的安全性有了更高的要求，要求严格控制网络资源的访问，防止计算机病毒和非法入侵者的破坏。本书旨在通过对计算机网络管理控制和技术措施的研究，提高网络系统数据的保密性、完整性以及网络服务的可用性和可审查性保护，保证网络系统的硬件、软件及系统中的数据资源能够完整、准确、连续运行且服务不受干扰破坏和非授权使用。同时为及时修改和优化网络配置、提高运行效率、消灭网络通信瓶颈提供相关技术和方法。

本书内容共分为八章，第一章和第二章系统论述了计算机网络和互联网的相关概念、体系结构、类别、性能以及系统划分，为计算机网络管理与技术的

研究奠定了理论基础；第三章论述了计算机网络存在的安全问题并进行了具体研究，提出了解决网络安全问题的技术方法，对其概念进行了详细的阐述；第四章在论述计算机病毒概念、产生、发展历程、特征以及类别的基础上，深入研究了计算机病毒的防治方法与技术原理、杀毒软件的配置与应用；第五章、第六章以及第七章针对计算机网络运行的安全性论述了保障网络安全的重要技术，重点研究了防火墙技术、数据加密技术以及身份认证与访问控制的原理和运用；第八章将计算机网络的管理与技术相结合，针对网络系统的安全运行，提出了一系列有效的网络安全防范策略。

本书由赵睿、康哲和张伟龙共同编写完成，具体分工如下：赵睿负责编写第一章至第三章的内容和全书的统稿工作，康哲负责编写第四章至第六章的内容，张伟龙负责编写第七章、第八章的内容。

本书结合了最新的网络安全技术成果、方法和实际应用，具有以下两个特点。

（1）内容先进，结构新颖。本书吸收了国内外大量的新知识、新技术、新方法和国际通用准则，注重科学性、先进性、操作性，图文并茂，便于读者理解。

（2）注重实用性。在本书的写作过程中，笔者坚持“实用、特色、规范”原则，突出实用性，在内容安排上将理论知识与实际应用有机结合。

最后，感谢在本书撰写过程中给予大力支持和帮助的各界同仁，对撰写过程中参阅的大量重要文献资料难以完全准确注明，在此深表诚挚歉意。

赵　睿

2018 年 7 月

目　录

第一章

计算机网络概述

在本章的开始，首先阐述了计算机网络在信息时代的作用，接着对互联网进行了概述，包括互联网基础结构发展的三个阶段，以及今后的发展趋势。然后，讨论了互联网组成的边缘部分和核心部分。在简单概述了计算机网络在我国的发展以及计算机网络的类别后，讨论了计算机网络的性能指标。最后，论述了整本书都要用到的重要概念——计算机网络的体系结构。

第一节　计算机网络在信息时代中的作用

我们知道，21 世纪的重要特征就是数字化、网络化和信息化，它是一个以网络为核心的信息时代。要实现信息化就必须依靠完善的网络，因为网络可以非常迅速地传递信息。因此，网络现在已经成为信息社会的命脉和发展知识经济的重要基础。网络对社会生活的很多方面以及社会经济的发展已经产生了不可估量的影响。

生活中有三大类网络大家都很熟悉，即电信网络、有线电视网络和计算机网络。按照最初的服务分工，电信网络向用户提供电话、电报及传真等服务；有线电视网络向用户传送各种电视节目；计算机网络则使用户能够在计算机之间传送数据文件。这三种网络在信息化过程中都起到了十分重要的作用，其中

发展最快并起到核心作用的则是计算机网络，这正是本书所要讨论的中心内容。

随着信息技术的发展，电信网络和有线电视网络都逐渐融入了现代计算机网络技术，扩大了原有的服务范围，而计算机网络也能够向用户提供电话通信、视频通信以及传送视频节目等服务。从理论上讲，把上述三种网络融合成一种网络就能够提供上述的所有服务，这就是很早以前提出来的“三网融合”。然而，事实并不如此简单，因为这涉及各方面的经济利益和行政管辖权的问题。

20 世纪 90 年代以后，以 Internet 为代表的计算机网络得到了飞速的发展，已从最初的仅供美国人使用的免费教育科研网络，逐步发展成为供全球使用的商业网络（有偿使用），成为全球最大的和最重要的计算机网络。可以毫不夸大地说，Internet 是人类自印刷术发明以来在存储和交换信息领域中的最大变革。

Internet 的中文译名并不统一，现有的 Internet 译名有以下两种。

(1) 因特网。这个译名是全国科学技术名词审定委员会推荐的。虽然因特网这个译名较为准确，但却长期未得到推广。有些地方会采用因特网这个译名。

(2) 互联网。这是目前流行最广的、事实上的标准译名。现在，我国的各种报纸杂志、政府文件以及电视节目中都毫无例外地使用这个译名。Internet 是由数量极大的各种计算机网络相互连接起来的，采用互联网这个译名能够体现出 Internet 最主要的特征。

也有些人愿意直接使用英文名词 Internet，而不使用中文译名，这避免了译名的不准确。但笔者认为，在中文教科书中，常用的重要名词应当用中文表示。当然，在一定的情况下，我们也不排斥使用国际通用的英文缩写词。例如，直接使用更简洁的“TCP”，比使用冗长的中文译名“传输控制协议”要方便得多，这样也更加便于我们阅读外文技术资料。

曾有人把 Internet 译为国际互联网。其实，互联网本来就是覆盖全球的，因此国际二字显然是多余的。

对于仅在局部范围互连起来的计算机网络，只能称为互连网，而不是互联网。

有时，我们往往使用更加简洁的方式表示互联网，即只用一个“网”字。例如，“上网”就是表示使用某个电子设备连接到互联网，而不是连接到其他

的网络上。还有如网民、网吧、网银（网上银行）、网购（网上购物）等。这里的“网”一般都不是指电信网或有线电视网，而是指当今世界上最大的计算机网络 Internet——互联网。

那么，什么是互联网呢？这个概念很难用几句话说清楚。但我们可以从两个不同的方面来认识互联网，即互联网的应用和互联网的工作原理。

绝大多数人认识互联网都是从接触互联网的应用开始的。现在的小孩都会上网玩游戏，看网上视频或和朋友在微信上聊天，而成年人则更多地在互联网上搜索和查阅各种信息。现在，人们经常利用互联网的电子邮件功能相互通信（包括传送各种照片和视频文件），这就使得传统的邮政信函的业务量大大减少。在互联网上购买各种物品，既方便又经济实惠，改变了必须到商店购物的方式。在互联网上购买机票或火车票，可以节省大量排队的时间，极大地方便了旅客。在金融方面，利用互联网进行转账或买卖股票等交易，都可以节省大量时间。需要注意的是，互联网的应用并不是固定不变的，而是不断有新的应用出现。因此，本书无法详细地介绍互联网的各种应用。

从应用这个方面认识互联网的门槛较低，因为这不需要懂得很多互联网的工作原理。现在，很多小学生都能够非常熟练地使用手机上的各种应用程序进行学习和娱乐。本书是大学的计算机网络教材，因此着重讲解的是计算机网络的工作原理而非网络应用。通过掌握计算机网络的基本工作原理，我们可以更好地理解互联网是怎样工作的，从另一个角度来认识互联网。

互联网之所以能够向用户提供许多服务，就是因为互联网具有两个重要基本特点，即连通性和共享。

所谓连通性（connectivity），就是互联网使上网用户之间，不管相距多远（例如，相距数千公里），都可以非常便捷、经济（在很多情况下甚至是免费的）地交换各种信息（数据以及各种音频视频），好像这些用户终端都彼此直接连通一样。这与使用传统的电信网络有着很大的区别。我们知道，传统的电信网向用户提供的最重要的服务就是人与人之间的电话通信，因此电信网也具有连通性这个特点。但使用电信网的电话用户，往往要为此向电信网的运营商缴纳相当昂贵的费用，特别是国际通信。虽然使用互联网通信更加经济便捷，但我们应注意，互联网具有虚拟的特点。例如，当你从互联网上收到一封电子邮件时，你可能无法准确知道对方是谁（朋友还是骗子），也无法知道发信人的地点（在附近，还是在地球对面）。

所谓共享就是指资源共享。资源共享的含义是多方面的，可以是信息共

享、软件共享，也可以是硬件共享。例如，互联网上有许多服务器（就是一种专用的计算机），存储了大量有价值的电子文档（包括音频和视频文件），可供上网的用户很方便地读取或下载（无偿或有偿）。由于网络的存在，这些资源好像就在用户身边一样方便使用。

现在，人们的生活、工作、学习和交往都已离不开互联网。设想一下，某一天我们所在城市的互联网突然瘫痪不能工作了，这会出现什么结果呢？这时，我们将无法购买机票或火车票，因为售票处无法通过互联网得知目前还有多少余票可供出售；我们也无法到银行存钱或取钱，无法交纳水电费和煤气费等；股市交易都将停顿；在图书馆我们也无法检索所需要的图书和资料。互联网瘫痪后，我们既不能上网查询有关的资料，也无法使用电子邮件和朋友及时交流信息，网上购物也将完全停顿。总之，这样的城市将会是一片混乱。由此可以看出，人们的生活越是依赖互联网，互联网的可靠性也就越重要。现在互联网已经成为社会最为重要的基础设施。

互联网现在可以向广大用户提供休闲娱乐的服务，如各种音频和视频节目。上网的用户可以利用鼠标随时点击各种在线节目。互联网还可进行一对一或多对多的网上聊天（文字的、声音的或视频的交流），使人们的社交方式发生了重大的变化。

现在，我们常常可以看到一种新的提法，即“互联网＋”。它的意思就是“互联网＋各个传统行业”，即利用信息通信技术和互联网平台来创造新的发展生态。实际上，“互联网＋”代表一种新的经济形态，其特点就是把互联网的创新成果深度融合于社会经济各领域之中，这就大大地提升了实体经济的创新力和生产力。但同时，我们也必须看到互联网的各种应用对各行各业的巨大冲击。例如，电子邮件迫使传统的电报业务退出市场。网络电话的普及，使得传统的长途电话（尤其是国际长途电话）的通信量急剧下降。快捷方便的网购造成了不少实体商店的停业。原来必须排长队购买火车票的网点已被非常方便的网购所替代。网约车的问世对出租车行业产生了的巨大冲击。这些例子说明互联网应用已对整个社会的各个领域都产生了很大的影响。

互联网给人们带来便利的同时也给人们带来了一些负面影响：有人肆意利用互联网传播计算机病毒，破坏互联网上数据的正常传送和交换；有的犯罪分子甚至利用互联网窃取国家机密和盗窃银行或储户的钱财；有人利用网络进行欺诈行为或在网上肆意散布谣言、不良信息；有的青少年因为沉迷网络而荒废自己大好的青春等等。

由于互联网已经成为世界上最大的计算机网络，因此，我们先对互联网进行概述，包括互联网的主要构件，这样读者就可以对计算机网络有一个初步的了解。

第二节　互联网概述

一、网络的网络

起源于美国的互联网[①]现已发展成为世界上最大的覆盖全球的计算机网络。

我们先给出关于网络、互连网、互联网（因特网）的一些最基本的概念。

请读者注意，在本书中，为了方便，下面出现的“网络”都是“计算机网络”的简称，而不是电信网或有线电视网。

计算机网络（简称网络）由若干结点（node）[②]和连接这些结点的链路（ink）组成。网络中的结点可以是计算机、集线器、交换机或路由器等（在后续的两章，我们将会介绍集线器、交换机和路由器等设备的作用），如图 1-1（a）所示，给出了一个具有四个结点和三条链路的网络。我们可以看到，三台计算机通过三条链路连接到一个集线器上，构成了一个简单的网络。在很多情况下，我们可以用一朵云表示一个网络。这样做的好处是可以不去关心网络中相当复杂的细节问题，因而可以集中精力研究与网络互连有关的一些问题。

网络之间还可以通过路由器互连起来，这就构成了一个覆盖范围更大的计算机网络。这样的网络称为互连网（internetwork 或 Internet），如图 1-1（b）所示。因此，互连网是“网络的网络”（network of networks）。

---

① 注：1994 年，全国自然科学名词审定委员会公布的名词中，Interconnection 是“互连”，interconnection network 是“互连网络”，internetworking 是“网际互连”。但 1997 年 8 月，全国科学技术名词审定委员会在其推荐名（一）中，将 internet、internetwork、interconnection network 的译名均推荐为“互联网”，而在注释中说“又称互连网”，即“互联网”与“互连网”这两个名词均可使用。但请注意，“联”和“连”并不是同义字。术语“互连”一定不能用“互联”代替。“连接”也一定不能用“联接”代替。

② 注：根据 MINGCI194 第 12 页，名词 node 的标准译名是：节点 08.078，结点 12.023。12.023 这一节是计算机网络，因此，在计算机网络领域，node 显然应当译为结点，而不是节点。但不知何种原因，在网络领域中，很多人宁愿使用不太准确的“节点”，也不愿使用标准译名“结点”。

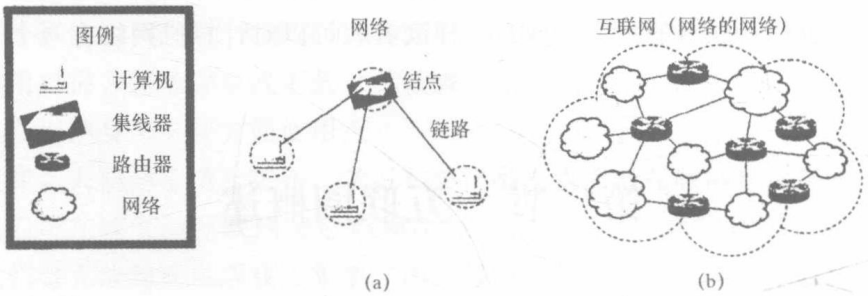

图 1-1　简单的网络（a）和由网络构成的互连网（b）

请读者注意，当我们使用一朵云来表示网络时，可能会有两种不同的情况。一种情况如图 1-1 所示，用云表示的网络已经包含了和网络相连的计算机。但有时为了讨论问题更方便（例如，要讨论几个计算机之间如何进行通信），也可以把有关的计算机画在云的外面，如图 1-2 所示。习惯上，与网络相连的计算机常称为主机（host）。这样，用云表示的互连网里面就只剩下许多路由器和连接这些路由器的链路了。

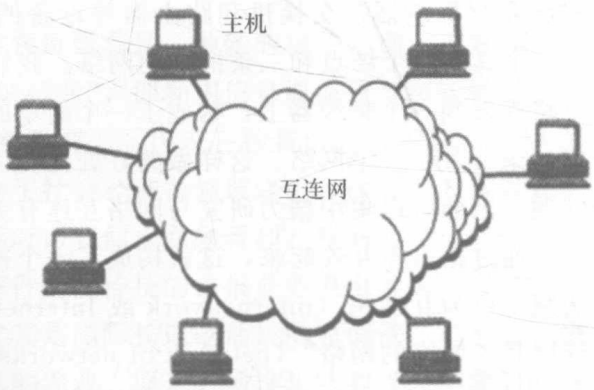

图 1-2　互连网与所连接的主机

这样，我们初步建立了下面的基本概念：网络把许多计算机连接在一起，而互连网则把许多网络通过路由器连接在一起。与网络相连的计算机常称为主机。

还有一点也必须注意，就是网络互连并不是把计算机仅仅简单地在物理上

连接起来，因为这样做并不能达到计算机之间相互交换信息的目的。我们还必须在计算机上安装许多使计算机能够交换信息的软件。因此，当我们谈到网络互连时，就隐含地表示在这些计算机上已经安装了适当的软件，因而在计算机之间可以通过网络交换信息。

现在使用智能手机上网已非常普遍。由于智能手机中有中央处理机 CPU，因此也可以把连接在计算机网络上的智能手机称为主机。实际上，智能手机已经不是个单一功能的设备，它既是电话机，但也是计算机、照相机、摄像机、电视机、导航仪等综合多种功能于一体的智能机器。

二、互联网基础结构发展的三个阶段

互联网的基础结构大体上经历了三个阶段的演进。但这三个阶段在时间划分上并非层次分明而是有部分重叠的，这是因为网络的演进是逐渐的，而并非在某个日期发生了突变。

第一阶段是从单个网络 ARPANET 向互连网发展的过程。1969 年，美国国防部创建的第一个分组交换网 ARPANET 最初只是一个单独的分组交换网（并不是一个互连的网络）。所有要连接 ARPANET 的主机都直接与就近的结点交换机相连。但到了 20 世纪 70 年代中期，人们已经认识到不可能仅使用一个单独的网络来满足所有的通信问题。于是，ARPA 开始研究多种网络（如分组无线电网络）互连的技术，于是产生了互连网络，这就是现今互联网的雏形。1983 年，TCP/IP 协议成为 ARPANET 上的标准协议，使得所有使用 TCP/IP 协议的计算机都能利用互联网相互通信，因而人们就把 1983 年作为互联网的诞生时间。1990 年，ARPANET 正式宣布关闭，因为它的实验任务已经完成。

请读者注意以下两个意思相差很大的名词——internet 和 Internet。

以小写字母 i 开始的 internet（互连网）是一个通用名词，它泛指由多个计算机网络互连而成的计算机网络。在这些网络之间的通信协议（即通信规则）可以任意选择，不一定非要使用 TCP/IP 协议。

以大写字母 I 开始的 Internet（互联网或因特网）则是一个专用名词，它指当前全球最大的、开放的、由众多网络相互连接而成的特定互连网，采用 TCP/IP 协议族作为通信的规则，其前身是美国的 ARPANET。

可见，任意把几个计算机网络互连起来（不管采用什么协议），并能够相互通信，这样构成的就是一个互连网（internet），而不是互联网（Internet）。

第二阶段的特点是建成了三级结构的互联网。从1985年起，美国国家科学基金会（NSF，National Science Foundation）就围绕六个大型计算机中心建设计算机网络，即国家科学基金网（NSFNET）。它是一个三级计算机网络，分为主干网、地区网和校园网（或企业网）。这种三级计算机网络覆盖了全美国主要的大学和研究所，并且成为互联网中的主要组成部分。1991年，NSF和美国的其他政府机构开始认识到，互联网必需扩大其使用范围，不应仅限于大学和研究机构。世界上的许多公司纷纷接入互联网，网络上的通信量急剧增大，这时互联网的容量已满足不了日常需要。于是，美国政府决定将互联网的主干网转交给私人公司来经营，并开始对接入互联网的单位收费。1992年，互联网上的主机超过100万台；1993年，互联网主干网的速率提高到45Mbit/s（T3速率）。

第三阶段的特点是逐渐形成了多层次ISP结构的互联网。从1993年开始，由美国政府资助的NSFNET逐渐被若干个商用的互联网主干网替代，而政府机构不再负责互联网的运营，这样就出现了一个新的名词：互联网服务提供者（ISP，Internet Service Provider）。在许多情况下，ISP就是一个进行商业活动的公司，因此它又常译为互联网服务提供商。例如，中国电信、中国联通和中国移动等公司，都是我国最有名的ISP。

ISP可以从互联网管理机构申请到很多IP地址（互联网上的主机都必须有IP地址才能上网），同时拥有通信线路（大ISP自己建造通信线路，小ISP则向电信公司租用通信线路）以及路由器等联网设备，因此任何机构和个人只要向某个IP交纳规定的费用，就可从该ISP获取所需IP地址的使用权，并可通过该ISP接入互联网。所谓“上网”，就是指“（通过某ISP获得的IP地址）接入互联网”。IP地址的管理机构不会把一个单个的IP地址分配给单个用户（不零售IP地址），而是把一批IP地址有偿租赁给经审查合格的ISP（只批发IP地址）。由此可见，现在的互联网已不是某个组织所拥有而是全世界无数大大小小的ISP所共同拥有的，这就是互联网也称为“网络的网络”的原因。

根据提供服务的覆盖面积以及所拥有的IP地址数目，ISP可以分为三个不同的层次：主干ISP、地区ISP和本地ISP。

主干 ISP 由几个专门的公司创建和维持，服务面积最大（一般都能够覆盖国家范围），并且还拥有高速主干网（例如 10Gbit/s 或更高）。部分地区的 ISP 网络也可直接与主干 ISP 相连。

地区 ISP 是一些较小的 ISP。这些地区 ISP 通过一个或多个主干 ISP 连接起来。它们位于等级中的第二层，数据率也低一些。

本地 ISP 给用户提供直接的服务（这些用户有时也称为端用户，强调是末端的用户）。本地 IP 可以连接到地区 ISP，也可直接连接到主干 ISP。绝大多数的用户都是连接到本地 ISP 的。本地 ISP 可以是一个仅仅提供互联网服务的公司，也可以是一个拥有网络并向自己的雇员提供服务的企业，或者是一个运行自己的网络的非营利机构（如学院或大学）。本地 ISP 可以与地区 ISP 或主干 ISP 连接。

图 1-3 是具有三层 ISP 结构的互联网的概念示意图，但这种示意图并不表示各 ISP 的地理位置关系。图中给出了主机 A 经过许多不同层次的 ISP 与主机 B 通信的示意图。

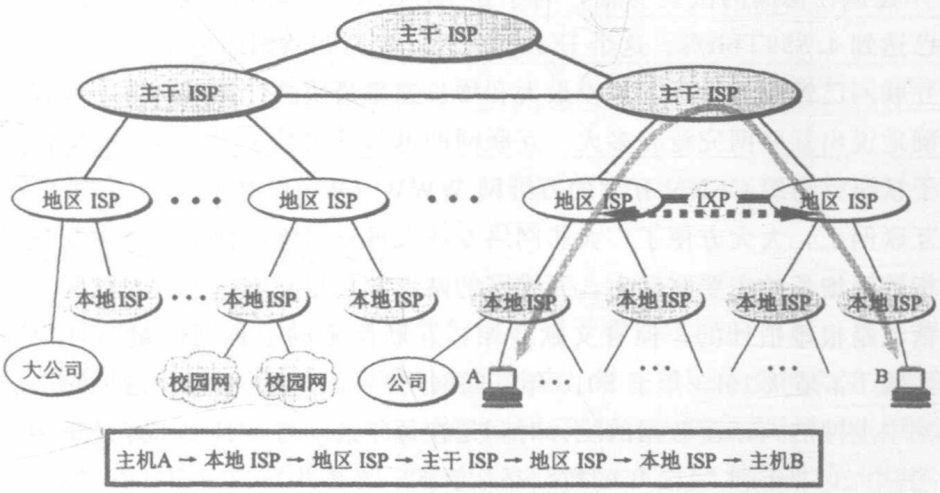

图 1-3　基于 ISP 的多层结构的互联网的概念示意图

从原理上讲，只要每一个本地 ISP 都安装了路由器并连接到某个地区 ISP，且每一个地区 ISP 也有路由器连接到主干 ISP，那么在这些相互连接的 ISP 的共同合作下，就可以完成互联网中的所有分组转发任务。但随着互联网