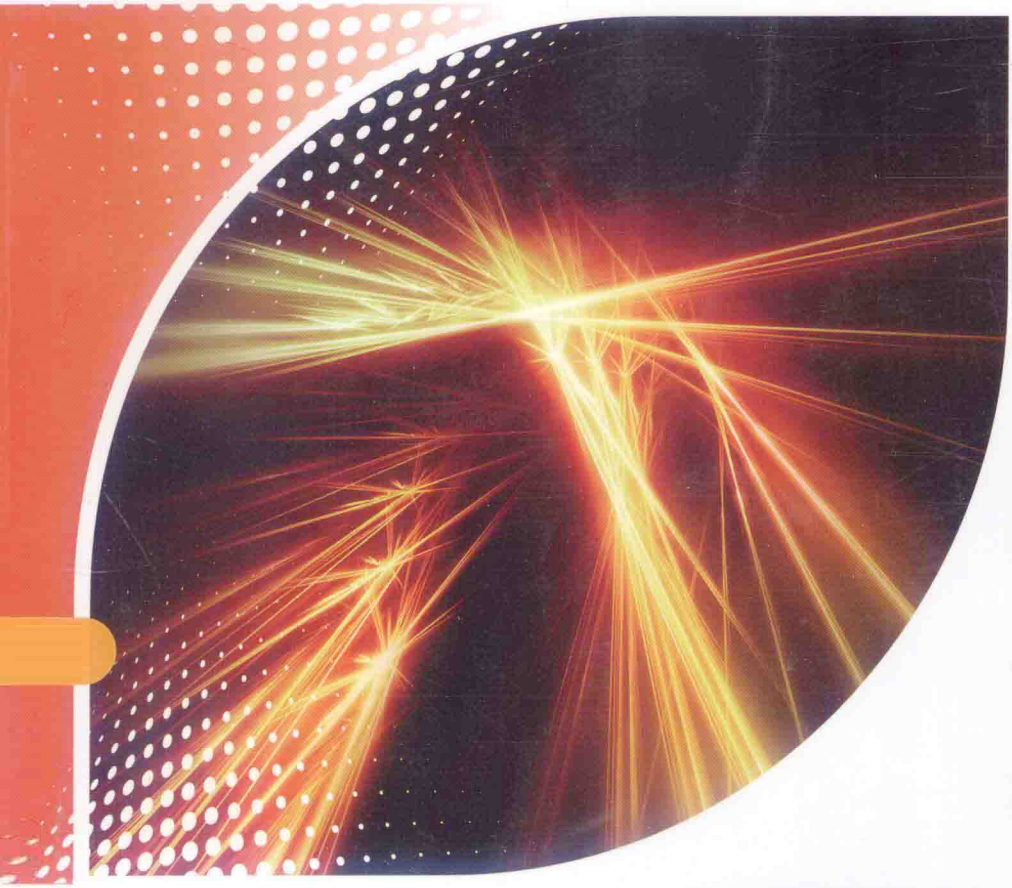
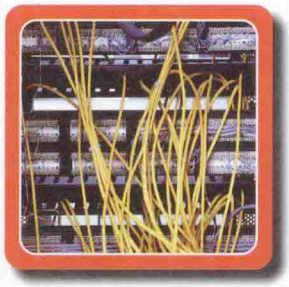
全国高等院校仪器仪表及自动化类“十二五”规划教材

网络技术与应用

◎ 冯先成　程 雯　田 怡　胡中功 等 编著





网络新技术：FTTH、三网融合、物联网技术和移动 IP 技术

QQ 通信安全漏洞及其防御＋以太网交换机设计＋网络仿真实验

因特网上常见服务所面临的各种安全威胁，以及解决威胁的方法

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

http://www.phei.com.cn

全国高等院校仪器仪表及自动化类“十二五”规划教材

网络技术与应用

冯先成　程　雯　田　怡
胡中功　左敬龙　孙　萍　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

“网络技术与应用”是一门专业必修课，其适用对象为测控、计算机、电子、电信、通信、机电、电气自动化等专业本科生。在网络技术飞速发展的今天，让学生在有限的时间内学到更多的知识，只有使用系统的方法来教学。这也是本书想要竭力实现的目标。通过本课程的学习，使学生能够在学习基本数据通信技术的基础上，对计算机网络原理及体系结构有全面的理解与掌握。

本书的特点是具有很强的实用性、针对性、技术性，仿真实验全面，网络设备设计介绍详细，知识覆盖范围广，图文并茂，同时反映计算机网络的一些最新发展技术。本书可供测控、计算机、电子、电信、通信、机电、电气自动化等专业本科生和研究生使用，同时对从事计算机网络相关工作的工程技术人员也有学习参考价值。

图书在版编目（CIP）数据

网络技术与应用/冯先成等编著. —北京：电子工业出版社，2014.2
全国高等院校仪器仪表及自动化类“十二五”规划教材
ISBN 978-7-121-21777-7

Ⅰ. ①网… Ⅱ. ①冯… Ⅲ. ①计算机网络－高等学校－教材 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字(2013)第 258607 号

策划编辑：郭穗娟
责任编辑：苏颖杰
印　　刷：北京市李史山胶印厂
装　　订：北京市李史山胶印厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：20.5　字数：525 千字
印　　次：2014 年 2 月第 1 次印刷
印　　数：3500 册　　定价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

全国高等院校仪器仪表及自动化类“十二五”规划教材

编 委 会

前　言

计算机网络是计算机技术和通信技术密切结合而形成的新的技术领域，是当今计算机的主流技术之一，也是迅速发展并在信息社会中得到广泛应用的一门综合性学科。随着因特网的飞速发展，了解和掌握最新的网络通信技术也变得更加重要。计算机网络是测控、计算机、电子、电信、通信、机电、电气自动化等专业本科生的必修课，也是一门重要的专业课，该课程在专业建设和课程体系中占据重要的地位和作用。

2000 年以来，网络技术发展日新月异，如局域网（特别是以太网）、TCP/IP 网络、VLAN、FTTH、三网融合、物联网等，不断有新思想、新技术涌现出来，这些内容也都需要不断地补充到本课程内容中来。本课程包含了越来越多的知识内容，网络教科书不断更新版本、补充内容，教材也越来越厚［如国外经典教材《计算机网络》（A. S. Tanenbaum），第 3 版、第 4 版，内容增多了，但基础理论部分缩减了］。

本书以网络体系结构和 TCP/IP 参考模型为主线，系统地讲授网络的模型、层次结构、网络通信原理、协议原理、路由原理等方面的内容，为学生的网络知识打下坚实的理论基础，同时也为学生建立一种概念：以太网、TCP/IP 只是网络的一种具体实现，而不是网络的全部，新的网络还可能随时出现。这样可拓宽学生的思路，让学生的想象力和创造力能充分发挥出来。

本书覆盖的知识面很广，第 1 章介绍计算机网络的起源、发展、分类、主要性能指标、TCP/IP 体系结构。第 2 章介绍数据通信系统的组成、性能指标，物理层的基本概念、传输介质。第 3 章着重讨论点对点协议 PPP、以太网、生成树协议 STP、虚拟局域网 VLAN 等。第 4 章详细讨论子网划分、路由与路由协议 RIP、OSPF 的实现机制、下一代的网际协议 IPv6、虚拟私有网 VPN、网络地址转换 NAT 等。第 5 章详细讨论用户数据报传输协议（UDP）、传输控制协议（TCP）的工作机制。第 6 章详细讨论应用层的协议——DNS、FTP、TELNET、E-mail、WWW、DHCP、SNMP、防火墙的工作原理。第 7 章详细介绍网络新技术——FTTH、三网融合和物联网。第 8 章详细讨论以太网交换机的硬件、软件设计。第 9 章详细介绍网络协议分析、通信协议原理、MAC 协议模拟、PPP 仿真、距离矢量、链路状态路由算法仿真、Cisco 19××系列交换机配置、Cisco 26××系列路由器配置等仿真实验。第 10 章介绍因特网安全技术。

尽管理解网络技术的原理很重要，但无助于提高实践动手能力。为提高学生的动手能力，本书在理论讲解的同时，提供大量的仿真实践，突出对学生动手能力的培养，注重实用技术。

本书的特色如下：

（1）本书体现很强的实用性、针对性、技术性——基于单片机控制的以太网交换机设计，二层、三层网络协议仿真等。将光纤通信、计算机网络等理论知识和实用的设备/产品结合起来，具有较强的可读性和可操作性。

（2）介绍网络新技术：

- 2010 年以后，应用最广泛、最受关注的网络新技术是 FTTH、三网融合和物联网技术；

- 移动 IP；
- QQ 通信安全漏洞及其防御；
- 因特网上常见的服务所面临的各种威胁，以及解决威胁的方法等内容。

（3）提供 7 个网络仿真实验。

（4）知识覆盖范围广，详细介绍以太网交换机系统的软/硬件内容设计。

参加本书编写工作的有武汉工程大学的冯先成、胡中功、田怡老师，武汉工程大学邮电与信息工程学院的程雯、孙萍老师，广东石油化工学院的左敬龙老师。全书由冯先成、程雯老师策划、统稿。

尽管我们为本书付出了十分的努力和心血，但书中疏漏和不当之处在所难免，敬请各位读者和专家提出宝贵意见，以便进一步完善教材内容。为配合本书的教学，免费提供电子教案，电子邮件地址：xcfeng68@hotmail.com。

编著者

2013 年 9 月

目　录

第1章 网络概述

1.1 网络的概念

网络（network）是一个复杂的人或物的互联系统。我们周围无时无刻不存在一张网，如电话网、电报网等；即使我们身体内部也存在许许多多的网络系统，如神经系统、消化系统等。计算机网络是21世纪最主要的网络之一。

在计算机网络出现的前期，计算机都是独立的设备，每台计算机独立工作，互不联系。计算机与通信技术的结合，对计算机系统的组织方式产生了深远的影响，使计算机之间的相互访问成为可能。不同种类的计算机通过同种类型的通信协议（protocol）相互通信，产生了计算机网络（computer network）。

计算机网络，就是把分布在不同地理区域的计算机以及专门的外部设备利用通信线路互联成一个规模大、功能强的网络系统，从而使众多的计算机可以方便地互相传递信息，共享信息资源。我们给出一个如此广泛的定义是因为IT业迅速发展，各种网络互联终端设备层出不穷，像计算机、打印机、WAP（Wireless Application Protocol）手机、掌上电脑PDA（Personal Digital Assistant）、网络电话等各种支持网络互联的设备。

一般来说，计算机网络可以提供以下一些主要功能：

（1）资源共享。网络的出现使资源共享变得很简单，交流的双方可以跨越空间的障碍，随时随地传递信息。

（2）信息传输与集中处理。数据是通过网络传递到服务器（server）中，由服务器集中处理后再回送到终端。

（3）负载均衡（load balancing）与分布处理（distributed processing）。举个典型的例子：一个大型ICP（因特网内容提供商）为了支持更多的用户访问它的网站，在全世界多个地方放置了相同内容的WWW（World Wide Web）服务器，通过一定技术使不同地域的用户看到放置在离他最近的服务器上的相同网页，以实现各服务器的负荷均衡，同时用户也节省了访问时间。

（4）综合信息服务。网络的一大发展趋势是多维化，即在一套系统上提供集成的信息服务，包括来自政治、经济等各方面的资源，甚至同时还提供多媒体信息，如图像、语音、动画等。在多维化发展的趋势下，许多网络应用的新形式不断涌现，如电子邮件（E-mail）、视频点播（VOD，Video on Demand）、电子商务（E-commerce）、视频会议（video conference）等，如图1.1所示。

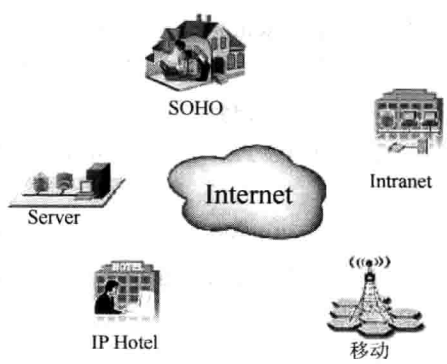


图1.1 网络的多维化

1.2 计算机网络的组成

计算机网络的组成元素可以分为两大类，即网络节点和通信链路。网络节点又可分为端节点和转接节点。端节点指信源和信宿节点，如用户主机和用户终端；转接节点指网络通信过程中起控制和转发信息作用的节点，如交换机、集线器、接口信息处理机等。通信链路是指传输信息的信道，可以是电话线、同轴电缆、无线电线路、卫星线路、微波中继线路、光纤缆线等。网络节点通过通信链路连接成的计算机网络，如图 1.2 所示。

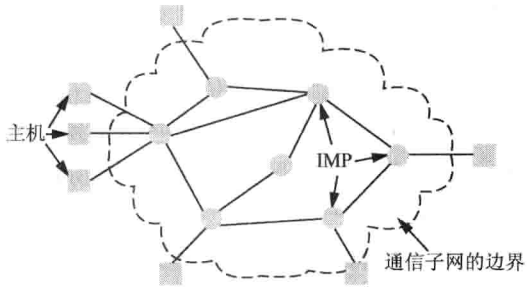


图 1.2 通信子网与资源子网

在图 1.2 中，虚线框外的部分称为资源子网。资源子网包括拥有资源的用户主机和请求资源的用户终端，它们都是端节点。框内的部分叫做通信子网，其任务是在端节点之间传送由信息组成的报文，负责数据通信处理的通信控制处理机与通信线路，主要由转接节点和通信链路组成。接口信息处理机（Interface Message Processor，IMP）是一种专用通信的计算机。

1.3 计算机网络的发展历史

计算机网络起始于 20 世纪 60 年代，当时网络的概念主要是基于主机（Host）架构的低速串行（serial）连接，提供应用程序执行、远程打印和数据服务功能。IBM 的 SNA（System Network Architecture，系统网络架构）与非 IBM 公司的 X.25 公用数据网络是这种网络的典型例子。当时，由美国国防部资助，建立了一个名为 ARPANET（即为阿帕网）的基于分组交换（packet switching）的网络，这个阿帕网就是今天的因特网最早的雏形。

20 世纪 70 年代，出现了以个人计算机为主的商业计算模式。最初，个人计算机是独立的设备，由于认识到商业计算的复杂性，要求大量终端设备的协同操作，局域网（Local Area Network，LAN）产生了。局域网的出现，大大降低了商业用户使用打印机和磁盘昂贵的费用。

20 世纪 80～90 年代，远程计算的需求不断增加，迫使计算机界开发出多种广域网络协议（包括 TCP/IP、IPX/SPX），满足不同计算方式下远程连接的需求，互联网快速发展起来，TCP/IP 得到了广泛应用，成为互联网的事实协议。计算机网络的发展历史如图 1.3 所示。

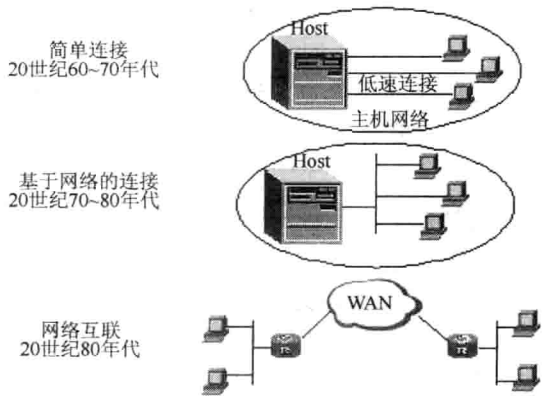


图 1.3 计算机网络的发展历史

1.3.1 军备竞赛和第一次联网

20 世纪 50 年代，美苏展军备竞赛。1957 年 10 月苏联发射第一颗质量为 83.6kg 的人造地球卫星“Sputnik1”，1957 年 10 月苏联第二颗卫星“Sputnik2”发射成功，该卫星质量为 500kg。

1951 年 MIT 成立著名的林肯实验室，研究“远距离预警系统”。这是一个军方主管并操纵的中央控制的中央结构的网络。1952 年，系统建成并投入使用，成为当时远距离访问网络的一个典型，这个网络完成 3 个任务：①采集从各个雷达站搜集来的信号；②通过计算判断是否有敌机来犯；③将防御武器对准来犯敌机。这是一个真正实时的人机交互作用的计算机网络系统，能够接收网络上各个军事部门传送过来的数据，能够按输入的指令来处理这些数据。由于在运行过程中还是需要人工干预，所以被称作“半自动化”系统。这个网络系统在当时的情报搜集方面立下汗马功劳。三个月后，美国成功发射“探险者 1 号”人造地球卫星，质量为 8kg。

美军方一向倚重的中央控制式的计算机网络的信息搜集能力和战时生存能力受到严重质疑。1958 年 1 月，艾森豪威尔总统向国会提出要建立美国国防部高级研究计划署（Defense Advanced Research Project Agency，即 DARPA，后改称 ARPA），希望不再发生毫无准备地看着类似苏联卫星上天这种事情发生。1962 年，古巴导弹危机，中央控制式网络抗打击能力受到现实威胁。美军方向肯尼迪总统提交建议书，为美国当时地网络布局设置感到担忧。肯尼迪命令 DARPA 着手改进网络结构的安全性，以保证美军用网络在遭受打击后，仍能够使各部门之间保持联系。DARPA 实际上是一个研究管理部门，起着组织、管理军事科学研究的作用。

第一个将两台不同的计算机连接起来的实验是由 Thomas Marill 提出来的。1965 年，Marill 代表美洲计算机公司向 ARPA 提交了一份计划，提议在马萨诸塞州和加利福尼亚州之间进行一次联网实验。ARPA 担心 Marill 的公司的规模太小不足以完成这项实验，于是建议由麻省理工学院的林肯实验室来主持这项实验。Roberts 和 Marill 通过只有 1200bps 的电话专线，将麻省理工学院林肯实验室的 TX-2 计算机和加利福尼亚州 SDC 系统发展公司的 Q-32 计算机连接到了一起。这是人类历史上首次实现不同计算机之间的远距离联网，而且，操作系统使用的是分时方式（time sharing）。在多用户环境真正同时处理不同的工作。计算机不是一次处理完一个用户提交的任务，而是为每个用户分配一小段的处理时间，并把用户的任务分成多个小段，然后对这些小段按照先后次序处理，由于计算机的速度很快，所以

用户感觉不到执行中间的停顿。尽管这次实验按计划完成了，并且也达到了预期的目的，可是接下来的问题仍然不少。

首先是传输速度。由于线路长而不稳定，这种联网方式的实际速度只有几百波特率，哪怕只是传送很小的一段信息，也要等上很长一段时间。如果军用网络不能在 1s 内做出反应，就等于没什么用处。

其次是网络的可靠性值得怀疑。由于使用的是电路交换方式，整条电路被占用，在直接从出发点把信号传到目的地的过程中，信号损失可能会很大。当然，应该建立一个什么样的网才是最重要的问题。通过首次联机实验，从侧面说明原有的中央控制型的以电路交换为基础的传统网络理论不适合用来建立新型的网络，也从反面证明了后来 Paul Baran 的理论——长距离传输数据应该使用分布式的包交换网络。

1.3.2 ARPANET 的诞生

1965 年，从国家宇航局（NASA）聘请到的 33 岁的 Robert Taylor 成为 ARPA 的一个关键机构——信息处理技术办公室（IPTO）的主管。Taylor 在位于美国五角大楼的办公室里放了 3 台计算机终端，分别连接着麻省理工学院、加州大学伯克利分校和圣莫尼卡市的主机，以便于和他手下的专家们进行交流。不过，3 台计算机终端的类型各不相同，并且各自使用了一套不同的操作系统。在这种情况下，Taylor 开始考虑实施一个可行的联网计划，一来解决相互交流的问题，二来减少计算机资源的浪费。1966 年，Taylor 走进 ARPA 局长，奥地利物理学家 Charles Herzfeld 的办公室，大胆提出联网项目的建议。由此确定了第一个 ARPANET 计划。而这个项目的领导人，就是 1965 年在林肯实验室负责远程联网实验的 Larry Roberts。Larry Roberts 是林肯实验室高级研究员，时年 28 岁。

1.3.3 ARPANET 面对的问题及解决

Roberts 加盟 ARPA 后，果然不负众望，他雷厉风行地调度人马，设计项目方案，不到一年时间，就提出了网络的构想。由于整个研究是在 ARPA 的组织下进行的，所以这个网被称做“ARPANET”（阿帕网），也就是“国防高级研究计划网”的意思。而后，Larry Roberts 就当之无愧地被称为“阿帕网之父”。

随着计划的不断改进和完善，Roberts 在描图纸上陆续绘制了数据以百计的网络连接设计图，ARPANET 框架结构逐渐成熟。不过，就在这期间遇到了两个棘手的问题：①如何使不同的计算机相互理解彼此的数据；②以怎样的方式将不同的计算机连接起来。

第一个问题：当时，不同的计算机之间无法相互通信。每家制造商都使用自己的方式来表示字母、数字和控制码。那时，在计算机中表示字符的方式就有 60 多种，单是 IBM 一个公司的设备中就使用了 9 种不同的字符集。虽然 Bob Bemer 1963 年就编完 ASCII，然而它被普遍采用却是 18 年以后的事了。在此之前，不同的计算机因为不同的字符集和不同的操作系统而根本无法直接相连交换信息。

第二个问题：是指采用什么样的网络结构和传输方式。尽管在此之前已经有人提出了分布式网络的理论，可是仍然还有不少人觉得应该使用由中央控制的电路交换网。因为，他们认为电话网是电路交换网的典型，既然电话网工作得很好，为什么按这种方式建立的计算机网络就不能好好地工作呢？他们甚至提议将网络控制中心放在奥马哈，因为这个城市正好处于美国的地理中心。以后的事实证明，这只是一个典型的经验性错误。第一次联

网实验已经证明这种方式不适合用来建立新型的数据网络，也不是符合国防部对新型网络的要求。

第一个问题的解决：1967年初，Taylor和Roberts在密歇根州安阿伯市召开了一次联网实验研讨会，请各研究人员对这个问题发表见解。在会上，多数人对Roberts的ARPANET计划持怀疑态度，因为不同的计算机硬件和软件互不兼容，计算机之间直接通信不仅困难重重，而且管理十分不便。不久，Roberts在林肯实验室的计算机专家W.clark的建议下，认识到应该设计出一种小型专用计算机，让它充当中介物，将不同计算机的数据转换成统一的格式然后进行传输。实际上，Clark此前就发明了一台用于实时数据采集用的计算机LINC（其功能类似于现在的MODEM），LINC拥有1KB内存，而且成本不超过2.5万美元。除了缺少微处理器之外（当时微处理器尚未发明），它实际上就是一台计算机。由于资金不足，Clark的LINC并没有最终实现，但类似于LINC这种简单的计算机完全符合条件去解决ARPANET设计中的这道难题。按照Clark的思想，所有提供资源的大型主机都不必亲自参与联网，而只需在网络与主机之间插入一台中介计算机。中介计算机只需做两件事：第一，接受远程网络传来的信息并转换为本地主机使用的格式；第二，负责线路调度工作，也就是说，为本地传出的信息选择输出路线，然后传递出去。这样一来，在网络上实际相互“对话”的只是统一的中介计算机。这个完美的方案从根本上解决了计算机系统不兼容的问题。Roberts将中介计算机正式命名为“接口信息处理机”（Interface Message Processor，IMP）。而IMP就是我们今天所熟悉的网络路由器（router）的雏形。1967年10月，美国计算机学会在田纳西州盖特林堡召开年会。Roberts抓住这次难得的机会，在会议上宣读了有关ARPANET的论文。虽然，论文中提出ARPANET中可以使用IMP来实现互不兼容的计算机联网，但网络通信可靠性差的缺陷还是让他感到不安。因为，ARPA要求他建设的是一个能够经受核攻击的通信网络。

第二个问题的解决：当时正处于冷战的紧张时期，像电话系统那种高度集中式的网络，即使主要系统的一小部分遭到损害，所有的长途通信都会被中断。至此，Roberts还没有找到一个既能高效传送信息，又能承受攻击的理想办法。英国科学家Donald Davies的研究成果给了Roberts启发。Devies提出的分组交换技术，使Roberts预感到难题即将解决。实际上，在Davies提出分组交换技术的两年内，美国兰德公司的Paul Baran已经提出类似的理论。于是，Roberts找出Baran提出的关于分组交换技术的报告，进行反复研究。1962年，在有军方思想库之称的兰德公司（RAND）工作的Paul Baran为公司提交了11份报告，讨论我们今天称为“包交换技术”（packet switching）和“存储转发”（store and forward）的工作原理。在这11份报告中，影响最大的是1964年3月发表的《论分布式通信网络》（On Distributed Communications Networks）。在这份报告中，概括了“冗余联结”的原理，并举出了多种可能的网络模型。用专业的网络理论来解释，传统的网络模型是“中央控制式网络”；Baran提出的网络模型是“分布式网络”（distributed networks）。Baran在报告中提出，要建立一种没有明显中央管理和控制的通信系统，在这种系统中，每一点都可以和另一点建立联系，这样破坏网络中的任何一点都不至于破坏整个网络。

分布式网络理论的提出，是网络发展中最具关键性的一步，它基本上奠定了现在互联网的特质：分布、开放、不受中央控制。英国国家物理实验室（NPL）的戴维斯（Davids）于1966年也提出了“分组”（packet）的概念，而在提出这个概念的会议上恰好就有ARPANET之父——Roberts。