第 10 章　Linux 网络基础

Linux 具备强大的网络功能，可与当前绝大多数主流的网络操作系统保持良好的兼容性。Linux 沿袭 UNIX 系统，采用 TCP/IP 作为主要的网络通信协议，同时也提供对 IPX/SPS、AppleTalk、ISDN、PPP、SLIP、PLIP、ATM 等协议的支持。由于 Linux 性能稳定，因此许多 ISP 都采用 Linux 架设网络服务器，包括 WWW、FTP、Mail Server、DNS 等。在对 Linux 主机进行基本的网络配置之后，可以使用该主机与其他主机进行通信。

10.1　计算机网络的发展

计算机网络是将地理位置分散的多台计算机按着通信协议有机地联接起来，实现计算机之间的信息交通、资源共享和协同工作的计算机复合系统。

计算机网络最早出现在 20 世纪 50 年代中期，源于美国的半自动地面防空系统(SAGE)。当时 SAGE 系统能够将远距离的雷达和测控设备的信息经过通信线路汇集到一台 IBM 计算机上进行处理和控制。通常 SAGE 被认为是计算机技术和通信技术相结合的最初尝试。

在 60 年代中后期，美国国防部(Department of Defense，缩写为 DoD)日益认识到其对计算机网络的依赖性，出于“如果敌人破坏了我们的网络会发生什么情况？我们会无法访问我们的计算机吗？”这样的考虑，于 1969 年由美国高级研究计划署(ARPA，Advanced Research Project Agency)组织和成功研制的世界上公认的第一个远程计算机网络 ARPAnet 网络。

ARPAnet 网络在 1969 年建成时仅有 4 个试验节点，到 1971 年 2 月已扩充为具备 15 个节点、23 台主机的计算机网络，并正式投入使用。由于现代计算机网络的许多概念和方法都起源于 ARPAnet，因此，人们通常将其视为是计算机网络的起源，同时也是 Internet 的起源。计算机网络发展到今，一般可分为以下四个阶段：

10.1.1　面向终端的计算机通信网络

计算机技术与通信技术结合，形成了计算机网络的雏形。此时的计算机网络仅仅是以单台计算机为中心的远程联机系统，因此也被称为“面向终端的计算机通信网络”。美国在 1963 年投入使用的飞机订票系统 SABRE-l，就是这类系统的典型代表之一。此系统以一台中心计算机为网络的主体，将全美范围内的 2000 多个售票终端通过电话线连接到中心计算机上，从而实现了联网订票。

10.1.2　初级计算机网络

随着计算机与通信技术的进一步发展，以及计算机网络体系结构与协议的深入研究，形成了最初的计算机网络，此时的计算机网络一般称为“初级计算机网络”。其中，20 世纪 60 年代后期到 20 世纪 70 年代初期发展起来的美国高级研究计划署的 ARPAnet 网络就是这类系统的典型代表。此时的计算机网络是由若干个计算机互联而成。同时，ARPAnet 网络将一个计算机网络划分为“通信子网”和“资源

子网”两大部分，目前的计算机网络仍沿用这种组合方式。

ARPAnet 网络是计算机网络技术发展过程中的一个里程碑，它的研究成果对促进网络技术的发展起到了十分重要的作用，ARPAnet 网络也为 Internet 的形成奠定了坚实的基础。

10.1.3　开放式的标准化计算机网络

20 世纪 70 年代末至 20 世纪 90 年代逐渐形成了“开放式标准化计算机网络”。这里指的“开放式”是相对于以往那些只能符合独家网络厂商要求的各自封闭的系统而言。在开放式网络中，所有的计算机和通信设备都遵循着共同认可的国际标准，从而可以保证不同厂商的网络产品可以在同一网络中顺利地进行通信。事实上，目前存在着两种占主导地位的网络体系结构，一种是 ISO(International Standards Organization，国际标准化组织)的 OSI(开放式系统互联)体系结构；另一种是 TCP/IP(传输控制协议/网际协议)体系结构，它也是事实上的网络标准。

10.1.4　新一代的计算机网络

互联网(Internet)的进一步发展要求新一代计算机网络必须提供高速、大容量、安全的综合性数字信息传递机制。通过使用 IPv6 技术，新一代互联网的 IP 地址空间将进一步扩展，现有的 IPv4 地址空间紧缺问题将得到解决；通过采用多层次路由结构、分层目录管理等技术，新一代互联网将有可能解决目前网络管理的无政府状态。总之，正在研究与发展着的“新一代的计算机网络”将向着全面互联、高速和智能化发展，并将继续得到更为广泛的应用。

10.2　网络基本类型

对计算机网络进行分类的标准很多。例如，按网络的覆盖范围分为，局域网 LAN(Local Area Network)、城域网 MAN(Metropolitan Area Network)、广域网 WAN(Wide Area Network)和互联网(Internet)。按网络的拓扑结构分类，星型结构、环型结构、总线型结构、星型和总线型结合的复合型结构。这些划分标准都从不同角度对计算机网络特征进行了描述。

10.2.1　按地理覆盖范围

按地理覆盖范围划分是一种通用网络划分标准。按该标准可以把各种网络类型划分为局域网、城域网、广域网和互联网四种。局域网一般应用于办公楼群、校园网、工厂及企事业单位等相对较小的区域内；城域网通常应用于一个大型城市或都市地区；广域网络也称为远程网，所覆盖的范围比城域网更大，一般是在不同城市之间实现互联；而互联网是全球范围内的计算机的互联互通。

1. 局域网(LAN)

局域网顾名思义即指在局部地区范围内使用的网络，其覆盖的地区范围较小，一般在几公里以内，最大距离不超过 10 公里，一般用于组建一个部门或单位的内部网络。通常所说的“LAN”就是指局域网。

局域网是在小型计算机和微型计算机大量推广使用之后才逐渐发展起来的计算机网络。一方面，局域网拓扑结构简单、组网灵活方便、易于管理与配置；另一方面局域网速率高，延迟小、成本低廉，因

此，深受广大用户的欢迎。局域网是目前最常见、应用最广也是最活跃的一种网络。

IEEE 的 802 标准委员会按介质访问方式定义了多种局域网，主要包括：以太网（Ethernet）、令牌环网（Token Ring）、光纤分布式接口网络（FDDI）、异步传输模式网（ATM）以及无线局域网（WLAN）。

2. 城域网(MAN)

城域网采用的是 IEEE802.6 标准，是介于局域网与广域网之间的一种大范围的高速网络，连接距离可以在 10～100 公里。

随着局域网的广泛使用，人们逐渐要求扩大局域网的使用范围，或者要求将已经使用的局域网互相连接起来，使其成为一个规模较大的城市范围内的网络，即城域网。例如将同一个城市内的政府机构的局域网、医院的局域网、电信的局域网以及公司企业的局域网连接起来组成城域网，从而实现大量用户、多种信息资源的互联互通。

城域网与局域网相比覆盖的范围更大，连接的计算机数量也更多，从某种意义上讲，是局域网在地理范围上的延伸。由于光纤连接的引入，使城域网中的高速互连成为可能。城域网既可以是私人网，也可以是公用网；既可以支持数据和语音传输，也可以与有线电视相连。

城域网多采用 ATM 技术做为骨干网。ATM 采用固定长度（53 字节）的 “信元交换”技术来替代传统的“包交换”技术，可以为不同的应用提供 25、51、155 和 622Mbps 几种不同的传输速率。由于 ATM 没有共享介质或包传递带来的延时，因此非常适合音频和视频数据的传输。但是 ATM 需要专门的软硬件，部署成本相对比较高。

由于各种原因，城域网的特有技术并没能在世界各国迅速地推广。相反，在实践中人们通常使用广域网的技术去构建与城域网目标、范围相当的网络。

3. 广域网(WAN)

广域网也称远程网(Wide Area Network)，所覆盖的范围比城域网（MAN）更广，可以跨越城市、地区、国家，甚至洲际，地理范围可从几百公里到几千公里。广域网通常以连接不同地域的大型主机系统或局域网为主要目的。由于距离较远，信息衰减比较严重，所以这种网络一般是要租用专线或者是自行铺设专线（例如使用光纤、双绞线、同轴电缆、微波、卫星、红外以及激光等）。因为所连接的用户多，总带宽有限，所以用户的终端连接速率一般较低，通常为 9.6Kbps～45Mbps。比较典型的广域网应用如中国移动的网络运营系统(包括计费系统、信息系统、综合结算系统和综合账务系统等)。

4. 互联网(Internet)

互联网又称为“因特网”，是世界上最大的计算机网络。互联网通过使用统一的协议（TCP/IP）将全球成千上万的计算机网络（广域网与广域网之间、广域网与局域网之间、局域网与局域网之间）连接起来，使得各网络之间可以交换信息、共享资源。由于互联网由全球范围内的计算机网络构成，对于互联网普通用户而言，Internet 拥有不计其数的网络资源，用户可以随时从 Internet 上获得所需的信息。

综上所述，各种计算机网络参数比较如表 10-1 所示。

表 10-1 局域网/城域网/广域网/互联网参数比较

网络类型	缩写	数据传输率	覆盖范围	典型应用
局域网	LAN	4M～10G	<10km	校园、楼宇
城域网	MAN	50Kbps～100Mbps	10~100km	城市
广域网	WAN	9.6Kbps～45Mbps	100~1000km	城市、国家、洲
互联网	Internet	9.6Kbps～45Mbps	无限制	全球互联

10.2.2　按拓扑结构

网络拓扑结构指网络中各个节点相互连接的方式，主要有星型拓扑结构、总线拓扑结构、、环型拓扑结构和混合型拓扑结构。

1. 星型拓扑结构

星型拓扑是目前在局域网中应用得最为普遍的一种结构。由于在该种网络结构中，各个网络节点通过点对点方式连接到中央节点上，整体呈现出星状分布状态，因此被称为星型拓扑结构，如图 10.1 所示。星型拓扑结构中的某一普通网络节点出现故障不会波及其他节点，但是一旦中心节点（通常由 Hub 或交换机组成）出现问题，其所在网络将陷入瘫痪。

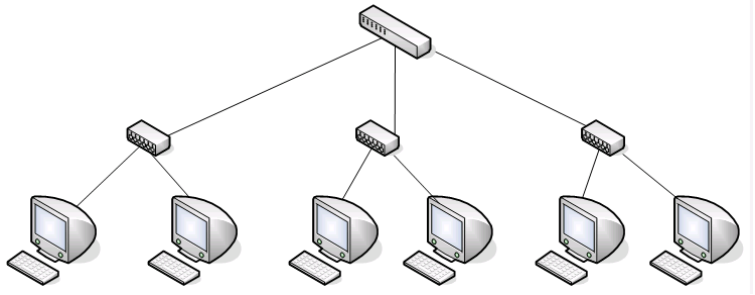

图 10.1 星型网络拓扑结构图

星型拓扑结构主要应用于 IEEE 802.2、IEEE 802.3 标准以太局域网中，目前用的最多的传输介质是双绞线，如常见的五类线、超五类双绞线等。

星型拓扑结构具有容易实现、易扩展、维护方便、传输数据快等优点，但同时也存在设备成本高，可靠性较低，资源共享能力差等不足。

注意：该种网络出现故障时，可以先从集线器或交换机等中央节点查起。每一台计算机在集线器或交换机上都有指示灯对应。如果是 10Mbps、100Mbps 自适应设备，则适应 10Mbps 连接时亮黄色灯，适应 100Mbps 连接时亮绿色灯，无连接时，灯不亮。

2. 总线拓扑结构

总线拓扑结构采用一根公用总线作为传输介质 ，所有设备都直接与总线相连，其结构如图 10.2 所示。总线上的信息多以基带形式串行传递，其传递方向总是从发送信息的节点开始向两端扩散，因此采用总线拓扑结构的网络又称为广播式计算机网络。

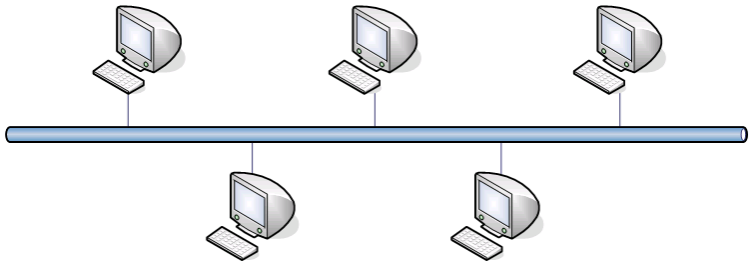

图 10.2 总线型网络拓扑结构图

在总线拓扑结构中，所有的工作站和服务器都连接到总线上，无中心节点，各个节点的地位是平等的。由于各节点是共用总线带宽的，所以在传输速度上会随着接入网络的节点的增多而下降。单个节点失效不影响整个网络的正常通信。但是如果总线出现故障，则整个网络或者相关主干网段就会瘫痪。

总线拓扑结构具有组网费用低、可靠性高、易扩展（但所能连接的节点数量有限）等优点，但是由于是共享总线，一次仅能允许一个节点发送数据，其他节点必须等待总线空闲后才能发送，因此存在数据传输率较低、总线负担过重等问题。而且该种类型的网络一旦发生连接错误，维护和检测都很不方便。

总线所采用的物理介质一般为同轴电缆（包括粗缆和细缆），少数也使用光纤。

3. 环型拓扑结构

环型拓扑一般仅适用于 IEEE 802.5 的令牌网（Token ring network）。在这种网络结构中所有节点首尾相接，连接成一个闭环，整个网络发送的信息就是在这个环中传递，如图 10.3 所示。网络中的节点若想发送信息，必须获得“令牌”，"令牌"会在环型连接中依次传递。

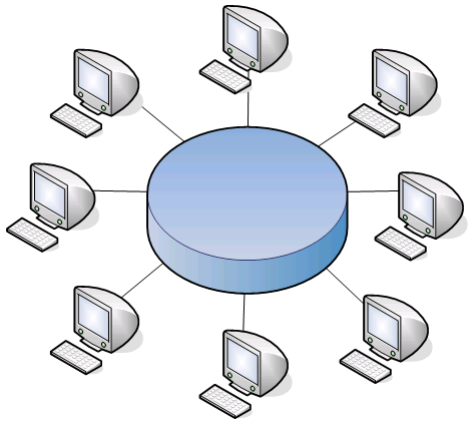

图 10.3 环型网络拓扑结构图

在环型拓扑中传送的数据要经过每个节点，如果有一个节点出现故障，将会造成整个网络的瘫痪。同时对故障节点的定位较难，维护起来非常不便。

环路上各节点都是自举控制，因而控制软件简单，但环路必须闭合才能正常工作，使得该网络不便于扩充。

令牌环一般由同轴电缆或光纤组成。

4. 混合型拓扑结构

混合型拓扑结构从星型结构和总线型结构演变而来，兼具星型结构和总线型结构的特点，是一种综合布线方式，如图 10.4 所示。

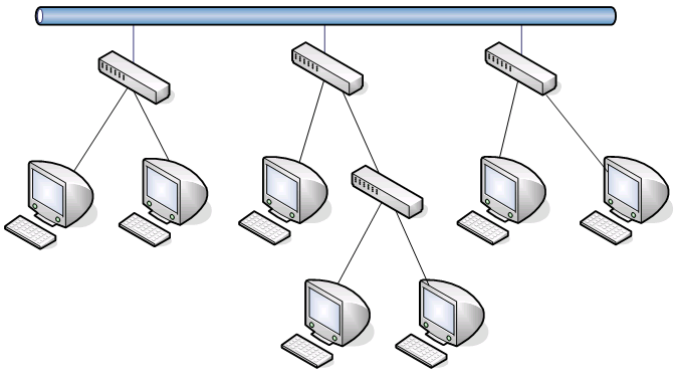

图 10.4 混合型网络拓扑结构图

混合拓扑结构更能满足较大网络的扩展需求，既突破了星型网络在传输距离上的局限，又解决了总

线型网络在连接节点数量上的限制。但是混合拓扑由于继承了总线型网络拓扑结构的特点，同样会存在较难维护的问题。

10.3　网络体系结构

计算机网络的体系结构是指该网络及其子系统所能完成功能的精确定义，通常采用层次结构进行描述。OSI/RM 以及 TCP/IP 是目前两个主要的参考模型。

10.3.1　OSI/RM 参考模型

OSI/RM（开放系统互连参考模型）是 ISO（Internation Standards Organization）在网络通信方面所定义的，用于连接异种计算机的开放协议标准。基于这个开放的模型，各网络设备厂商就可以遵照共同的标准来开发网络产品，最终实现彼此兼容。

整个 OSI/RM 模型共分 7 层，从下往上共依次为：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，如图 10.5 所示。

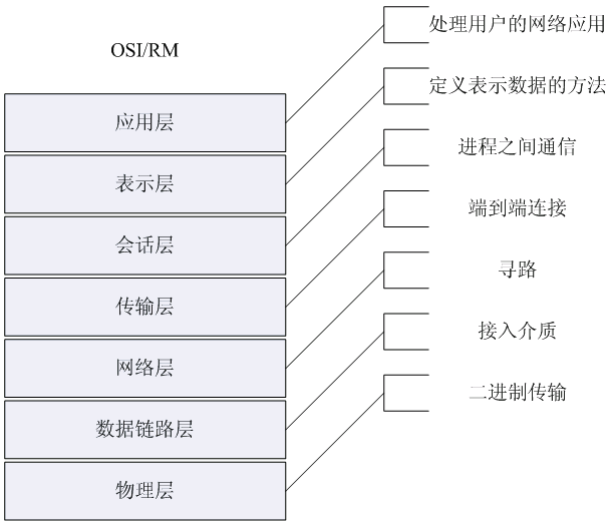

图 10.5 OSI/RM 参考模型

其中相邻层之间可以通信，第 1 层到第 3 层属于通信子网的范畴，第 5 到第 7 层属于资源子网的功能范畴，第 4 层是中间层，连接上下 3 层。当接受数据时，数据是自下而上传输；当发送数据时，数据是自上而下传输。虽然这种通信流程垂直通过各层次，但每一层都在逻辑上能够直接与远程计算机系统的相应层直接通信。为构建这种层次间的逻辑连接，需要发送端在每一层都要在数据报文前增加报文头。该报文头只能被远程计算机的相应层识别和使用。接收端接收到数据报文后会删去报文头，每一层都删去该层负责的报文头，最后将数据传递给相关的应用程序，其过程如图 10.6 所示。

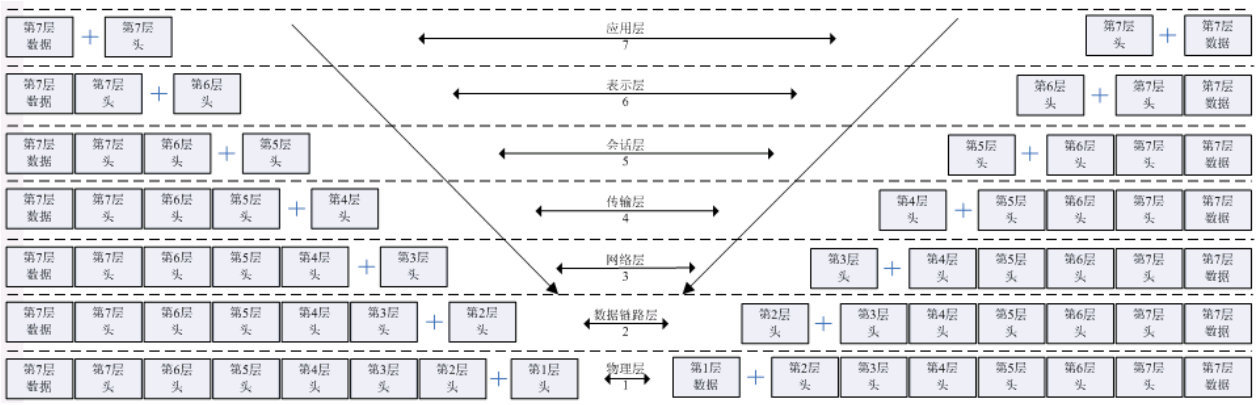

图 10.6 OSI/RM 层间通信原理

各层功能如下：

（1）物理层

物理层位于整个 OSI 参考模型的最低层，其主要任务就是为上一层的数据链路层提供一个物理连接，透明地传送比特流。物理层建立在物理介质上，提供机械和电气接口，包括电缆、物理端口以及附属设备。物理层提供的服务包括：物理连接、物理服务数据单元顺序化（接收物理实体收到的比特顺序，与发送物理实体所发送的比特顺序相同）和数据电路标识。

（2）数据链路层

数据链路层是建立在物理传输能力的基础上，用于在两个相邻节点间的链路上无差错地传送以帧（Frame）为单位的数据。

数据链路层的主要任务就是进行数据封装和数据链接的建立。封装的数据信息由 4 部分组成，其中地址段含有发送节点和接收节点的地址，控制段用来表示数格连接帧的类型，数据段包含实际要传输的数据，差错控制段用来检测传输中出现的帧错误。

数据链路层可使用的协议有 SLIP、PPP、X25 和帧中继等。常见的集线器和低档的交换机以及 Modem 之类的拨号设备都是工作在这个层次上。工作在这个层次上的交换机通常称“第二层交换机”。

数据链路层的功能包括：数据链路连接的建立与释放、构成数据链路数据单元、数据链路连接的分裂、定界与同步、顺序和流量控制、差错的检测和恢复等。

（3）网络层

网络层属于 OSI 中的第 3 层，解决的是网际的通信问题，即选择合适的路由和交换节点，透明地向目的节点交付发送节点所发送的分组。网络层的主要功能是寻路，即选择到达目标主机的最佳路径，并沿该路径传送数据包。

除此之外，网络层还具有流量控制和拥挤控制的功能。现在较高档的交换机也可直接工作在这个层次上，由于该层具备路由功能且属于第 3 层，通常称为“第三层交换机”。

网络层的功能包括：建立和拆除网络连接、路径选择和中继、网络连接多路复用、分段和组块、服务选择和传输以及流量控制。

（4）传输层

传输层在网络两个节点之间建立端到端的通信信道，主要解决的是数据在网络之间的传输质量问题。传输层提供两端点之间可靠、透明的数据传输，执行端到端的差错控制、顺序控制和流量控制，管理多路复用和解复用。传输层是计算机通信体系结构中关键的一层，主要涉及的是网络传输协议，如 TCP 协议。

传输层的功能包括：映像传输地址到网络地址、多路复用与分割、传输连接的建立与释放、分段与

重新组装、组块与分块。

（5）会话层

会话层提供面向通信的逻辑用户接口。会话可能是一个用户通过网络登录到一个主机，或一个正在建立的用于传输文件的连接。

会话层的功能主要有：会话连接到传输连接的映射、数据传送、会话连接的恢复和释放、会话管理、令牌管理和活动管理。

（6）表示层

表示层主要解决用户信息的语法表示问题，如用于文本文件的 ASCII 和 EBCDIC 表示形式。如果通信双方用不同的数据表示方法，彼此之间就不能互相理解。表示层就是用于屏蔽这种不同之处。表示层的功能主要有：数据语法转换、语法表示、表示连接管理、数据加密和数据压缩。

（7）应用层

应用层是 OSI 参考模型的最高层，直接面对用户的具体应用。应用层包含用户应用程序执行通信任务所需要的协议和功能，如电子邮件和文件传输等应用。

在 7 层网络中，第 1、2 层处理网络信道问题；每 3、4 层处理传输服务问题；每 5、6、7 层处理应用服务问题。

10.3.2　TCP/IP 参考模型

与 OSI 参考模型不同，TCP /IP 模型更侧重于互联设备间的数据传送，而不是严格的功能层次划分，因而为协议的具体实现留下很大的余地。一般而言，OSI 参考模型比较适合于解释互联网络通信机制，而 TCP /IP 是互联网络协议事实上的标准。从体系结构角度看，TCP/IP 参考模型分为 4 层：网络接口层、网络层、传输层和应用层。其层次结构及与 OSI 参考模型的对应关系如图 10.7 所示。

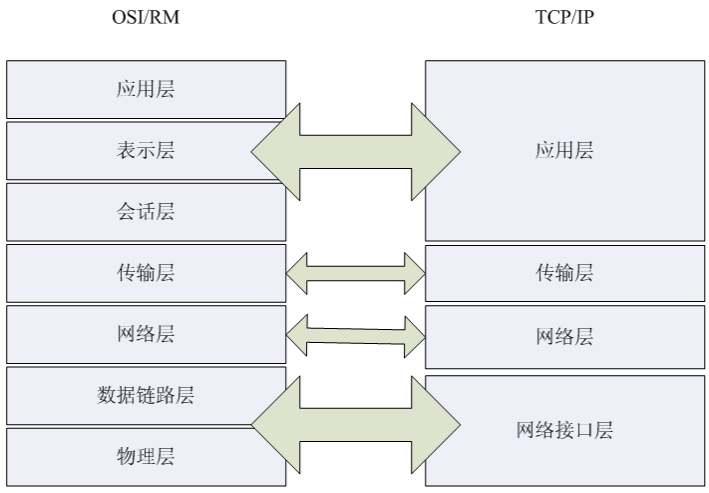

图 10.7 TCP/IP 与 OSI/RM 对应关系

可以看到，TCP/IP模型中的应用层在功能上与OSI/RM模型的最上面3层相当，网络接口层与OSI/RM模型的最下面2层相当。TCP/IP参考模型是在TCP/IP协议出现很久以后才发展起来的，由于其更强调功能分布而不是严格的功能层次的划分，因此比OSI/RM模型更灵活。TCP/IP各层含义及功能如下所述。

（1）网络接口层(Network Interface Layer)。

TCP/IP 模型将与物理网络相关的部分称为网络接口层，与 OSI/RM 的物理层和数据链路层相对应。负责接收上层递交来的数据报，并把该数据报发送到指定的网络上，同时负责接收来自网络的数据报，

并传递给上层。

网络接口层也称为 TCP/IP 链路层，与 Ethernet（以太网）、Token Ring（令牌环网）以及 ATM（异步传输模式）等网络接入技术密切相关。各种网络接入技术说明如表 10-2 所示，其中 Ethernet 技术近年得到了充发的发展和广泛的应用。

（2）网络层(Internet Layer)。

TCP/IP 模型中的网络层对应于 OSI/RM 的网络层，用于解决互联网中计算机到计算机的通信问题。与网络层密切相关的是 IP 协议，即 Internet Poctocol（网际协议）。网络层把来自传输层的报文分组封装在 IP 数据报(Datagram)中，然后按路由选择算法将数据报发送到相应的网络接口。与此同时，网络层还要接受下层递交过来的数据包，校验数据报的有效性，删除报头，使用路由选择算法确定该数据报应该由本地处理，还是转发出去。

在网络层还有一个重要的协议——ICMP（Internet Control Message Protocol），即网际控制报文协议。该协议与 ping 命令联合使用，可以查看当前计算机节点与本地网络上的其他节点的连通性。

（3）传输层(Transport Layer)

TCP/IP 模型中的传输层对应于 OSI/RM 的传输层，其任务是提供应用程序之间端到端(End-to-End)的通信。传输层将要发送的报文或数据流分成更小的段，即报文分组(Packet)，然后把每个报文分组连同报文目的地址一并递交给网络层。与此同时，传输层也接收来自下层的报文分组，重组成完整的报文或数据流。传输层对数据流具有一定的调节作用，确保其完整、正确，并按顺序递交。

TCP/IP模型中的传输层主要包括TCP(Transmission Control Protocol, 即传输控制协议)和UDP（User Datagram Protocol，用户数据报协议）两个协议。1974年，在ARPAnet诞生后的短短5年里，Vinton Cerf和Robert Kahn发明了TCP。TCP在IP之上提供了一个可靠的，连接式的协议，可以提供了比其他协议更多的保护。TCP要求在提供相应服务前必须先建立连接（三次握手机制），因此TCP也被称为面向连接的协议（Connection-oriented）。而UDP数据包传输基于尽力递交，没有差错修正、重传、重新排序等机制，无需先建立连接，因此UDP也称为无连接协议（Connectionless）。

（4）应用层

TCP/IP 将 OSI/RM 的传输层之上的所有层统称为应用层。在应用层，用户调用访问网络的应用程序，应用程序与传输层协议相配合，用以发送和接收用户所需的数据。

TCP/IP 应用层协议比较多，常见的有 HTTP、FTP、POP3 等。每个应用层协议通常会使用一些指定的端口（端口类似于电视机中的频道，将应用程序指定到正确的端口，就可以接收和发送与该端口相关的数据，TCP/IP 有 65536 个可用端口）。一些特定用途的端口由 Internet Assigned Numbers Authority（www.iana.org）分配，如 HTTP 使用 80，FTP 使用 21 以及 POP3 使用 110。表 10-3 列举了几个主要的 TCP/IP 应用层协议及其相关端口。

表 10-2 主要网络接入技术说明

类型	说明
Ethernet	标准以太网，遵守IEEE802.3标准。最早由Xerox（施乐）公司创建，在1980年由DEC、Intel和Xerox三家公司联合制定的标准。采用CSMA/CD（带有冲突检测的载波侦听多路访问）访问控制方法，理论最高可达10Mb/s。以太网主要有两种传输介质：双绞线和同轴电缆。
Fast Ethernet	快速以太网，遵守IEEE802.3u标准，理论最高可达100Mb/s，传输介质要求5类或5类以上的电览。
GB Ethernet	千兆以太网，遵守IEEE802.3z标准，理论最高可达1000Mb/s，传输介质一般采用光纤。
10GB Ethernet	10G以太网，理论最高可达10000Mb/s，目前还处于研发阶段，还没有得到实质应用。
Token Ring	令牌环网，IBM公司于70年代创建，遵守IEEE802.5标准.。数据传输速度为4Mbps或16Mbps，新型的快速令牌环网速度可达100Mbps。令牌环网的传输方法在物理上采用了星形拓扑结构，但逻辑上仍是环形拓扑结构。由于只有具有令牌的计算机才被允许传递数据，因此比Ethernet效率更高。
FDDI	FDDI的英文全称为“Fiber Distributed Data Interface”，即“光纤分布式数据接口”，使用基于IEEE802.5令牌环标准的令牌传递MAC协议。可提供多达100Mb/s的数据传输速度，支持长达2KM的多模光纤，

	最多可容纳1000个节点。
ATM	ATM的英文全称为“Asynchronous Transfer Mode”，即“异步传输模式”。ATM是一种信元交换技术（使用53字节固定长度的信元进行交换），由于没有共享介质或包传递带来的延时，非常适合音频和视频数据的传输。ATM具有不同的速率，分别为25、51、155、622Mbps，从而为不同的应用提供不同的速率。
PPP	PPP的英文全称为“ Point-to-Point Protocol”，即点对点协议。PPP由IETF（Internet Engineering Task Force）定义，用于取代串行IP（Series Line Internet Potocol，SLIP），支持多种协议，有错误检测和链路管理功能。目前利用PPP通过调制解调器接入Internet，仍是最为普遍的方法。
WLAN	WLAN英文全称为“Wirrless Local Area Network”，即无线局域网。WLAN遵守802.11系列标准，该系列共分4个标准，分别为：802.11b、802.11a、802.11g和802.11z。其中802.11b传输速度为11MB/s，802.11a标准的连接速度可达54MB/s。802.11g兼容802.11b与802.11a两种标准的。802.11z专门加强了无线局域网安全。

表 10-3 主要的TCP/IP应用层协议

协议	端口	说明
FTP	21	实现文件传输的基本协议，利用FTP协议可以把本地文件上传到网络上的另一台计算机上（FTP服务器），也可从网络上（FTP服务器）下载所需的文件。目前有许多软件站点就是通过FTP协议来为用户提供下载服务的。
HTTP	80	用于网页的超文件链接协议（Hypertest Transfer Protocol）。
HTTPS	443	Secure HTTP
SSH	22	Secure Shell，加密计算机之间的通信，是Telnet的安全性版本。
Telnet	23	Telnet用明文方式建立计算机之间的通信连接，可以登录到远程计算机上，并进行信息访问，包括读取所需的数据库、进行联机游戏、建立对话服务以及访问电子公告牌，但只能进行些字符类操作和会话。
SMTP	25	Simple Network Management Protocol，用于发送电子邮件，负责邮件的发送、分拣和存储。
POP3	110	用于接收电子邮件的Post Office Protocol，负责将邮件通过SLIP/PPP协议连接下载到用户计算机上。
SNMP	161	用于网络管理的Simple network Management protocol。
IPP	631	Internet Print Protocol，与Common Unix Print System（CUPS）相关。
SWAT	901	Samba服务的Web管理工具。
NFS	2049	用于Linux/UNIX计算机之间文件的共享。
IMAP	143	使用Internet消息访问协议的邮件阅读器。

在/etc/services 文件中列出了 Red Hat Enterprise Linux 5 中所使用的 TCP/IP 应用层协议的完整列表，其中包括服务的名称、关联的端口号以及相关说明，如下所示：

```
#vi /etc/services
...  ...
# 21 is registered to ftp, but also used by fsp
ftp              21/tcp
ftp              21/udp          fsp fspd
ssh               22/tcp                          # SSH Remote Login Protocol
ssh               22/udp                           # SSH Remote Login Protocol
telnet           23/tcp
telnet           23/udp
# 24 - private mail system
lmtp              24/tcp                          # LMTP Mail Delivery
lmtp              24/udp                           # LMTP Mail Delivery
smtp              25/tcp           mail
smtp              25/udp           mail
...  ...
```

10.4　网络配置基本内容

在 Linux 主机上，通过对网络基本内容的配置，可以将计算机连接到网络上，实现与其他计算机之间的通信。网络配置通常涉及主机名、IP 地址、子网掩码、网关地址、域名服务器地址等内容。

10.4.1　主机名

主机名用于在网络上标识一台计算机的名称，通常该主机名在网络中是唯一的。

10.4.2　IP 地址

发送到 Intetnet 上的数据之所以够找到目的计算机，是因为任何一个连接到 Intemet 上的计算机都有一个惟一的网络地址。为了确保 Intemet 上的每一个网络地址始终是惟一的，国际网络信息中心（NIC）会根据网络的大小为每一个申请者统一分配 IP 地址。

IP 地址分为 IPv4 和 IPv6 两个版本。IPv4 由于设计上的局限，目前除了美国外，各国都出现 IP 地址短缺现象。IPv6 所要解决的主要是 IPv4 协议中 IP 地址远远不够的现象。

IPv4 使用点分十进制数来描述地址，共 32 位长，由 4 个分段的十进制数组成。例如，用二进制描述的 32 位地址如下：

```
01111110100010000000000010010111 1
```

为了方便阅读，通常将32位地址进行分组，每8位为一组：

```
01111110100010000000000010010111 1
```

最后，将每个8位数据转换成十进制，并用小数点隔开。IPv4点分十进制描述的地址如下：

```
126 . 136 . 1 . 47
```

与记忆二进制位串（如0 1 1 1 1 1 1 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 1 1 1 1）相比，记忆IP地址126 . 136 . 1 . 47更加容易。

IPv6 采用冒分十六进制来描述地址，共 128 位，由 8 个分段的十六进制数组成。例如：

```
FEDC : BA98 : 7654 : 3210 : FEDC : BA98 : 7654 : 3210
```

个别字段中前面的0可以不写，但是每段必须至少有一位数字。

当IPv4和IPv6节点混用时，可以采用另一种表示形式：

```
x : x : x : x : x : x : d . d . d . d
```

其中x是地址中6个高阶16位段的十六进制值，d是地址中4个低价8位段的十进制值(标准IPv4表示)。例如：

```
0 : 0 : 0 : 0 : 0 : 0 : 1 3 . 1 . 6 8 . 3
0 : 0 : 0 : 0 : 0 : F F F F : 1 2 9 . 1 4 4 . 5 2 . 3 8
```

也可以写成压缩格式：

```
: : 1 3 . 1 . 6 8 . 3
: : F F F F . 1 2 9 . 1 4 4 . 5 2 . 3 8
```

IPv4 地址由网络号（网络 ID）和主机号（主机 ID）两部分构成。如上所述，可以将 IPv4 地址划分为 4 个分段的十进制数，如图 10.8 所示。

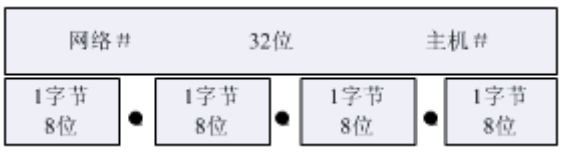

图 10.8 IPv4 地址划分

按照 IPv4 协议规定，互联网上的 IPv4 地址共有 A、B、C、D、E 五类。下面主要介绍 IPv4 地址分类。

（1）A 类 IP 地址

A 类地址是最大的地址组，用前面 8 位来标识网络号（其中规定最前面一位为“0”），其余 24 位标识主机地址，如下所示：

```
0nnnnnnnhhhhhhhhhhhhhhhhhhhhhhh
```

其中字母“n”表示网络号位，字母“h”表示主机号位。可以看到 A 类地址的第一段取值（也即网络号）可以是“00000001～01111111”之间任一数字，转换为十进制后即为 1～126 之间。其余各段合在一起表示主机号。由于主机号没有做硬性规定，所以 A 类 IP 地址范围为“1.0.0.0～128.255.255.255”，其中 127.0.0.1 专门用于回环主机地址，127.0.0.0 专门用于回环网络，10.0.0.0～10.255.255.254 是内部网络地址。

A 类地址主要针对大型政府网络，全世界总共只有 126 个可用的 A 类网络，每个 A 类网络最多可以连接多达 16777214 台计算机。下面是一些 A 类地址网络号：

```
10 . 0 . 0 . 0
44 . 0 . 0 . 0
101 . 0 . 0 . 0
120 . 0 . 0 . 0
```

（2）B 类 IP 地址

B 类地址用前面 16 位来标识网络号，其中最前面两位规定为“10”，其余 16 位标识主机号，如下所示：

```
10nnnnnnnnnnnnnnhhhhhhhhhhhhhhh
```

可以看到 B 类地址的第一段取值“10000000～10111111”，转换成十进制后即为 128～191 之间。第一段、第二段合在一起表示网络号，第三段、第四段合在一起标识网络上的主机号。由于主机号没有做硬性规定，所以 B 类地址的范围为“128.0.0.0～191.255.255.255”， 其中 172.16.0.0～172.31.255.254 地址段专门用于内部网络。

B 类地址适用于中等规模的网络，全世界大约有 16000 个 B 类网络，每个 B 类网络最多可以连接 65534 台计算机。

下面是一些 B 类地址网络号：

```
137 . 55 . 0 . 0
129 . 33 . 0 . 0
190 . 254 . 0 . 0
150 . 0 . 0 . 0
168 . 30 . 0 . 0
```

（3）C 类 IP 地址

C 类地址用前面 24 位来标识网络号（其中最前面三位规定为“110”），其余 8 位标识主机号，如下所示：

```
110nnnnnnnnnnnnnnnnnnnnnhhhhhhhh
```

可以看到 C 类地址的第一段取值为“11000000～11011111”之间，转换成十进制后即为 192～223。第一段、第二段、第三段合在一起表示网络号，第四段标识网络上的主机号。由于主机号没有做硬性规定，所以 C 类地址范围为“192.0.0.0～223.255.255.255”， 其中 192.168.0.0～192.168.255.255 为内部专用地址段。

C 类地址适用于教室、机房等小型网络，每个 C 类网络最多可以有 254 台计算机。这类地址是所有

的地址类型中地址数最多的，但这类网络所允许连接的计算机数也是最少的。下面是一些 C 类网络号：

```
204 . 238 . 7 . 0
192 . 153 . 186 . 0
199 . 0 . 44 . . 0
191 . 0 . 0 . 0
```

222 . 222 . 31 . 0

（4）D 类 IP 地址：

D 类地址用于多重广播组，一个多重广播组可能包括 1 台或多台主机，也可能没有主机。D 类地址的最高位为“1110”，如下所示：

```
1 1 1 0 n n n n n n n n n n n n n n n n n n n n h h h h h h h h
```

其中第一段取值为“11100000～11101111”，转换成十进制即为 224～239，其余各位用于设定客户机参加的特定组，取值址范围为“224.0.1.1～239.255.255.255”。在多重广播操作中没有网络或主机位，数据包将传送到网络中选定的主机子集中，只有注册了多重广播地址的主机才能接收到数据包。

（5）E 类地址

E 类地址是实验性地址，保留作为以后使用。E 类地址的最高位为“1111”，第一段取值“11110000～11110111”，转换成十进制即为 240～247。248～254 暂无规定。

A 类、B 类、C 类网络地址结构组成如图 10.9 所示。

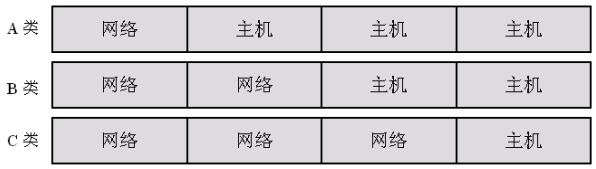

图 10.9 A 类、B 类、C 类网络地址结构

A 类、B 类、C 类网络地址特点如表 10-4 所示。

表 10-4 A类、B类、C类网络地址特点

类别	网络标识位	网络位数	主机位数	网络数	地址数
A	0	8	24	126	16777214
B	10	16	16	16384	65534
C	110	24	8	2097152	254

10.4.3　子网与子网掩码(subnet mask)

子网掩码主要用于标明子网是如何划分的，即地址的哪一部分是包含子网的网络号，哪一部分是网络中的主机号。掩码与 IP 地址一样，由 32 位组成，用点分十进制来描述。缺省情况下，掩码包含两个域：网络域和主机域，分别对应网络号和主机号。

通常将 IP 地址的网络位号全改为“1”，将主机位号全改为“0”，即为该 IP 地址的子网掩码。例如将 IP 地址为“192.168.57.128”的网络位号“192.168.57”全改为“1”，将主机位号“57”全改为“0”，可得该 IP 地址的子网掩码为“255.255.255.0”。

A 类、B 类、C 类地址的标准子网掩码分别为：A 类为 255.0.0.0；B 类为 255.255.0.0；C 类为 255.255.255.0。例如某 IP 地址为“172.16.56.45”，由于首字段为“172”，属于 B 类地址“128～191”范围内，所以该 IP 地址为 B 类地址，由此可推得其子网掩码为“255.255.0.0”，与“172.16.56.45”进行逻辑与运算，可得该地址所在网络的网络号为“172.16”。

利用子网掩码和 IP 地址，也可以计算 IP 地址所对应的网络号。例如已知某 IP 地址为“10.1.1.182”，子网掩码为“255.0.0.0”，则通过将“10.1.1.182”和“255.0.0.0”进行逻辑与运算，可得该 IP 地址的网络号为“10”。

10.4.4　广播地址(broadcast address)

广播地址使用户能将消息一次性传递到自己所在网络的全体成员中。广播地址设定规则为：主机部分被设置为 255(二进制位为全 1)，网络部分保持不变。例如，某 IP 地址为 192.68.56.6，其中“192.168.56”表示网络地址，占用了前 24 位，后 8 位是主机地址。将后 8 位全部设置为 1 就可以得到其广播地址为“192.168.56.255”。

10.4.5　网关地址(gateway)

主机的 IP 地址设置正确后可以和同网段的其他主机进行通信，但还不能与不同网段的外网主机进行通信。为了与外部网络进行通信，需要正确设置网关地址。

网关通常是提供外部网络连接的路由器，一般至少有两个网络接口：一个连接局域网，另一个提供外网连接。

对于需要连接外部网络的主机，需要正确设置本地局域网内至少一个网关的 IP 地址，任何不同网段主机间进行的通信都将通过网关进行。

10.4.6　域名服务器地址(DNS)

仅仅正确设置了 IP 地址和网关地址，只能保证用户通过 IP 地址和其他主机进行通信。为了能够使用更为简易的主机域名进行通信，需要指定至少一个 DNS 服务器的 IP 地址。所有的域名解析任务都会通过指定的 DNS 服务器来完成。

实际上，DNS 服务器上存放着主机 IP 地址与其主机域名之间的对应关系。DNS 服务器收到域名解析请求之后，就将域名解析为 IP 地址，然后反馈回去。使用域名将大大减轻用户记忆的负担。例如，访问北京理工大学，就可以输入如下地址：http://www.bit.edu.cn。

10.4.7　DHCP 服务器

网络中的每一台计算机都拥有惟一 IP 地址。主机的 IP 地址可分为静态地址和动态地址两类。静态地址一般由用户手工设定（指定 IP 地址、子网掩码等），设定成功后永久生效。为了保证正常的网络通信，静态地址的设定通常需要咨询网络管理员。动态地址则由用户指定的 DHCP 服务器负责自动分配。用户每次接入网络时，由 DHCP 服务器从其地址池中动态选择一个没被使用的 IP 地址分配给用户临时使用。当用户退出网络时（关机或断开网络连接），所使用的 IP 地址会被释放，由 DHCP 服务器重新分配。

注意：DHCP 是动态主机分配协议，主要用于简化主机 IP 地址的分配和管理。用户可以利用 DHCP 服务器管理动态分配的 IP 地址及其他相关的网络配置，如 DNS、WINS 等。

10.5　配置以太网连接

以太网（Ethernet）是目前使用最为广泛的计算机网络之一。与 Windows 中设置网络连接类似，在 Red Hat Enterprise Linux 5 中配置以太网连接需要正确设置 IP 地址、子网掩码、网关、DNS 等信息。

10.5.1　添加以太网连接

在 Red Hat Enterprise Linux 5 的安装过程中，如果用户没有对以太网连接进行配置，或安装完毕后又添加了新的以太网网卡，就需要用户添加以太网连接。

（1）单击面板中的【系统】菜单，选择【管理】子菜单，然后选择【网络】选项，打开【网络配置】窗口，如图 10.10 所示。

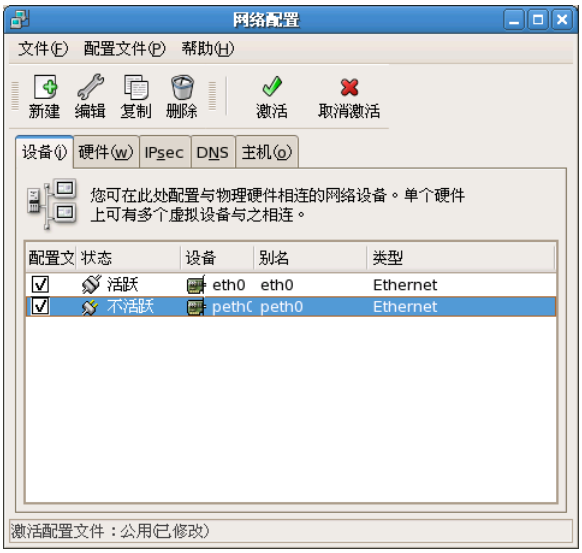

图 10.10【网络配置】窗口

（2）保持【设备】选项卡处于选择状态，在工具栏中单击【添加】，打开【添加新设备类型】对话框，如图 10.11 所示。其中列出了可选的设备类型，包括以太网连接、ISDN 连接、调制解调器连接、令牌环连接、无线连接以及 xDSL 连接。

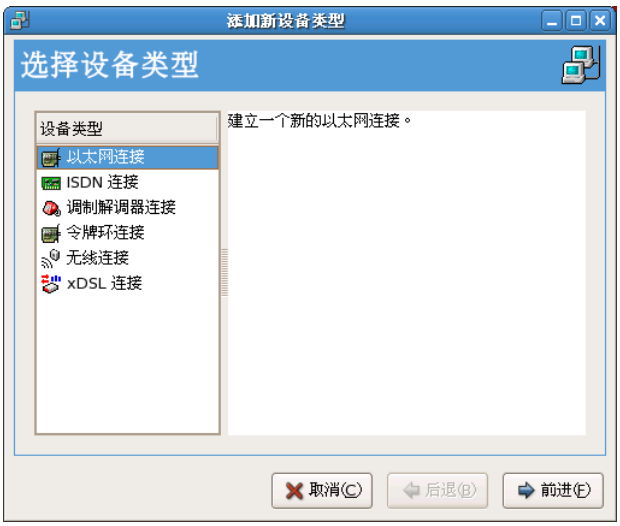

图 10.11 选择添加新设备类型

（3）选择【以太网连接】，单击【前进】按钮，在弹出的【选择以太网设备】对话框中，系统列出了目前识别的所有以太网网卡，选择需要添加的以太网网卡，如图 10.12 所示。

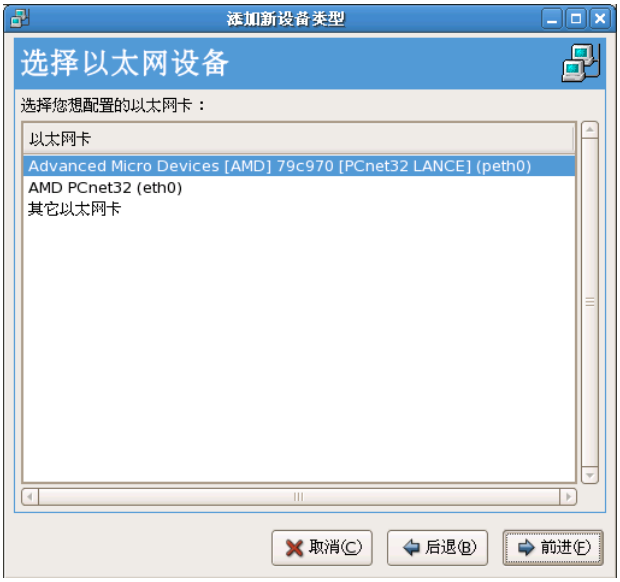

图 10.12 选择添加的网卡

（4）如果硬件列表中没有所需要的以太网设备，可以选择【其它以太网卡】选项来添加硬件设备。选择【其它以太网卡】，单击【前进】按钮，系统弹出【选择以太网适配器】对话框，如图 10.13 所示。

图 10.13 添加新的网卡设备

（5）在【适配器】下拉列表框中选择以太网卡的制造商和型号。如果该网卡是系统的第一块网卡，在【设备】下拉列表框中选择【eth0】，如果是第二块网卡，选择【eth1】，依此类推。单击【前进】按钮，打开【配置网络设备】对话框中，如图 10.14 所示。

图 10.14 配置网络

（6）如果网络内存在一台 DHCP 服务器，可以设置【自动获取 IP 地址设置使用】为“dhcp”；如果用户手工配置网络，选择【静态设置的 IP 地址】选项，然后输入 IP 地址、子网掩码、默认网关地址。设置完毕后，单击【前进】按钮，完成新设备的添加。

（7）新添加的以太网设备需要激活才能正常工作。选择需要激活的以太网设备，单击图 10.10 中工具栏中的【激活】按钮。如果设备被正确激活，在列表框状态栏中可以看到设备状态为“活跃”。

10.5.2　修改网络配置

（1）如果用户需要修改网络配置，单击面板中的【系统】菜单，选择【管理】子菜单，然后选择【网络】选项，打开如图 10.10 所示的【网络配置】窗口。在列表框中选择需要修改的网络设备，单击工具栏中的【编辑】按钮，弹出【以太网设备】对话框，如图 10.15 所示。

图 10.15 修改网络配置

（2）在【常规】选项卡，用户可以重新编辑网卡的 IP 地址、子网掩码、网关地址等选项。单击【路由】标签，打开【路由】选项卡，如图 10.16 所示。

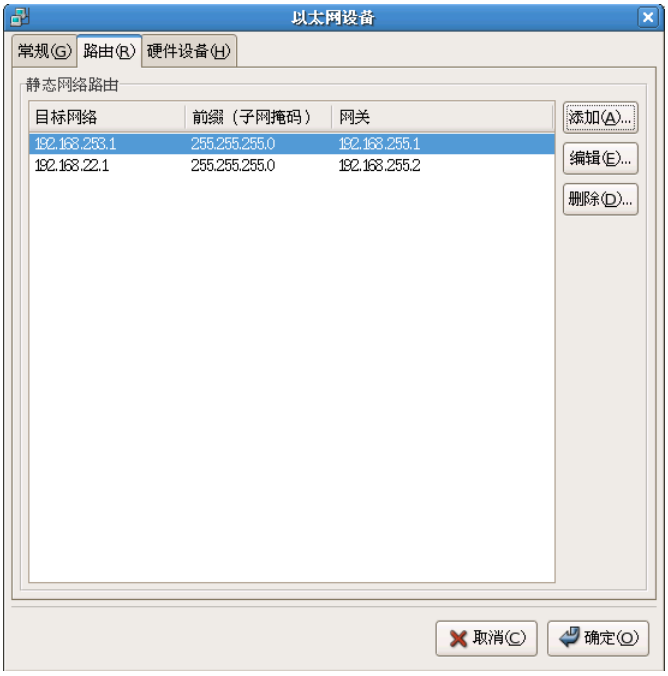

图 10.16 添加路由

（3）在【路由】选项卡中，可以添加、编辑、删除静态网络路由。静态网络路由需要设置目标网络的网络地址，子网掩码以及所需经过的网关。

10.5.3　使用配置文件

通常一个物理硬件设备可以与多个逻辑网络设备相对应。例如，如果系统上已经安装了一块以太网卡（eth0），可以使用不同的别名、不同的配置项来配置一个或多个逻辑网络设备，这些设备都和 eth0 相关联。如果用户需要在不同的网络环境中使用同一台计算机，只需为其在不同的网络环境中设置使用不同的逻辑网络设备。切换使用的逻辑网络设备即可实现网络配置的更改。

例如分别需要在家中和公司中使用同一台笔记本电脑，但家中网络使用的是静态 IP 地址，而公司使用的是 DHCP，那么就可以配置两个逻辑网络设备，分别用于家庭和公司。

每个逻辑设备是通过配置文件来进行设置的。配置文件记录了逻辑设备的所有配置项。通过【网络配置】窗口的【配置文件】菜单，可以对配置文件进行创建、复制、删除等操作，如图 10.17 所示。

图 10.17 配置文件菜单

新建一个配置文件按如下步骤操作：

（1）在图 10.17 中选择【配置文件】菜单，选择【新建】，系统弹出如图 10.18 所示的【新配置文件】对话框。

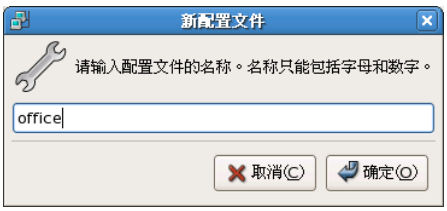

图 10.18 创建新的配置文件

（2）输入新配置文件的名称，然后单击【确定】按钮，返回【网络配置】主窗口。在菜单栏单击【配置文件】菜单，可以看新添加的配置文件已经出现菜单底部。从主窗口底部的状态栏也可以看出，

当前正在工作的配置文件为 office。

修改一个配置文件按如下步骤操作：

（1）在如图 10.17 所示的【网络配置】窗口中选择【配置文件】菜单，选择需要修改的配置文件，例如“defaultCopy0”.

（2）单击【配置文件】菜单中的【属性】选项，在弹出的【新配置文件】对话框里输入需要修改的配置文件的新名称。

如果在【配置文件】菜单中选择【复制】，系统会对当配置文件，例如“defaultCopy0”，进行复制，副本取名为“defaultCopy0Copy0”并添加到【配置文件】菜单中。如果在【配置文件】菜单中选择【删除】，会对当前使用的配置文件（defaultCopy0）进行删除，如图 10.19 所示。

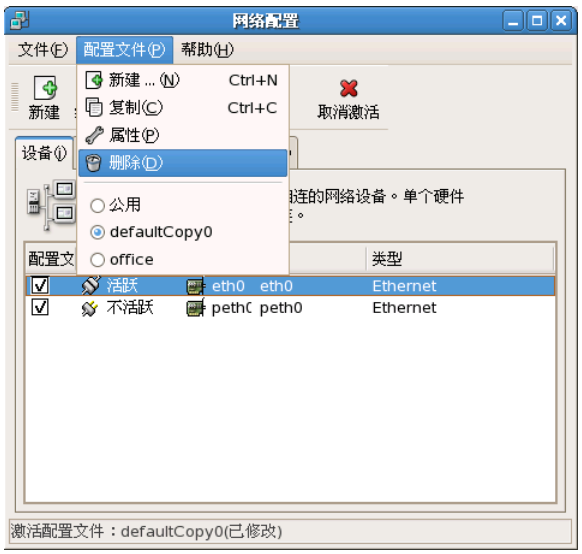

图 10.19 删除配置文件

106　连接 Internet

如今，互联网已经成为人们日常生活中不可缺少的工具。在 Red Hat Enterprise Linux 5 中提供了多种接入互联网的方法，其中包括：

- 使用调制解调器建立连接
- 使用 xDSL 建立连接
- 使用 ISND 建立连接
- 使用无线建立连接
- 使用以太网建立连接

10.6.1　使用 modem 拨号上网

现在仍有很多人，包括一些小企业仍然在使用 modem 和电话线连接到互联网。modem 通常接在计算机的串中上（如 COM1、COM2），然后接到电话线插口中。

在拨号上网之前需要申请一个互联网服务提供商（ISP）的账号，然后用户可以使用 modem 向互联

网服务提供商拨号，拨号成功后即连接到互联网上。拨号上网最常使用的是点对点协议（PPP）。

在 Red Hat Enterprise Linux 5 中可以使用两种方法实现拨号上网。一种是通过系统自带的配置向导，另一种是通过 KPPP 应用程序。

1. 通过配置向导建立拨号连接

（1）在面板【系统】菜单中选择【管理】，然后选择【网络】，打开如图 10.10 所示的【网络配置】窗口，单击【添加】按钮，系统将弹出【添加新设备类型】对话框，在【选择设备类型】列表中选择【调制解调器连接】，如图 10.20 所示。

图 10.20 选择建立【调制解调器连接】

（2）单击【前进】按钮，系统会开始自动检测调制解调器，检测可能会花费一段时间。如果未能自动识别，系统将弹出【选择调制解调器】对话框，如图 10.21 所示。

图 10.21 选择调制解调器

（3）在【选择调制解调器】对话框中可以对所使用的调制解调器进行选择，可以设定波特率和流程控制以及是否有拨号音等选项。单击【前进】按钮，系统将打开【选择提供商】对话框，如图 10.22 所示。

图 10.22 选择提供商

（4）在该对话框中，输入网络提供商所提供的电话号码以及登录名和口令。在【提供商名称】文本框中输入网络提供商的名称，单击【前进】按钮，将弹出【IP 设置】对话框，如图 10.23 所示。

图 10.23 设置播号网络 IP

（5）在【IP 设置】窗口中，根据网络提供商所提供的信息选择是自动获取 IP 还是手工设置静态 IP。单击【前进】按钮，将弹出【建立拨号连接】对话框，单击【应用】按钮就可以完成调制解调器的设置。系统返回到【网络配置】主窗口，可以看到新添加了一个 modem 类型的设备，如图 10.24。

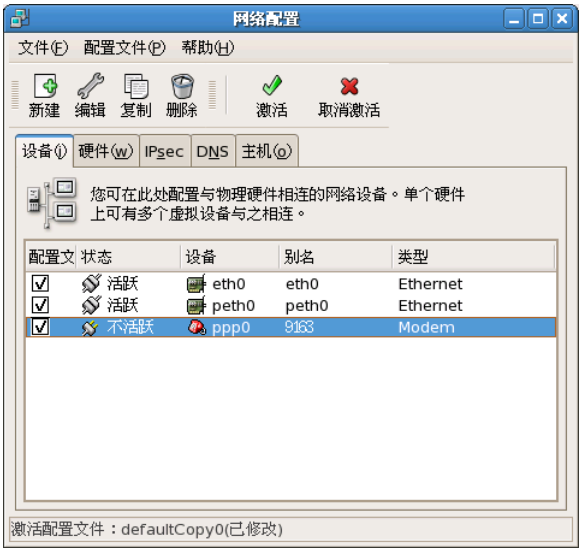

图 10.24 添加了 modem 类型的设备

（6）新添加的 modem 并没有处于工作状态，单击工具栏中的【激活】按钮，尝试将其激活。

2. 使用 KPPP 拨号上网

KPPP 用于拨号，是 pppd 的拨号前端。用户可以通过 KPPP 设置拨号网络，并通过拨号连接到提供网络服务的 ISP。除了用于拨号，KPPP 还具有拨号监视、通信费用记录、拨号终端调试等功能。在 Red Hat Enterprise Linux 5 中，系统默认安装了 KPPP 程序。

（1）在命令行输入“kppp”命令来启动 KPPP 程序，也可以在面板【应用程序】菜单中选择【Internet】子菜单，然后选择【KPPP】选项来启动 KPPP 程序，如图 10.25 所示。

图 10.25 KPPP 主界面

（2）如果用户已经设置拨号网络，只需在【连接到】下拉列表框中选择接入的 ISP，输入登录账号和密码，单击【连接】按钮即可进行拨号。如果用户没有设置任何拨号网络，单击【配置】按钮，系统将弹出 KPPP 配置对话框，如图 10.26 所示。

图 10.26【KPPP 配置】对话框

（3）在【KPPP 配置】对话框中选择【账户】选项卡，如果还没有建立账户，列表框中显示为空。单击【新建】按钮，创建一个新的账户，系统会弹出【创建新账户】提示，如图 10.27 所示。

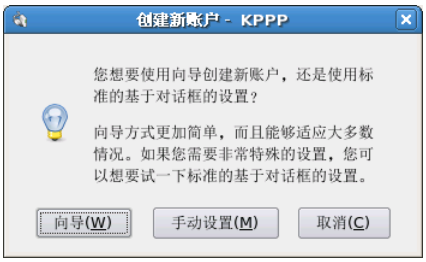

图 10.27 选择向导或手动方式创建账户

（4）如果选择【向导】方式建立新账户会比较简单，适用于大多数情况，但由于向导方式的 ISP 列表没有将中国大陆包括在内，所以只能选择【手动设置】。单击【手动设置】按钮，弹出如图 10.28 所示的【新建账户】对话框。其中【链接名称】用于输入所建链接的名称标识，单击【电话号码】列表框右侧的【添加】按钮，添加拨出的电话号码。认证方式通常是【PAP/CHAP】，有些 ISP 会要求采用脚本或终端方式。

图 10.28【新建账户】对话框

（5）单击【IP】标签，切换到【IP】选项卡，如图 10.29 所示。在【IP】选项卡中根据 ISP 的要求，选择动态或静态 IP。选择静态 IP 需按 ISP 的要求输入正确的 IP 地址和子网掩码。

图 10.29【IP】选项卡

（6）单击【网关】标签，切换到【网关】选项卡，如图 10.30 所示。在【网关】选项卡中选择默认网关，并且选中【将默认路由指派给此网关】。如果 ISP 提供有指定的静态网关，需按要求输入静态网关的 IP 地址。

图 10.30【网关】选项卡

（7）单击【DNS】标签，切换到【DNS】选项卡，如图 10.31 所示。在【DNS】选项卡中，选择【自动】，则连接建立后，会使用系统自动分配的 DNS 服务器。如果 ISP 提供有指定的 DNS，需按要求选择【手工】，然后输入 DNS 的 IP 地址。

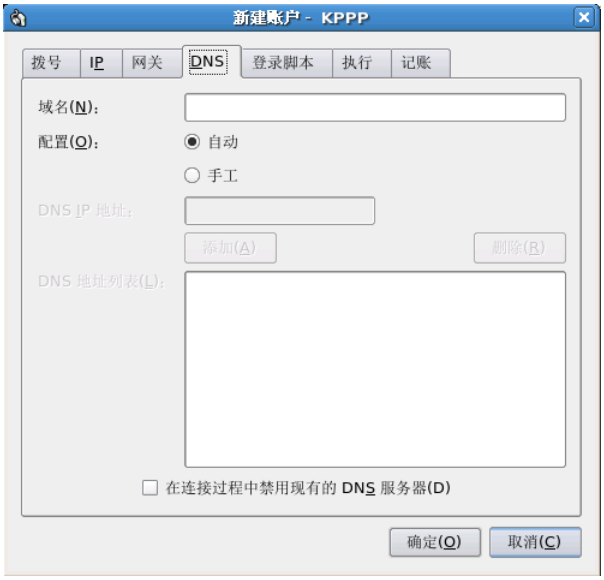

图 10.31【DNS】选项卡

（8）在图 10.31 中，单击【确定】按钮，返回【KKK 配置】对话框，选择【调制解调器】选项卡，如图 10.32 所示。

图 10.32【调制解调器】选项卡

（9）如果系统没有设置过调制解调器，则列表框为空，可以通过【新建】按钮，进行创建。单击【新建】按钮，弹出如图 10.33 所示的【新建调制解调器】对话框。

图 10.33 新建调制解调器

（10）在【新建调制解调器】对话框中，设置调制解调器的名称，调制解调器使用的设备文件，选择流控、行结束符以及连接速度等。单击【确定】按钮，返回【KPPP 配置】对话框。

（11）在图 10.26 所示的【KPPP 配置】对话框中选择【图表】选项卡，可以设置是否【启用流量图表】，对输入输出流量进行统计，同时还可以设置背景、文本、输入字节、输出字节所使用的颜色，如图 10.34 所示。

图 10.34【图表】选项卡

（12）在图 10.26 所示的在【KPPP 配置】对话框中选择【杂项】选项卡，可以设置 pppd 超时时间、断线后是否自动重拨、是否在断开时退出 KPPP 等选项，如图 10.35 所示。

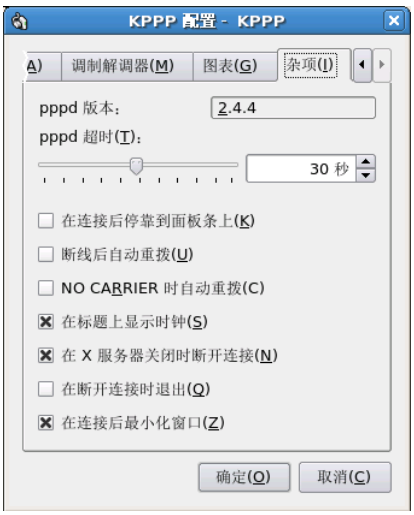

图 10.35【杂项】选项卡

（13）设置好账号后，就可以在如图 10.25 所示的 KPPP 主界面中输入用户名、密码进行拨号连接。

10.6.3　使用 xDSL 拨号上网

xDSL（Digital Subscriber Line，数字用户线路）可以通过电话线实现高速传输。xDSL 种类很多，包括 ADSL（非对称，下载比上传快），IDSL（远程 ISDN 线路）和 SDSL（对称，下载与上传同速）等，其中用户使用比较多的是 ADSL。使用 ADSL 拨号上网时，需要 ADSL 调制解调器（通常由 ISP 提供），同时还需要一个 ISP 账号和密码。

（1）选择面板中的【系统】菜单，选择【管理】，然后单击【网络】，打开如图 10.10 所示的【网络配置】窗口。单击【添加】按钮，在弹出的【选择设备类型】对话框中，选择【xDSL 连接】选项，如图 10.36 所示。

图 10.36 添加 xDSL 连接

（2）单击【前进】按钮，打开【配置 DSL 连接】对话框，如图 10.37 所示。

图 10.37 配置 ADSL 连接

（3）在【配置 DSL 连接】对话框中，选择该账号使用的以太网设备，根据 ISP 提供的信息，输入 ISP 名称和账号的用户名及密码。单击【前进】按钮，弹出【建立 DSL 连接】对话框，单击【应用】按钮完成配置。

（4）ADSL 连接配置完成后，可以在【网络配置】窗口的列表框中看到“xDSL”设备，如图 10.38 所示。新添加的 xDSL 设备并没有处于工作状态，单击工具栏中的【激活】按钮，尝试将其激活。

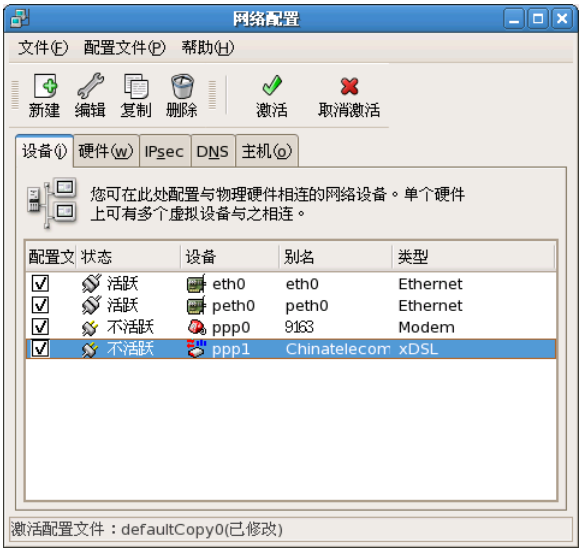

图 10.38 添加 xDSL 设备

10.6.4　使用 ISDN 拨号上网

ISDN（Integrated Services Digital Network，综合业务数字网）是一种国际标准，为用户入网提供了端到端的数字链接。ISDN 使用电话载波线路进行拨号连接，在程控数字交换机内采用了数字交换技术，在交换机之间采用了数字中继，但在入网接口上仍然采用模拟话音信号进行传输。ISDN 能够支持包括数据、文字、语音、图像（小于 2.048Mb/s）在内的各种综合业务。使用 ISDN 拨号上网时，需要 ISDN 适配器（通常由 ISP 提供），同时还需要一个 ISP 账号和密码。

（1）打开面板中的【系统】菜单，选择【管理】子菜单，然后单击【网络】选项，打开如图 10.10 所示的【网络配置】窗口。单击【添加】按钮，在弹出的【选择设备类型】对话框中，选择【ISDN 连接】选项，如图 10.39 所示。

图 10.39 添加 ISDN 连接

（2）单击【前进】按钮，打开【选择 ISDN 适配器】对话框，如图 10.40 所示。在【选择 ISDN 适配器】对话框中可以对所使用的 ISDN 适配器进行配置，默认使用【Euro ISDN】通道协议。

图 10.40 选择 ISDN 适配器

（3）单击【前进】按钮，系统将打开【选择提供商】对话框，如图 10.41 所示。在该对话框中，输入 ISND 网络提供商所提供的电话号码以及登录名和口令。在【提供商名称】文本框中输入网络提供商的名称。

图 10.41 选择提供商

（4）单击【前进】按钮，将弹出【IP 设置】对话框，如图 10.42 所示。在【IP 设置】窗口中，【封装模式】选择“同步 PPP”，根据网络提供商所提供的信息选择是自动获取 IP 还是手工设置静态 IP。

图 10.42 IP 设置

（5）单击【前进】按钮，将弹出【建立 ISDN 连接】对话框，单击【应用】按钮完成 ISDN 的设置。系统返回到【网络配置】主窗口，可以看到新添加了一个 ISDN 类型的设备，如图 10.43 所示。

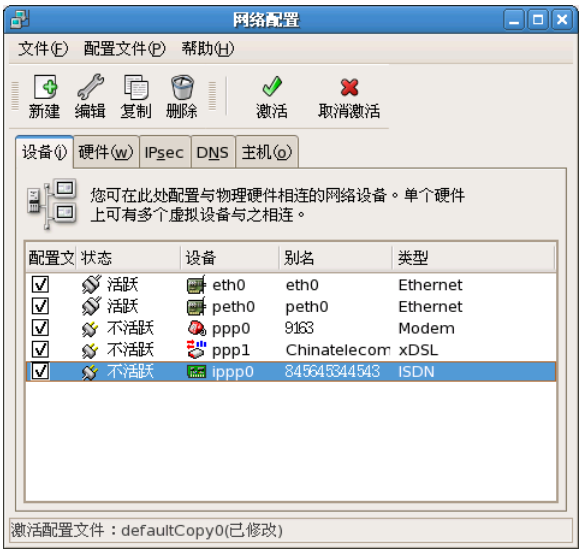

图 10.43 添加 ISDN 设备

（6）新添加的 ISDN 并没有处于工作状态，单击工具栏中的【激活】按钮，尝试将其激活。

10.6.5　使用无线连接

如果要把计算机连接到一个 WAP（Wireless Access Point，无线访问点）或一个对等无线网络，需要对计算机中的无线网络设备进行配置。

（1）打开面板中的【系统】菜单，选择【管理】子菜单，然后单击【网络】选项，打开如图 10.10 所示的【网络配置】窗口。单击【添加】按钮，在弹出的【选择设备类型】对话框中，选择【无线连接】，如图 10.44 所示。

图 10.44 选择无线连接

（2）单击【前进】按钮，打开【选择无线连接】对话框，如图 10.45 所示，其中列出了所有系统已识别的无线网络设备。

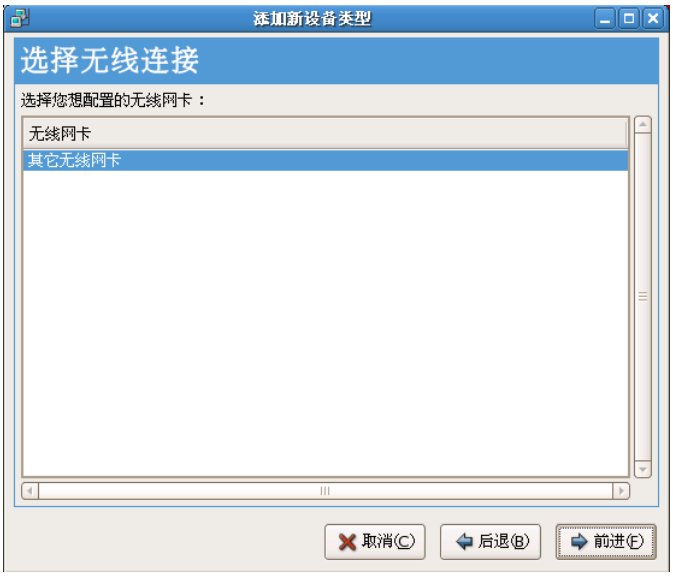

图 10.45 选择无线连接

（3）如果在【选择无线连接】对话框没有所需的设备，在图 10.45 中选择【其它无线网卡】，单击【前进】按钮，打开【选择以太网适配器】对话框。在【适配器】下拉列表框中，选择安装的无线网卡设备，继续单击【前进】按钮，将打开【配置无线连接】对话框，如图 10.46 所示。

图 10.46 配置无线连接

（4）在【配置无线连接】对话框中，可以指定无线网络的名称（SSID）、通道、传输率以及密钥。单击【前进】按钮，将打开【配置网络设置】对话框。在【配置网络设置】对话框中，设置 IP 获得的方式（手工设定或是 DHCP）。单击【前进】按钮，将弹出【建立无线连接】对话框，单击【应用】按钮就可以完成无线网络的设置。系统返回到【网络配置】主窗口，可以看到新添加了一个“Wireless”类型的设备，如图 10.47 所示。

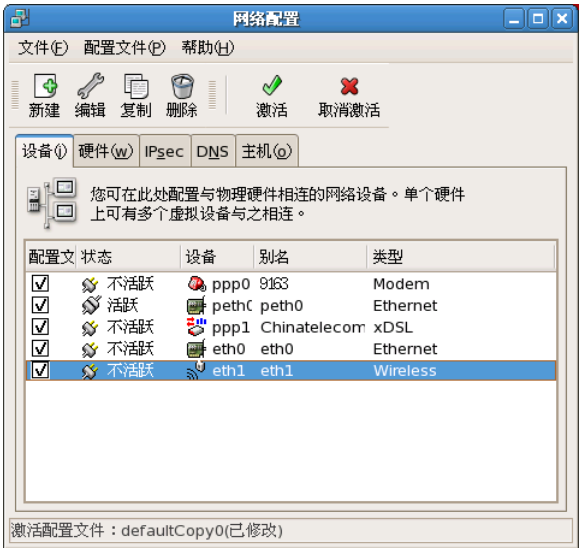

图 10.47 添加无线网络设备

（5）新添加的无线网络设备并没有处于工作状态，单击工具栏中的【激活】按钮，尝试将其激活。

10.7　网络管理常用命令及应用实例

在 Red Hat Enterprise Linux 5 中提供了大量的网络管理命令，利用这些命令可以对网络进行快速配

置，也可以协助诊断网络故障。

10.7.1　hostname 命令

hostname 命令用于显示和更改系统的主机名，命令格式为：

```
hostname　[主机名]
```

直接使用 hostname 命令将显示当前系统的主机名称，例如：

```
# hostname
localhost
```

可以使用 hostname 命令修改当前系统的主机名称，例如：

```
# hostname　rhel5
# hostname
rhel5
```

10.7.2　ifconfig 命令

ifconfig 命令类似于 Windows 下的 ipconfig，用于获取和修改网络接口配置信息。

1. ifconfig 命令的一般格式

ifconfig 命令格式为：

```
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
          [add <address>[/<prefixlen>]]
          [del <address>[/<prefixlen>]]
          [[-]broadcast [<address>]]　[[-]pointopoint [<address>]]
          [netmask <address>]　[dstaddr <address>]　[tunnel <address>]
          [outfill <NN>] [keepalive <NN>]
        [hw <HW> <address>]　[metric <NN>]　[mtu <NN>]
        [[-]trailers]　[[-]arp]　[[-]allmulti]
        [multicast]　[[-]promisc]
        [mem_start <NN>]　[io_addr <NN>]　[irq <NN>]　[media <type>]
        [txqueuelen <NN>]
        [[-]dynamic]
        [up|down] ...
```

ifconfig 命令可以指定许多选项，主要选项说明如表 10-5 所示。

表 10-5 ifconfig命令主要选项说明

选项	说明
-a	显示所有接口信息，包括活动和非活动的。
-v	以冗余模式显示详细信息。
-s	以短列表格式显示接口信息，每个接口只显示一行摘要数据。
up	激活一个不活动的接口。
down	与up相反，关闭一个接口。
netmask [地址]	为一个指定接口设置网络掩码。
broadcast [地址]	为一个指定接口设置广播地址。
[地址]	设置指定接口的IP地址。
[接口]	显示一个指定接口的信息。

2. 显示已激活的网络接口信息

例如不带任何选项使用 ifconfig 命令，可以显示当前系统中活动的网卡信息，命令行为：

```
# ifconfig
eth0        Link encap:Ethernet  HWaddr 00:0C:29:A5:0E:30
            inet addr:192.168.255.128  Bcast:192.168.255.255  Mask:255.255.255.0
            inet6 addr: fe80::20c:29ff:fea5:e30/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:2060 errors:0 dropped:0 overruns:0 frame:0
            TX packets:794 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:222787 (217.5 KiB)  TX bytes:151286 (147.7 KiB)
            Interrupt:16 Base address:0x2000

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:4467 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4467 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6309541 (6.0 MiB)  TX bytes:6309541 (6.0 MiB)
```

3. 显示所有网络接口信息

使用“ifconfig　-a”命令可以显示系统中所有网卡的信息，包括活动和非活动。例如：

```
# ifconfig  -a
eth0        Link encap:Ethernet  HWaddr 00:0C:29:A5:0E:30
            inet addr:192.168.255.128  Bcast:192.168.255.255  Mask:255.255.255.0
            inet6 addr: fe80::20c:29ff:fea5:e30/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:2060 errors:0 dropped:0 overruns:0 frame:0
            TX packets:794 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:222787 (217.5 KiB)  TX bytes:151286 (147.7 KiB)
            Interrupt:16 Base address:0x2000

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:4467 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4467 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6309541 (6.0 MiB)  TX bytes:6309541 (6.0 MiB)

peth0       Link encap:Ethernet  HWaddr FE:FF:FF:FF:FF:FF
            BROADCAST MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:0 (0.0 b)  TX bytes:9312 (9.0 KiB)
...  ...
```

4. 显示指定的网络接口信息

使用“ifconfig [接口]”命令可以显示指定接口的信息（无论该接口是否处于活动状态），例如显示回环网络接口信息，命令行为：

```
# ifconfig  lo
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:4467 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4467 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6309541 (6.0 MiB)  TX bytes:6309541 (6.0 MiB)
```

5. 关闭与激活指定的网络接口

使用“ifconfig down [接口]”命令关闭指定接口，例如关闭本地回环网络接口，命令行为：

```
# ifconfig  lo  down
# ifconfig  lo                    // 查看 lo 是否已处于关闭状态
lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            LOOPBACK  MTU:16436  Metric:1
            RX packets:4467 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4467 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6309541 (6.0 MiB)  TX bytes:6309541 (6.0 MiB)
//lo 已处于非活动状态
```

与之相反，使用“ifconfig up [接口]”命令可以启动指定接口，例如启动本地回环网络接口，命令行为：

```
# ifconfig  lo  up
```

6. 设定指定网络接口的 IP 地址

使用“ifconfig [接口] IP 地址”命令可以指定接口的 IP 地址，例如指定 eth0 的 IP 地址为 192.168.254.128，命令行为：

```
# ifconfig  eth0  192.168.254.128
# ifconfig   eth0
eth0        Link encap:Ethernet  HWaddr 00:0C:29:A5:0E:30
            inet addr:192.168.254.128  Bcast:192.168.255.255  Mask:255.255.255.0
            inet6 addr: fe80::20c:29ff:fea5:e30/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:2084 errors:0 dropped:0 overruns:0 frame:0
            TX packets:800 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:224895 (219.6 KiB)  TX bytes:151818 (148.2 KiB)
            Interrupt:16 Base address:0x2000
```

例如使用 ifconfig 命令配置一台安装 3 块网卡的主机，第 1 块网卡连接网络 192.168.214.0，第 2 块网卡连接网络 192.168.202.0，第 3 块网卡连接网络 192.168.200.0，则 3 块网卡的配置命令为：

```
ifconfig eth0  192.168.214.0  broadcast  192.168.214.255  netmask  255.255.255.0
ifconfig eth1  192.168.202.0  broadcast  192.168.202.255  netmask  255.255.255.0
ifconfig eth2  192.168.200.0  broadcast  192.168.200.255  netmask  255.255.255.0
```

10.7.3　ifup 命令

ifup 命令用于启动指定的非活动网卡，与“ifconfig　up”命令相似，例如启动本地回环网络接口，命令行为：

```
#ifup   lo
# ifconfig lo                          // 查看 lo 是否已处于关闭状态
lo          Link encap:Local Loopback
            inet addr:127.0.0.1   Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING   MTU:16436   Metric:1
            RX packets:4467 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4467 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6309541 (6.0 MiB)   TX bytes:6309541 (6.0 MiB)
//lo 已处于活动状态
```

10.7.4　ifdown 命令

ifdown 命令用于关闭指定的活动网卡，与“ifconfig　down”命令相似，例如关闭本地回环网络接口，命令行为：

```
# ifdown   lo
# ifconfig   lo                        // 查看 lo 是否已处于关闭状态
lo          Link encap:Local Loopback
            inet addr:127.0.0.1   Mask:255.0.0.0
            LOOPBACK   MTU:16436   Metric:1
            RX packets:4467 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4467 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6309541 (6.0 MiB)   TX bytes:6309541 (6.0 MiB)
//lo 已处于非活动状态
```

10.7.5　route 命令

route 命令用于显示和动态修改系统当前的路由表。

1. route 命令的一般格式

route 命令的格式为：

```
route      [-CFvnee]
           [-v]   [-A   family]   add [-net|-host] target [netmask Nm] [gw Gw]
           [metric N] [mss M] [window W]   [irtt   I]   [reject]   [mod]   [dyn]
           [reinstate] [[dev] If]
           [-v]   [-A   family]   del [-net|-host] target [gw Gw] [netmask Nm]
           [metric N] [[dev] If]
           [-V] [--version] [-h] [--help]
```

2. 显示当前路由信息

不带任何选项直接使用 route 命令，可以显示系统当前的路由信息，例如：

```
# route
```

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use   Iface
192.168.255.0   *               255.255.255.0   U       0       0       0     eth0
default         192.168.255.254 0.0.0.0         UG      0       0       0     eth0
```

3. 添加和删除路由信息

使用“route add ”和“route del”命令可以在当前路由表中添加或删除路由信息，例如：

```
//显示当前系统的路由表信息
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use   Iface
192.168.255.0   *               255.255.255.0   U       0       0       0     eth0
172.16.0.0      *               255.255.0.0     U       0       0       0     eth0
default         192.168.255.254 0.0.0.0         UG      0       0       0     eth0
```

使用“route del”命令删除 172.16.0.0 网络的路由信息，命令行为：

```
# route  del  -net 172.16.0.0  netmask  255.255.0.0
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use   Iface
192.168.255.0   *               255.255.255.0   U       0       0       0     eth0
default         192.168.255.254 0.0.0.0         UG      0       0       0     eth0
//已经成功删除 172.16.0.0 网络的路由信息
```

使用“route add”命令添加 172.16.0.0 网络的路由信息，命令行为：

```
# route  add  -net 172.16.0.0  netmask  255.255.0.0
SIOCADDRT: 没有那个设备
# route  add  -net 172.16.0.0 netmask 255.255.0.0 dev eth0
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use   Iface
192.168.255.0   *               255.255.255.0   U       0       0       0     eth0
172.16.0.0      *               255.255.0.0     U       0       0       0     eth0
default         192.168.255.254 0.0.0.0         UG      0       0       0     eth0
//已经成功添加 172.16.0.0 网络的路由信息
```

4. 添加和删除默认网关

使用“route add default gw 网关 IP 地址 dev 接口”和“route del default gw 网关 IP 地址”命令可以添加和删除系统当前路由表中的默认网关信息，例如在当前路由表中添加默认网关 192.168.255.254，命令行为：

```
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use   Iface
192.168.255.0   *               255.255.255.0   U       0       0       0     eth0
172.16.0.0      *               255.255.0.0     U       0       0       0     eth0
#route  add  default  gw  192.168.255.254  dev  eth0
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use   Iface
192.168.255.0   *               255.255.255.0   U       0       0       0     eth0
172.16.0.0      *               255.255.0.0     U       0       0       0     eth0
```

```
default         192.168.255.254    0.0.0.0         UG    0      0        0 eth0
```

使用“route del default　gw”命令删除已存在的默认网关，命令行为：

```
#route  del  default  gw   192.168.255.254  dev  eth0
# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.255.0   *               255.255.255.0   U     0      0        0 eth0
172.16.0.0      *               255.255.0.0     U     0      0        0 eth0
//已经删除默认的网关
```

例如，在网络 192.168.200.0 中有一台主机，该主机有两块网卡，IP 地址分别为 192.168.200.10 和 172.16.0.111，分别连接网络 192.168.200.0 和 172.16.0.0。要在该网络的主机 192.168.200.56 中增加到达 172.16.0.0 的路由，命令行为：

```
#route  add  -net  172.16.0.0  gw  172.16.10.111  netmask  255.255.0.0  metric  1
```

10.7.6　ping 命令

ping 命令使用 ICMP 协议，主要用于测试网络的连通性。

1. ping 命令的一般格式

ping 命令的格式为：

```
ping  [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline]
      [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
      [-M mtu discovery hint] [-S sndbuf]
      [ -T timestamp option ] [ -Q tos ] [hop1 ...] destination
```

其中主要选项说明如表 10-6 所示。

表 10-6 ping命令主要选项说明

选项	说明
-c count	测试中发出的分组数。如果不指定count，ping命令会连续发送测试分组，直到按Ctrl+c强行中断该命令
-s packetsize	以字节为单位指定分组报文的大小，缺省为56字节
-b	允许ping广播地址
-i interval	指定分组发送的间隔时间，只有根用户可以指定小于0.2秒的时间间隔
-q	静默模式，只显示最后的统计信息
-S sndbuf	指定socket发送缓冲大小
-t	设置TTL（IP生存期）
-W timeout	定义等待响应的时间
-T timestamp option	设置指定的IP时间戳

例如，检测一台主机 Computer1 到另一台主机 Computer2 之间是否连通，可以在主机 Computer1 上执行下面的命令：

```
# ping  Computer2
PING Computer2.bit.edu.cn (192.168.200.2) 56(84) bytes of data.
64 bytes from Computer2.bit.edu.cn (192.168.200.2): icmp_seq=1 ttl=64 time=0.068 ms
64 bytes from Computer2.bit.edu.cn (192.168.200.2): icmp_seq=2 ttl=64 time=0.029 ms
64 bytes from Computer2.bit.edu.cn (192.168.200.2): icmp_seq=3 ttl=64 time=0.029 ms
64 bytes from Computer2.bit.edu.cn (192.168.200.2): icmp_seq=4 ttl=64 time=0.031 ms
//按“Ctrl+c”键终止 ping 命令
--- Computer2.bit.edu.cn ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.029/0.039/0.068/0.017 ms
```

发送过量的测试分组并不能很好地利用网络和系统资源，一般对于一次测试，发送 5 个分组报文已经足够。

2. 指定发送分组的数量

使用选项“-c”可以指定发送分组的数量，例如：

```
# ping  -c 5  192.168.255.128
PING 192.168.255.128 (192.168.255.128) 56(84) bytes of data.
64 bytes from 192.168.255.128: icmp_seq=1 ttl=64 time=0.192 ms
64 bytes from 192.168.255.128: icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from 192.168.255.128: icmp_seq=3 ttl=64 time=0.031 ms
64 bytes from 192.168.255.128: icmp_seq=4 ttl=64 time=0.032 ms
64 bytes from 192.168.255.128: icmp_seq=5 ttl=64 time=0.032 ms
--- 192.168.255.128 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.030/0.063/0.192/0.064 ms
```

3. 指定发送分组的大小

使用“-s”选项可以指定发送分组的大小，例如向 192.168.255.128 发送 6 个发组，每个分组大小为 6553 字节，命令行为：

```
# ping  -s  6553  -c 5  192.168.255.128
PING 192.168.255.128 (192.168.255.128) 6553(6581) bytes of data.
6561 bytes from 192.168.255.128: icmp_seq=1 ttl=64 time=1.63 ms
6561 bytes from 192.168.255.128: icmp_seq=2 ttl=64 time=0.034 ms
6561 bytes from 192.168.255.128: icmp_seq=3 ttl=64 time=0.034 ms
6561 bytes from 192.168.255.128: icmp_seq=4 ttl=64 time=0.033 ms
6561 bytes from 192.168.255.128: icmp_seq=5 ttl=64 time=0.034 ms
--- 192.168.255.128 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 5003ms
rtt min/avg/max/mdev = 0.033/0.300/1.635/0.597 ms
```

为了防止大数据包攻击，ping 命令不允许发送过大的分组，最大分组不能超过 65507 字节，例如：

```
# ping  -s  65535  192.168.255.128
Error: packet size 65535 is too large. Maximum is 65507
```

10.7.7　nslookup 命令

nslookup 命令主要用于测试 DNS 服务器是否工作正常，除此之外，还可以对域名和 IP 地址进行查询。例如查询北京理工大学网站（www.bit.edu.cn）的 IP 地址，使用 nslookup 命令如下：

```
#nslookup
//“>”是 nslookup 命令环境的提示符，输入待查询的域名 www.bit.edu.cn
> www.bit.edu.cn
Server:  dns.bj.unicomcdma.com
Address:  220.192.0.130
//以上为所使用的 DNS 服务器
Non-authoritative answer:
Name:     www.bit.edu.cn
Address:  202.204.80.38
```

```
//输入待查询的 IP 地址
> 202.204.80.38
Server:    dns.bj.unicomcdma.com
Address:   220.192.0.130
//以上为所使用的 DNS 服务器
Name:      www.bit.edu.cn.80.204.202.in-addr.arpa
Address:   202.204.80.38
//使用“exit”命令退出 nslookup 命令环境
>exit
#
```

也可以不进入 nslookup 命令交互模工，直接使用命令查询 IP 地址或域名，如下所示：

```
#nslookup   www.bit.edu.cn
Server:    dns.bj.unicomcdma.com
Address:   220.192.0.130

Non-authoritative answer:
Name:      www.bit.edu.cn
Address:   202.204.80.38
```

查询 IP 地址为 202.204.80.38 的服务器的域名，命令行为：

```
#nslookup   202.204.80.38
Server:    dns.bj.unicomcdma.com
Address:   220.192.0.130

Name:      www.bit.edu.cn.80.204.202.in-addr.arpa
Address:   202.204.80.38
```

10.7.8　arp 命令

arp 命令可以实现从 IP 地址到以太网 MAC 地址之间的转换，arp 命令的主要选项如表所示。

```
arp [-v]                [-i <if>] -d   <hostname> [pub][nopub]
arp [-vnD] [<HW>] [-i <if>] -f   [<filename>]
arp [-v]    [<HW>] [-i <if>] -s   <hostname> <hwaddr> [temp][nopub]
arp [-v]    [<HW>] [-i <if>] -s   <hostname> <hwaddr> [netmask <nm>] pub
arp [-v]    [<HW>] [-i <if>] -Ds <hostname> <if> [netmask <nm>] pub
```

arp 命令主要选项说明如表 10-7 所示。

表 10-7 arp命令主要选项说明

选项	说明
-a	以BSD默认格式显示arp表中所有记录项
-e	以Linux默认格式显示arp表中所有记录项
-s	设置一个新的arp记录项
-d	删除一个arp记录项
-i	指定网络接口
-f	从指定文件读取新的记录项
-v	冗余模式

例如查询 arp 表中的所有记录项，命令行为：

```
# arp   -a
Computer1.bit.edu.cn (192.168.255.1) at 00:50:56:C0:00:01 [ether] on eth0
Computer2.bit.edu.cn (192.168.255.5) at 00:50:DA:8C:00:46 [ether] on eth0
```

```
Computer3.bit.edu.cn (192.168.255.5) at 00:E0:D0:18:A6:C7 [ether] on eth0
```

以 Linux 默认格式显示所有的 arp 表记录项，命令行为：

```
# arp   -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.255.254          ether   00:50:56:E8:11:7E   C                     eth0
192.168.255.1            ether   00:50:56:C0:00:01   C                     eth0
```

10.7.9　netstat 命令

netstat 命令主要用于显示网络的连接状态、查询路由表、对网络接口进行统计。netstat 命令格式如下：

```
netstat [address_family_options] [--tcp|-t] [--udp|-u] [--raw|-w] [--listening|-l] [--all|-a] [--numeric|-n] [--numeric-hosts] [--numeric-ports] [--numeric-ports] [--symbolic|-N] [--extend|-e[--extend|-e]] [--timers|-o] [--program|-p] [--verbose|-v] [--continuous|-c] [delay]
```

netstat 常用选项如表 10-8 所示。

表 10-8 netstat常用选项说明

选项	说明
-r	显示核心路由表
-g	显示多播组成员信息
-c	进行动态显示，每隔1秒更新1次
-p	显示每个socket所属的进程号和程序名
-l	显示所有处于侦听模式的socket
-a	显示所有的socket，无论其是否处于侦听状态
-n	以IP地址形式（即数字格式）进行显示

例如，查看当前系统中的路由表，命令行为：

```
# netstat   -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.255.0   *               255.255.255.0   U         0 0          0 eth0
172.16.0.0      *               255.255.0.0     U         0 0          0 eth0
default         192.168.255.254 0.0.0.0         UG        0 0          0 eth0
```

例如，查看当前系统中所有处于侦听状态的 socket，命令行为：

```
# netstat   -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address         State
tcp        0      0 localhost.localdomain:2208  *:*                     LISTEN
tcp        0      0 *:sift-uft                  *:*                     LISTEN
tcp        0      0 *:netbios-ssn               *:*                     LISTEN
tcp        0      0 *:sunrpc                    *:*                     LISTEN
tcp        0      0 *:ftp                       *:*                     LISTEN
...   ...
```

10.7.10　traceroute 命令

traceroute 命令用于检测到达目的地的路由状况。traceroute 在每个 ttl 值发送 3 个分组，如果有一个发出的分组没有接收到响应，traceroute 就显示 1 个“*”，如果有响应则显示响应路由的名字和地址。

traceroute 以毫秒为单位计算分组的往返时间。

例如使用 traceroute 命令对到达 www.bit.edu.cn 的路由进行跟踪，命令行为：

```
#tracerout    -n   www.bit.ed
traceroute to www.bit.edu.cn [202.204.80.38],30 hops max, 40 byte packets
  1    220.192.0.1       352 ms    379 ms    359 ms
  2    220.192.0.20      358 ms    359 ms    339 ms
  3    220.192.0.222     332 ms    357 ms    339 ms
  4    192.168.32.2      333 ms    339 ms    359 ms
  5     *   *   *
  ...   ...
 30     *   *   *
```

可以看到，在第 5 行路由就丢失了目标，从而在每一跳只显示 3 个“*”，直接其跳数达到 30 为止。

10.7.11　利用常用命令分析局域网连通故障

当网络不通时，联合使用 ping、netstat、nslookup 以及 traceroute 命令可以进行故障的分析和诊断。一般步骤如下：

（1）使用 ping 命令测试回环地址、本机 IP 地址和网关地址

使用“ping 127.0.0.1”命令和“ping　本机 IP 地址”命令检查本机的 TCP/IP 协议是否设置正确，网卡是否正常工作。

如果 ping 回环地址正确，说明 TCP/P 协议没有问题，否则需要重新安装 TCP/IP 协议。

如果 ping 本机的 IP 地址结果正确，说明网卡配置正确，否则需对网卡的软硬件进行检查，一般分为如下两步进行：首先检查硬件，检查网卡和与之相连的交换机上的指示灯是否都亮，如果有一边不亮，说明在相应那边的设备可以有问题，也可能是网线有问题。若硬件无故障，则检测网卡驱动程序是否安装正确。首先用户需要确认其所安装的系统内核是否支持该网卡。Red Hat Enterprise Linux 5 和最近两年出品的大多数硬件是兼容的，用户可以到 Red Hat 的官方网站上（https://hardware.redhat.com/）查找最新支持的硬件列表进行兼容性确认。如果不兼容，则上网查找相应的驱动程序更新或补丁。如果系统内核支持该网卡，用户需要对驱动程序的设置做进一步的检查。通常可以先卸载驱动程序，然后再尝试重新安装。

（2）使用 netstat、nslookup、traceroute 命令检查路由、DNS 的设置

如果 ping 命令测试回环地址、本机 IP 地址以及网关地址的结果都正常，说明故障出现在网络层之上。联合使用 netstat、nslookup、traceroute 命令分别检查路由、DNS 设置是否有正确。