- TCP/IP 简介
- ARP 与 RARP 通讯协议
- IPv4 与定位
- IPv4 静态路由
- OSPF 通讯协议
- 网络地址转换与防火墙
- IP Version 6
- 传输层通讯协议——TCP 与 UDP

Red Hat Linux 9 网络管理

□ 李蔚泽 编著

清华大学出版社

Red Hat Linux 9 网络管理

李蔚泽　编著

清华大学出版社

北　京

内 容 简 介

Linux 绝佳的网络功能堪称当今操作系统中的佼佼者，无论在功能或支持工具上，都有令人满意的表现。建立强有力的网络系统，Linux 将是最佳的选择，但在使用 Linux 的网络功能之前，需要对网络管理有清晰且正确的概念，这是本书的重点所在。

本书是一本理论与实务并重的书籍，它将原本复杂的 TCP/IP 网络管理，以 15 个章节来分别讨论。同时，为了使读者都能奠定扎实的基础，本书特别遵循 OSI 与 TCP/IP 的层级架构，从网络传输的最底层行为逐层介绍，并以最新版的 Red Hat Linux 9 为操作平台，本书可以使每位读者在最短的时间内掌握网络管理的精髓。

本书具体内容包括：网络架构与技术、TCP/IP 简介、ARP 与 RARP 通信协议、IPv4 与寻址、网络基本管理、IPv4 静态路由、动态路由管理、OSPF 通信协议、ICMP 与 IGMP、网络地址转换与防火墙、IP Version 6、传输层通信协议—TCP 与 UDP、应用程序层、常见的网络应用程序、故障排除与系统监视。

本书适用于政府机关、企事业单位、学校的网络管理人员及广大网络爱好者参考学习。

版 权 声 明

图书在版编目（CIP）数据

Red Hat Linux 9 网络管理/李蔚泽编著. —北京：清华大学出版社，2003

ISBN 7-302-07871-8

Ⅰ. R… Ⅱ. 李… Ⅲ. Linux 操作系统 Ⅳ. TP316.89

中国版本图书馆 CIP 数据核字（2003）第 122102 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：许存权

文稿编辑：余　姬

封面设计：秦　铭

版式设计：冯彩茹

印 刷 者：北京通州大中印刷厂

装 订 者：三河市化甲屯小学装订二厂

发 行 者：新华书店总店北京发行所

开　　本：185×260　**印张**：23.25　**字数**：515 千字

版　　次：2004 年 1 月第 1 版　2004 年 1 月第 1 次印刷

书　　号：ISBN 7-302-07871-8/TP·5718

印　　数：1～5000

定　　价：32.00 元

序

随着全球网络化的盛行，面对国内一片针对微软售价的斥责，无论企业或个人都急于寻找一个既稳定又经济的操作系统，满足网络管理的需求。相信许多人也会直接想到“Linux”这个令人又爱又恨的东西，虽然它具有数不尽的优点，但是学习的门坎极高，又让许多人望而却步。

所谓“师父领进门，修行在个人”，这一直是笔者从事写作时心中的那把尺，因为无论学识如何渊博，都无法在一本书中道尽所有细节。所以，笔者只希望在与读者一同学习这个主题时，能担任启蒙的角色，给予各位正确的观念，同时消去因无知带来的恐惧。

本书共包含 15 个章节，各章节的顺序原则上都遵循 OSI 与 TCP/IP 的层级架构，由下而上逐层介绍，这可增加学习的效率。因此，建议读者依照本书的章节顺序研读，以保持学习的连贯性。

在本书开始的第 1 章、第 2 章中，介绍与网络架构和 TCP/IP 有关的基本内容，这是所有网络管理员必备的基本知识。第 3 章是说明 ARP 与 RARP 通信协议的主题，这也是所有网络活动的基础。

第 4 章至第 11 章介绍 TCP/IP 最重要的层级——网络层，在网络层中主要讨论的主题是寻址与路由通信协议，如 IPv4、IPv6、OSPF、ICMP、IGMP、NAT 与防火墙的内容都包含于此。由于此处的理论性较强，所以最好的学习方法就是配合工具的操作，来验证理论的实用性。

第 12 章、第 13 章和第 14 章分别介绍传输层和应用层的功能，其中包含 TCP、UDP 以及许多常见的网络应用程序。在本书第 15 章，介绍日常维护时的故障排除与系统监视原则，同时配合多种工具的使用，帮助读者实际应用于日常的工作。

全书是笔者经过许多研究测试，以及无数挑灯夜战的成果，虽然辛劳，但求能满足读者的需求，同时也希望它是我们共同学习的起点。如果本书有遗漏或不详之处，还请读者不吝赐教与提携，以使本书再版时更臻完美。

李蔚泽

2003 年 4 月

本 书 特 色

Linux 绝佳的网络功能堪称当今操作系统中的佼佼者，无论在功能及支持工具上，都有令人满意的表现。因此，若正考虑建置强而有力的网络系统，Linux 将会是最佳的选择，但在使用 Linux 的网络功能之前，需要的是对网络管理清晰且正确的概念，这也是本书强调的所在。

本书是一本理论与实务并重的书籍，它将原本复杂的 TCP/IP 网络管理，以 15 个章节来分别讨论。同时，为了使读者都能奠定扎实的基础，笔者特别遵循 OSI 与 TCP/IP 的层级架构，从网络传输的最底层行为逐层介绍，并以最新版的 Red Hat Linux 9 为操作平台，相信可以使每位读者在最短的时间内，掌握网络管理的精髓。

使用本书可以了解以下的重点：

- 网络的类型
- 网络架构与技术
- TCP/IP 简介
- ARP 与 RARP 通信协议
- IPv4 与寻址
- 网络基本管理
- IPv4 静态路由
- 动态路由管理
- OSPF 通信协议
- ICMP 与 IGMP
- 网络地址转换与防火墙
- IP Version 6
- 传输层通信协议——TCP 与 UDP
- 应用程序层
- 常见的网络应用程序
- 故障排除与系统监视

目　录

第 1 章　网络架构与技术

- ✦ 网络的目的与优点
- ✦ 网络的类型
- ✦ 什么是拓扑
- ✦ 缆线的种类
- ✦ 以太网络与存取方法

在本书的开始，先不直接切入 **TCP/IP** 的核心主题，而是先说明有关网络架构及技术等基本概念，因为这些内容不仅是每位读者都应该具备的知识，更与后面的章节息息相关，所以无论以前是否已学习过这方面的内容，希望读者能通过本章的介绍，可以对网络有基本的认识。

1.1　网络的目的与优点

“网络”（Network）可能是近 10 年来最热门的名词，不仅仅是信息业，似乎各行各业都急于与它产生关连，而这种种的现象都只是为了获得使用网络的最大目的——共享（Sharing）。

在传统的单机（Standalone）时代里，所有的资源都属于个人，因此在使用上相当不便，这也间接阻碍了信息的流通。例如业务部门的人员若需要使用会计部门的账目数据时，必须先到会计部门的计算机中，将数据复制到磁盘中，然后再回到业务部门进行读取。但若是这两个部门的距离很远，则花费在传递的时间就可想而知，这也是促成网络发展的最大动力。

而在使用网络后，计算机间的实体距离可完全由网络传输来取代，也就是说，以往需由人员亲自进行的信息交换，在网络环境中都可通过电子信号的传递来执行，这样可加速信息的传播能力。除此之外，使用网络的优点还有：

- ✦ 节省数据储存空间

在单机的环境中，使用者经常需要使用相同的信息，例如员工通信簿，因此每台计算机都必须储存这份数据。但若是改以网络的方式，管理员可以只建立一份数据，然后将它共享在网络上，就可大大降低数据的储存空间。

- ✦ 维持信息正确性

在网络中使用单一版本的文件，除了降低数据储存的空间外，另一个好处是可以维持信息的正确性，而不会因为使用者个别的修改，而造成信息内容的不同步，这个现象在数据库（Database）中更显得重要。

✦ 硬件的共享

系统在网络化后，不仅属于软件方面的文件可以共享，其他硬件也同样具有此功能，其中最常见的例子就是“网络打印机”。也就是说，利用共享的概念，原本个人使用的打印机，可以通过网络的连接以供其他人员使用，这可节省在硬件方面的投资，如图 1-1 所示。

✦ 在线通信

通过网络的传输，使用者之间的通信变得迅速又简单，因此应运而生的是多种在线通信方式，例如电子邮件、电子功能调度（Scheduling）和群件软件（Groupware）等，这些新式的通信方法可同时兼具经济与效率的优点。

图 1-1 利用网络共享打印机

1.2 网络的类型

网络的设计虽然各有不同，但是依照网络的特性与功能，可以简单地区分为“对等式”与“主从式”两类，在本节中，将分别说明这两种网络类型的定义，以帮助读者建立正确的概念。

1.2.1 对等式网络

“对等式”（Peer-to-Peer）是网络设计上最简单的类型，如同它的名称一样，计算机与计算机之间都是“对等”的关系，也就是说，并没有谁隶属于谁的概念，每台主机都拥有独立的文件与打印机等资源。而它们与独立于操作系统的主机的不同只在于通过网线将

彼此相互连接并且共享资源，以提高资源的使用性，一般常见的“组”（Group）就是属于对等式的结构，如图 1-2 所示。

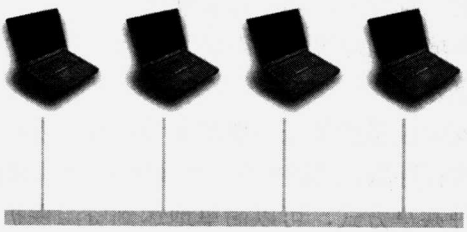

图 1-2　对等式网络

对等式网络的适用环境

对等式网络虽然具有简单的特性，但并不是所有的网络都适合使用这种架构，以下是在决定使用对等式网络前所应考虑的重点：

✦　网络大小

这是用来决定是否选择对等式网络的首要考虑，因为在规划后若要变更为从式架构，必须重新设计所有的内容，包括操作系统、安全性和扩充性等。而最简单的判断方式是，一般对等式网络大多适用于少于十台计算机的网络环境，当然这并非是绝对的标准，但因为管理上缺乏统一的机制，所以若对等式网络中的主机数目太多，则容易增加管理上的困难。

✦　成本

网络架构的成本很难以绝对的方法来判断，较客观的方式是与主从式网络作比较，得到相对低的成本估算。对等式网络因为软件、缆线或网络设备的不同，都比主从式网络相对便宜，因此若有预算上的限制，可以采用此方式来架构网络。

✦　操作系统

由于对等式网络的架构较为简单，所以几乎目前所有的网络操作系统（Network Operating System，NOS）都可用来组成对等式网络，例如 Windows XP、Windows NT 和 Windows 2000 等。

✦　网络所在位置

因为对等式网络的计算机大多数让一般使用者作为桌面计算机，所以通常所处的位置较为集中，而且不需置于特殊的环境，例如控制温湿度或是有门卫管制的房间。

✦　管理方式

管理方式是对等式网络与主从式网络最大的不同点，在对等式环境中，每一台计算机的使用者都具有管理权限，也就是说，该使用者能指定计算机中的文件或打印机是否提供其他人使用。这个管理方式虽然可以符合每位管理员的需求，但也缺乏一套统一的标准，因此在主机数目较多的网络中，常会造成使用者诸多不便，例如使用者欲存取不同的资源前，必须取得该台计算机管理员设定的密码。

✦ 未来发展

因为对等式网络在主机数量和管理方式上都有所限制，所以扩充的能力较差，若是企业网络在可预见的未来将有大幅变动，则不建议使用。相反地，如果网络并不会有太大的扩充机会，例如大型办公环境，则对等式网络仍不失为一简便的解决方案。

✦ 安全性与资源共享方式

对等式网络最常见的安全性措施就是在资源上设定密码保护，不论任何人，只要知道该项资源的密码都可对其进行存取，这种安全性等级就称为共享级（Sharing Level）。如果在小范围的网络中使用这种共享方式，可以简单地达到资源保护的目的，但是无法依照个别使用者进行限制，所以若需要高度安全性的环境并不建议使用对等式网络。

1.2.2 主从式网络

“主从式”（Client/Server）是目前最有效率的网络设计，它是由少数强而有力的“服务器”（Server）来担任资源的提供者，而在使用者（Client）的计算机中只存放客户端程序。因为客户端与服务器可能分别存在不同的网络上，例如服务器可能位于公司的局域网上，而客户端则来自世界各地，并通过 Internet 来进行存取，这可使网络的设计更有弹性，如图 1-3 所示。

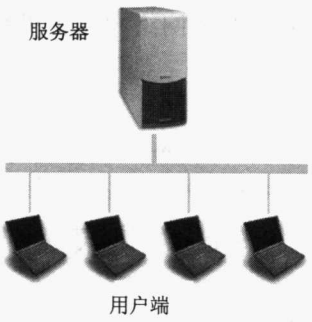

图 1-3 主从式网络

主从式网络的适用环境

主从式网络虽然具有较强的功能，但并非所有网络都适合这种架构，以下是主从式网络所应考虑的重点：

✦ 网络大小

这是用来决定是否选择主从式网络的首要考虑，因为在主从式网络中需配备为数不等的服务器，所以通常网络中包含的主机数量也较多，一般都在 10 台计算机以上。所以若是网络中的主机数目众多，主从式架构应该是较佳的选择。

✦ 成本

主从式架构的成本通常都比对等式网络高，因为需使用数台担任服务器的计算机（不

提供一般客户端使用），而且这些计算机的等级均较一般客户端计算机高，因此若没有预算上的限制，建议使用此方式来架构网络。

✦ 操作系统

由于主从式网络中担任服务器的计算机，必须同时服务许多客户端，所以使用的操作系统也和一般客户端不同，通常用来担任服务器的操作系统有：Linux、Windows NT/2000 和 Novell 等。

✦ 网络所处环境

因为主从式网络中的服务器需要保持极佳的效能，以随时接受来自客户端的要求，所以除了管理员之外，一般使用者不应在服务器上操作。同时为了安全性及其他温湿度的要求，大多数的服务器都位于专用的房间内，例如有门卫管制的恒温环境。

✦ 管理方式

主从式网络与对等式网络在管理方式上极为不同，在主从式的环境中，客户端计算机并没有共享的资源，因为所有的共享资源都集中在少数的服务器中，这是属于集中式（Centralization）的管理模式。在此架构下，所有文件或打印机的存取都凭借管理员的指定，而且因为系统维护工作较为专业和繁重，所以需要专门的人员来担任。

✦ 未来发展

在主从式网络中，最重要的角色是服务器，若是服务器的功能强大，则可服务大量的客户端，例如万维网服务器就是最好的例子，因此主从式网络具有较佳的扩充能力。若是企业网络在可预见的未来将有大幅变动，则建议使用主从式架构。

✦ 安全性与资源共享方式

主从式网络在安全性和资源共享上都较对等式网络更好，因为主从式网络并不直接对资源设定存取密码，而是以个人使用的账号及密码为根据，这种以“个人”为主的安全性等级就称为“用户级”（User Level）。例如，管理员可以授予用户 Jack 和 Tom 对打印机不同的使用权限。

1.3　什么是拓扑

在讨论网络的主题时，“拓扑”（Topology）是相当重要的专有名词，它是指网络上的计算机、缆线、集线器以及其他设备所组成的配置方式，有时也用 Physical Layout、Design、Diagram 和 Map 的名称。因为在计算机能够共享资源或执行其他通信任务前，彼此必须以介质相互连接，而为了提高网络运作的效能，管理员必须设计良好的拓扑规划。

所有的拓扑都是源自 3 种基本设计：总线型、星型和环型，只要利用此 3 种基本拓扑，就可延伸出多种的拓扑应用，因此在本小节中，将详细说明 3 种基本拓扑的内容。

1.3.1 总线拓扑

“总线”（Bus）是最早出现的网络拓扑类型，它是属于线型（Linear）的结构，它利用一条电缆线将网络上的所有计算机连接起来，这条主要的电缆就称为“主干线”（Backbone），如图 1-4 所示。

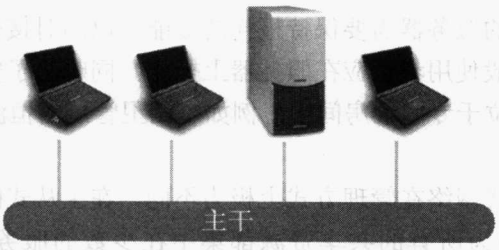

图 1-4 总线与主干

在总线中的任一台计算机传送数据时，网络上所有的计算机都会接收到此广播的消息，但是只有目标计算机才会接收来自传送端的数据，而其他计算机则会丢弃此消息。因为在同一个时间内只允许一台计算机传送数据，而其他计算机若要传送数据则必须等待，直到网络中没有任何广播消息为止，所以总线拓扑属于“竞争式”的拓扑。

虽然总线网络较为单纯，而且架设成本也很低，然而只要某一节点发生问题的时候，整个网络便会瘫痪，所以总线网络并不适用于有大量计算机的网络。

在总线拓扑中，计算机之间进行通信必须注意以下 3 个重点：

- 发送信号：网络数据以广播的方式发送到网络中的所有计算机，但只有指定的目标主机才可接受信息，其他计算机则将此信息丢弃。
- 信号反弹（Signal Bounce）：因为数据是发送给整个网络，所以会沿着整个电缆一个接着一个传输下去，如果信号不被终止的话，它将会反弹，并继续沿着电缆一直传输回来，进而阻止其他的计算机发送信号，因此信号只要到达正确的目标地址，它就必须中止。
- 端接器（Terminator）：要阻止信号继续反弹，网络缆线的两端必须放置一个称为“端接器”的组件来吸收多余的信号，如图 1-5 所示。

图 1-5 端接器

信号加强

当网络的距离增加时，原来由传送端送出的信号会因距离的增加而减弱，若是信号强度降低至一定的限度后，会引起信号的无法辨识，甚至于目的地计算机会得到错误的信息。为了避免这个问题，可以使用“中继器”（Repeater）来加强或是重新产生信号，它的功能和模拟信号中的“放大器”（Amplifier）一样。因此，为了确保信号的正确，必须在一定的距离内使用中继器。

但在使用中继器重新产生信号时需注意一点，在 802.3 协议中规定必须遵守“5-4-3 原则”（5-4-3 Rule），此原则的内容如下：

- 所谓的“5”是指网络最多只能有 5 个网络区段（Segment），而所谓 Segment 是网络上的一个区段，在区段内所有的计算机都使用同一个传输媒介。
- 所谓的“4”是指网络上最多只能使用 4 个中继器。
- 所谓的“3”是指在 5 个网络区段中，最多只能利用 3 个区段来连接计算机，其余的两个区段必须净空，以作为内部连接（Inter-Link）之用，如图 1-6 所示。

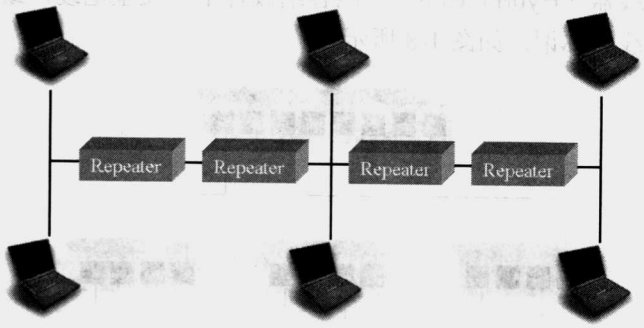

图 1-6　“5-4-3 原则”示意图

1.3.2　星型拓扑

星型拓扑是目前最为普遍的布线方式，网络上的各节点都连接到一个中继设备，通常这个中继设备就是“集线器”（Hub）。若是星型网络上的任何一个节点发生问题，也不会影响到其他节点，所以星型网络的优点是其稳定性较总线网络高，但架设此种网络比起总线网络需要额外的集线器成本，而且通常必须使用较长的缆线，如图 1-7 所示。

集线器的使用

虽然星型拓扑中的任一节点故障都不会影响其他计算机的通信，但若是集线器无法正常工作，则所有的计算机将完全无法传送数据，因此集线器可说是星型拓扑中最重要的组件。