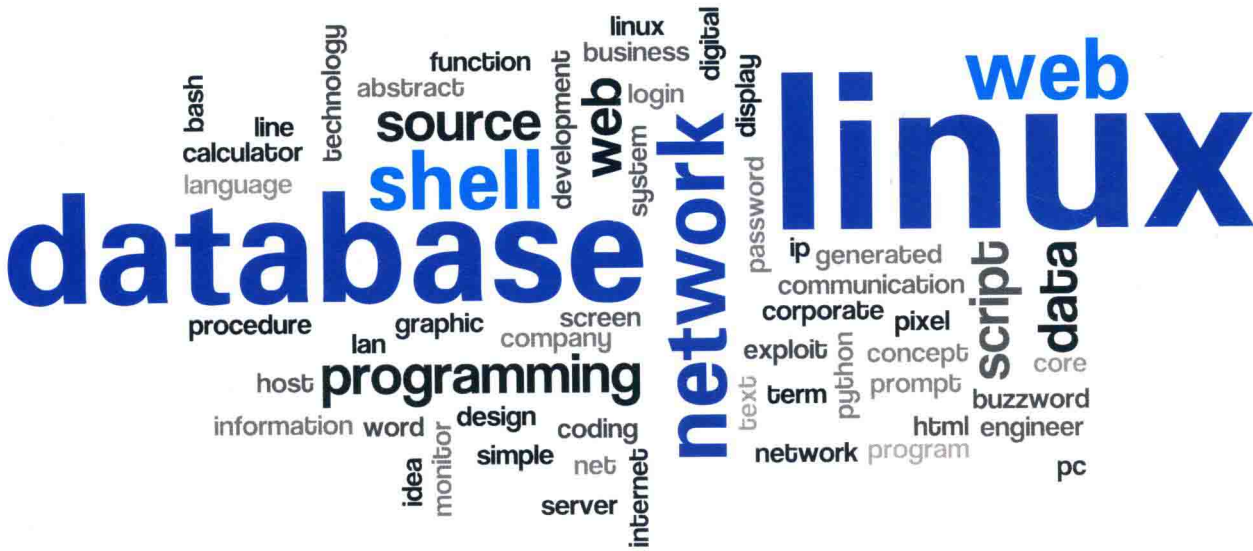
每时每课 给你新机会

课工场 kgc.cn

云计算工程师系列

北京课工场教育科技有限公司 出品



◉ 视频课程 ◉ 案例素材 ◉ 交流社区 ◉ QQ讨论组

Linux网络服务与Shell脚本攻略

主编 肖睿 江骏

中国水利水电出版社
www.waterpub.com.cn

云计算工程师系列

Linux 网络服务与 Shell 脚本攻略

主 编 肖 睿 江 骏

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

本书针对具备 Linux 基础的人群，采用案例或任务驱动的方式，由入门到精通，采用边讲解边练习的方式，使得读者在学习的过程中完成多个运维项目案例。本书分为 Linux 网络服务、Shell 脚本、Linux 防火墙三大部分。首先简单介绍了常用的服务，包括 DHCP、Samba、FTP、Postfix，然后介绍了 DNS、SSH、YUM、NFS、PXE、Cobbler 自动装机，接下来介绍了 Shell 脚本的应用，最后介绍了 Linux 防火墙原理及应用。本书内容也是学习 Linux 的必备，需要多动手多练习，为后续学习打下坚实的基础。

本书通过通俗易懂的原理及深入浅出的案例，并配以完善的学习资源和支持服务，为读者带来全方位的学习体验，包括视频教程、案例素材下载、学习交流社区、讨论组等终身学习内容，更多技术支持请访问课工场 www.kgc.cn。

图书在版编目（CIP）数据

Linux网络服务与Shell脚本攻略 / 肖睿，江骏主编
. -- 北京 : 中国水利水电出版社，2017.5
（云计算工程师系列）
ISBN 978-7-5170-5363-7

Ⅰ. ①L… Ⅱ. ①肖… ②江… Ⅲ. ①Linux操作系统
—程序设计 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2017)第094812号

策划编辑：祝智敏　责任编辑：周益丹　加工编辑：高双春　封面设计：梁　燕

书　名	云计算工程师系列 Linux网络服务与Shell脚本攻略 Linux WANGLUO FUWU YU Shell JIAOBEN GONGLÜE
作　者	主 编 肖 睿 江 骏
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座 100038） 网 址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电 话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京泽宇印刷有限公司
规　格	184mm × 260mm　16 开本　13 印张　281 千字
版　次	2017 年 5 月第 1 版　2017 年 5 月第 1 次印刷
印　数	0001—3000 册
定　价	39.00 元

丛书编委会

前　言

“互联网＋人工智能”时代，新技术的发展可谓是一日千里，云计算、大数据、物联网、区块链、虚拟现实、机器学习、深度学习等等，已经形成一波新的科技浪潮。以云计算为例，国内云计算市场的蛋糕正变得越来越诱人，以下列举了2016年以来发生的部分大事。

1．中国联通发布云计算策略，并同步发起成立“中国联通沃云＋云生态联盟”，全面开启云服务新时代。

2．内蒙古斥资500亿元欲打造亚洲最大云计算数据中心。

3．腾讯云升级为平台级战略，旨在探索云上生态，实现全面开放，构建可信赖的云生态体系。

4．百度正式发布“云计算＋大数据＋人工智能”三位一体的云战略。

5．亚马逊AWS和北京光环新网科技股份有限公司联合宣布：由光环新网负责运营的AWS中国（北京）区域在中国正式商用。

6．来自Forrester的报告认为，AWS和OpenStack是公有云和私有云事实上的标准。

7．网易正式推出“网易云”。网易将先行投入数十亿人民币，发力云计算领域。

8．金山云重磅发布“大米”云主机，这是一款专为创业者而生的性能王云主机，采用自建11线BGP全覆盖以及VPC私有网络，全方位保障数据安全。

DT时代，企业对传统IT架构的需求减弱，不少传统IT企业的技术人员，面临失业风险。全球最知名的职业社交平台LinkedIn发布报告，最受雇主青睐的十大职业技能中“云计算”名列前茅。2016年，中国企业云服务整体市场规模超500亿元，预计未来几年仍将保持约30%的年复合增长率。未来5年，整个社会对云计算人才的需求缺口将高达130万。从传统的IT工程师转型为云计算与大数据专家，已经成为一种趋势。

基于云计算这样的大环境，课工场（kgc.cn）的教研团队几年前开始策划的“云计算工程师系列”教材应运而生，它旨在帮助读者朋友快速成长为符合企业需求的、优秀的云计算工程师。这套教材是目前业界最全面、专业的云计算课程体系，能够满足企业对高级复合型人才的要求。参与本书编写的院校老师还有江骏等。

课工场是北京大学下属企业北京课工场教育科技有限公司推出的互联网教育平台，专注于互联网企业各岗位人才的培养。平台汇聚了数百位来自知名培训机构、高校的顶级名师和互联网企业的行业专家，面向大学生以及需要“充电”的在职人员，针对与互联网相关的产品设计、开发、运维、推广和运营等岗位，提供在线的直播和录播课程，并通过遍及全国的几十家线下服务中心提供现场面授以及多种形式的教学服务，并同步研发出版最新的课程教材。

除了教材之外，课工场还提供各种学习资源和支持，包括：

- 现场面授课程
- 在线直播课程
- 录播视频课程
- 授课 PPT 课件
- 案例素材下载
- 扩展资料提供
- 学习交流社区
- QQ 讨论组（技术，就业，生活）

以上资源请访问课工场网站 www.kgc.cn。

本套教材特点

（1）科学的训练模式

- 科学的课程体系。
- 创新的教学模式。
- 技能人脉，实现多方位就业。
- 随需而变，支持终身学习。

（2）企业实战项目驱动

- 覆盖企业各项业务所需的 IT 技能。
- 几十个实训项目，快速积累一线实践经验。

（3）便捷的学习体验

- 提供二维码扫描，可以观看相关视频讲解和扩展资料等知识服务。
- 课工场开辟教材配套版块，提供素材下载、学习社区等丰富的在线学习资源。

读者对象

（1）初学者：本套教材将帮助你快速进入云计算及运维开发行业，从零开始逐步成长为专业的云计算及运维开发工程师。

（2）初中级运维及运维开发者：本套教材将带你进行全面、系统的云计算及运维开发学习，逐步成长为高级云计算及运维开发工程师。

课工场出品（kgc.cn）

课程设计说明

课程目标

读者学完本书后，能够掌握 Linux 系统常用服务的原理与配置，学会使用 Shell 脚本对 Linux 系统与服务进行管理，以及 Linux 系统防火墙的原理与配置。

训练技能

- 掌握 Linux 系统常用服务的配置。
- 掌握 Shell 脚本基本语法与流程控制语句。
- 掌握 Sed 与 Awk 工具的使用。
- 理解防火墙工作原理，并且掌握 iptables 与 firewalld 防火墙的基本配置。

设计思路

本书采用了教材 + 扩展知识的设计思路，扩展知识提供二维码扫描，形式可以是文档、视频等，内容可以随时更新，能够更好地服务读者。

教材分为 12 个章节、3 个阶段来设计学习，即网络服务、Shell 脚本、防火墙，具体安排如下：

- 第 1 章～第 6 章介绍常见网络服务，包括 DNS、远程访问控制、YUM 仓库、NFS 共享、PXE 网络装机、Cobber 自动装机等内容。对于一些基础的服务不做重点介绍，读者可以访问课工场网站进行学习。
- 第 7 章～第 10 章介绍的是 Shell 脚本，包括 Shell 脚本的书写规范、变量的使用、条件语句、case 语句、循环语句，以及常用的编程工具 Sed、Awk 和正则表达式等内容。对于 Shell 脚本，后续课程会结合具体的应用提供更多的场景及案例。
- 第 11 章～第 12 章介绍的是防火墙，包括 iptables 防火墙的编写规则、SNAT/DNAT 策略、防火墙脚本以及 CentOS 7 采用的 firewalld 防火墙。

章节导读

- 技能目标：学习本章所要达到的技能，可以作为检验学习效果的标准。
- 内容讲解：对本章涉及的技能内容进行分析并展开讲解。
- 操作案例：对所学内容的实操训练。
- 本章总结：针对本章内容的概括和总结。

- 本章作业：针对本章内容的补充练习，用于加强对技能的理解和运用。
- 扩展知识：针对本章内容的扩展、补充，对于新知识随时可以更新。

学习资源

- 学习交流社区（课工场）
- 案例素材下载
- 相关视频教程

更多内容详见课工场 www.kgc.cn。

目　录

前言
课程设计说明

第 1 章　Linux 网络设置与基础服务 1
1.1　查看及测试网络 2
1.1.1　查看网络配置 2
1.1.2　测试网络连接 5
1.2　设置网络地址参数 6
1.2.1　使用网络配置命令 7
1.2.2　修改网络配置文件 9
1.3　DHCP 服务 11
1.4　Samba 服务 12
1.5　FTP 服务 14
1.5.1　FTP 服务基础 14
1.5.2　匿名访问的 FTP 服务 15
1.5.3　用户验证的 FTP 服务 18
1.6　Postfix 邮件系统 20
本章总结 22
本章作业 22

第 2 章　DNS 域名解析服务 23
2.1　BIND 域名服务基础 24
2.1.1　DNS 系统的作用及类型 24
2.1.2　BIND 的安装和配置文件 25
2.2　构建缓存域名服务器 29
2.3　构建主从域名服务器 31
2.3.1　构建主域名服务器 31
2.3.2　构建从域名服务器 34
2.4　构建分离解析的域名服务器 36
本章总结 38
本章作业 39

第 3 章　远程访问及控制 41
3.1　SSH 远程管理 42
3.1.1　配置 OpenSSH 服务端 42
3.1.2　使用 SSH 客户端程序 44
3.1.3　构建密钥对验证的 SSH 体系 46
3.2　TCP Wrappers 访问控制 49
3.2.1　TCP Wrappers 概述 49
3.2.2　TCP Wrappers 的访问策略 50
本章总结 51
本章作业 52

第 4 章　部署 YUM 仓库与 NFS 服务 53
4.1　部署 YUM 仓库服务 54
4.1.1　构建 YUM 软件仓库 54
4.1.2　使用 yum 工具管理软件包 56
4.2　NFS 共享存储服务 59
4.2.1　使用 NFS 发布共享资源 59
4.2.2　在客户机中访问 NFS 共享资源 60
4.2.3　NFS 客户端 mount 的挂载参数说明 62
本章总结 64
本章作业 64

第 5 章　PXE 高效批量网络装机 65
5.1　部署 PXE 远程安装服务 66
5.1.1　搭建 PXE 远程安装服务器 66
5.1.2　验证 PXE 网络安装 68
5.2　实现 Kickstart 无人值守安装 70

5.2.1 准备安装应答文件 70
5.2.2 实现批量自动装机 74
本章总结 75
本章作业 75

第 6 章 Cobbler 自动装机 77
6.1 Cobbler 概述 78
6.2 安装 Cobbler 环境 78
6.3 配置 Cobbler 服务 81
6.3.1 配置案例 82
6.3.2 YUM 仓库管理 92
6.4 PXE 菜单管理 93
6.4.1 设置 PXE 菜单密码 93
6.4.2 定制 PXE 菜单 94
6.5 Cobbler 的 Web 管理 95
6.5.1 设置 Cobbler web 登录密码 96
6.5.2 Cobbler web 的使用 97
本章总结 101

第 7 章 Shell 编程规范与变量 103
7.1 Shell 脚本编程规范 104
7.1.1 Shell 脚本应用场景 104
7.1.2 Shell 编程规范 104
7.1.3 管道与重定向 106
7.2 Shell 脚本变量揭秘 109
7.2.1 自定义变量 109
7.2.2 特殊变量 114
本章总结 117
本章作业 117

第 8 章 Shell 编程之条件语句 119
8.1 条件测试 120
8.2 if 语句 124
8.2.1 if 语句的结构 124
8.2.2 if 语句应用示例 126
本章总结 129
本章作业 129

第 9 章 Shell 编程之 case 语句与循环语句 131
9.1 使用 case 分支语句 132
9.2 使用 for 循环语句 135
9.3 使用 while 循环语句 138
9.4 Shell 函数应用 141
9.5 Shell 脚本调试 142
本章总结 143
本章作业 143

第 10 章 Shell 编程之 Sed 与 Awk 145
10.1 正则表达式概述 146
10.2 Sed 工具概述 149
10.3 Awk 工具介绍 154
10.4 Shell 编程实战 159
本章总结 161
本章作业 162

第 11 章 Linux 防火墙（一） 163
11.1 Linux 防火墙基础 164
11.1.1 iptables 的表、链结构 164
11.1.2 数据包过滤的匹配流程 166
11.2 编写防火墙规则 167
11.2.1 基本语法、数据包控制类型 167
11.2.2 添加、查看、删除规则等基本操作 168
11.2.3 规则的匹配条件 170
本章总结 173
本章作业 174

第 12 章 Linux 防火墙（二） 175
12.1 SNAT 策略及应用 176
12.1.1 SNAT 策略概述 176
12.1.2 SNAT 策略的应用 178
12.2 DNAT 策略及应用 179
12.2.1 DNAT 策略概述 179
12.2.2 DNAT 策略的应用 180

12.3 规则的导出、导入 183
12.3.1 规则的备份及还原 183
12.3.2 使用 iptables 服务 184
12.4 使用防火墙脚本 185
12.4.1 防火墙脚本的构成 185
12.4.2 防火墙脚本示例 188
12.5 firewalld 防火墙 189
12.5.1 区域的概念 189
12.5.2 字符管理工具 190
12.5.3 图形管理工具 193
本章总结 195
本章作业 195

第1章

Linux 网络设置与基础服务

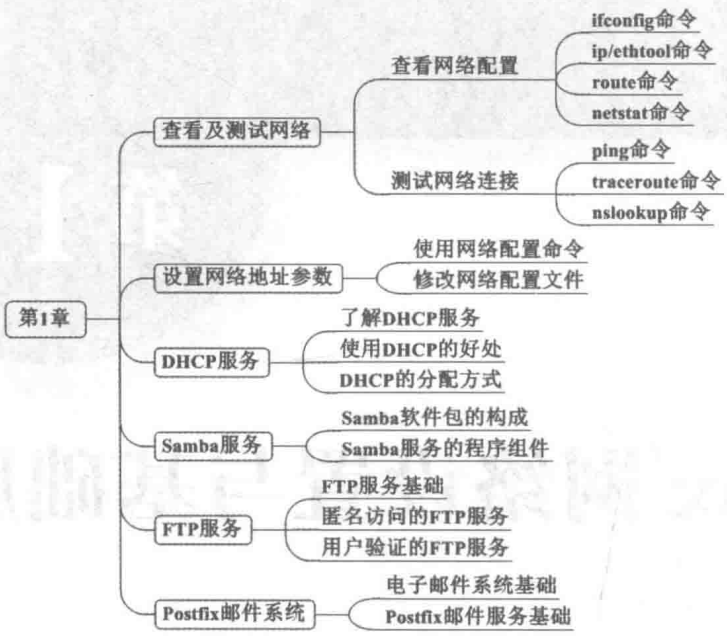
技能目标

- 学会查看及测试网络
- 学会设置网络地址参数
- 了解 DHCP、Samba、FTP、Postfix 服务

本章导读

之前大家已经学习了 Linux 系统的基本管理命令和技巧，为进一步学习 Linux 网络服务打下了基础。从本章开始，我们将陆续开始学习 Linux 系统的网络设置、文件服务、域名解析等在网络服务器方面的应用。

知识服务



1.1 查看及测试网络

查看及测试网络配置是管理 Linux 网络服务的第一步，本节中将学习 Linux 系统中的网络查看及测试命令，其中讲解的大多数命令以普通用户权限就可以完成操作。

1.1.1 查看网络配置

1. 使用 ifconfig 命令查看网络接口地址

主机的网络接口卡（网卡）通常称为“网络接口”。在 Linux 系统中，使用 ifconfig 命令可以查看网络接口的地址配置信息。

（1）查看活动的网络接口设备

当 ifconfig 命令不带任何选项和参数时，将显示当前主机中已启用（活动）的网络接口信息。例如，直接执行 ifconfig 命令后可以看到 eth0、lo 这两个网络接口的信息。这里要注意，CentOS 7 之前的网卡命名采用 eth0、eth1 等，而 CentOS 7 版本采用了一致的网络设备命名（Consistent Network Device Naming），该命名是与物理设备本身相关的。常见的其他网卡命名例如 eno16777736，表示板载的以太网设备（板载设备索引编号为 16777736）。但也可以将默认的网卡命名修改成 eth0、eth1 的形式，参见本章的知识服务。

```
[root@localhost ~]# ifconfig

eth0    flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

```
        inet 192.168.4.11  netmask 255.255.255.0  broadcast 192.168.4.255
        ……                          // 省略部分内容

        ……                          // 省略部分内容

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        ……                          // 省略部分内容
```

在上述输出结果中，eth0 对应为第 1 块物理网卡，lo 对应为虚拟的回环接口。

- eth0：第 1 块以太网卡的名称。“eth0”中的“eth”是“ethernet”的缩写，表示网卡类型为以太网，数字“0”表示第 1 块网卡。如果有多个物理网卡，则第 2 块网卡表示为“eth1”，第 3 块网卡表示为“eth2”，以此类推。
- lo：“回环”网络接口，“lo”是“loopback”的缩写，它并不代表真正的网络接口，而是一个虚拟的网络接口，其 IP 地址默认是“127.0.0.1”。回环地址通常仅用于对本机的网络测试。

如果想要查看所有网络接口信息，只需要在 ifconfig 命令后面加上 -a 选项即可，即 ifconfig -a。

（2）查看指定的网络接口信息

当只需要查看其中某一个网络接口的信息时，可以使用网络接口的名称作为 ifconfig 命令的参数（不论该网络接口是否处于激活状态）。例如，执行“ifconfig eth0”命令后可以只查看网卡 eth0 的配置信息。

```
[root@localhost ~]# ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.4.11  netmask 255.255.255.0  broadcast 192.168.4.255
        inet6 fe80::250:56ff:fe81:2986  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:81:29:86  txqueuelen 1000  (Ethernet)
        RX packets 5638126  bytes 457742188 (436.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72986  bytes 5962876 (5.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

从上述命令显示的结果中，可以获知 eth0 网卡的一些基本信息，如下所述。

- ether：表示网络接口的物理地址（MAC 地址），如“00:50:56:81:29:86”。网络接口的物理地址通常不能更改，是网卡在生产时确定的全球唯一的硬件地址。
- inet：表示网络接口的 IP 地址，如“192.168.4.11”。
- broadcast：表示网络接口所在网络的广播地址，如“192.168.4.255”。
- netmask：表示网络接口的子网掩码，如“255.255.255.0”。

除此以外，还能够通过“TX”“RX”等信息了解到通过该网络接口发送和接收的数据包个数、流量等更多属性。

2. 使用 ip/ethtool 命令查看网络接口

ip/ethtool 与 ifconfig 命令相同，也是参看网络接口的命令。但与 ifconfig 相比，ip/ethtool 命令的功能更强大，它不仅仅可以查看网络接口的基本信息，还可以查看更深层的内容，如查看网络接口的数据链路层、网络层信息和网络接口的速率、模式等信息。其中常用的命令有：

- ip link：查看网络接口的数据链路层信息。
- ip address：查看网络接口的网络层信息。
- ethtool eth0：查看指定网络接口的速率、模式等信息。

3. 使用 route 命令查看路由表条目

Linux 系统中的路由表决定着从本机向其他主机、其他网络发送数据的去向，是排除网络故障的关键信息。直接执行 route 命令可以查看当前主机中的路由表信息，在输出结果中，Destination 列对应目标网段的地址，Gateway 列对应下一跳路由器的地址，Iface 列对应发送数据的网络接口。

```
[root@localhost ~]# route
Kernel IP routing table
Destination  Gateway      Genmask        Flags  Metric  Ref  Use  Iface
192.168.4.0  *            255.255.255.0  U      0       0    0    eth0
default      192.168.4.1  0.0.0.0        UG     0       0    0    eth0
```

当目标网段为“Default”时，表示此行是默认网关记录；当下一跳为“*”时，表示目标网段是与本机直接相连的。例如，从上述输出信息中可以看出，当前主机与 192.168.4.0/24 网段直接相连，使用的默认网关地址是 192.168.4.1。

若结合“-n”选项使用，可以将路由记录中的地址显示为数字形式，这可以跳过解析主机名的过程，在路由表条目较多的情况下能够加快执行速度。例如，执行“route -n”命令后，输出信息中的“*”地址将显示为“0.0.0.0”，默认网关记录中的“default”也将显示为“0.0.0.0”。

```
[root@localhost ~]# route -n
Kernel IP routing table
Destination  Gateway      Genmask        Flags  Metric  Ref  Use  Iface
192.168.4.0  0.0.0.0      255.255.255.0  U      0       0    0    eth0
0.0.0.0      192.168.4.1  0.0.0.0        UG     100     0    0    eth0
```

4. 使用 netstat 命令查看网络连接情况

通过 netstat 命令可以查看当前系统的网络连接状态、路由表、接口统计等信息，是了解网络状态及排除网络服务故障的有效工具。以下是 netstat 命令常用的几个选项。

- -a：显示当前主机中所有活动的网络连接信息（包括监听、非监听状态的服务端口）。
- -n：以数字的形式显示相关的主机地址、端口等信息。
- -r：显示路由表信息。

- -l：显示处于监听（Listening）状态的网络连接及端口信息。
- -t：查看 TCP 协议相关的信息。
- -u：显示 UDP 协议相关的信息。
- -p：显示与网络连接相关联的进程号、进程名称信息（该选项需要 root 权限）。

通常使用“-anpt”组合选项，以数字形式显示当前系统中所有的 TCP 连接信息，同时显示对应的进程信息。结合命令管道使用“grep”命令，还可以在结果中过滤出所需要的特定记录。例如，执行以下操作可以查看本机中是否有监听“TCP 80”端口（即标准 FTP 服务）的服务程序，输出信息中包括 PID 号和进程名称。

```
[root@localhost ~]# netstat -anpt | grep ":80"
tcp6       0      0 :::80                   :::*                    LISTEN      15613/httpd
```


1.1.2 测试网络连接

1. 使用 ping 命令测试网络连通性

使用 ping 命令可以向目的主机持续地发送测试数据包，并显示反馈结果，直到按 Ctrl+C 组合键后中止测试，并显示最终统计结果。例如，以下操作将测试从本机到另一台主机 192.168.4.110 的连通性情况，连接正常时会收到返回的数据包。

```
[root@localhost ~]# ping 192.168.4.110
PING 192.168.4.110 (192.168.4.110) 56(84) bytes of data.
64 bytes from 192.168.4.110: icmp_seq=1 ttl=128 time=0.694 ms
64 bytes from 192.168.4.110: icmp_seq=2 ttl=128 time=0.274 ms
……                          // 按 Ctrl+C 组合键中止执行

--- 192.168.4.110 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1162ms
rtt min/avg/max/mdev = 0.274/0.484/0.694/0.210 ms
```

运行 ping 测试命令时，若不能获得从目标主机发回的反馈数据包，则表示在本机到目标主机之间存在网络连通性故障。例如，若看到“Destination Host Unreachable”的反馈信息，则表示目的主机不可达，可能目标地址不存在或者主机已经关闭；若看到“Network is unreachable”的反馈信息，则表示没有可用的路由记录（如默认网关），无法达到目标主机所在的网络。

```
[root@localhost ~]# ping 192.168.4.123
PING 192.168.4.123 (192.168.4.123) 56(84) bytes of data.
From 192.168.4.11 icmp_seq=2 Destination Host Unreachable
From 192.168.4.11 icmp_seq=3 Destination Host Unreachable
……                          // 省略部分内容
```

当网络中存在影响通信过程稳定性的因素（如网卡故障、病毒或网络攻击等）时，使用 ping 命令测试可能会频繁看到“Request timeout”的反馈结果，表示与目标主机间的连接超时（数据包响应缓慢或丢失）。除此以外，当目标主机有严格的防火墙限

制时，也可能收到发回“Request timeout”的反馈结果。

2. 使用 traceroute 命令跟踪数据包的路由途径

使用 traceroute 命令可以测试从当前主机到目的主机之间经过了哪些网络节点，并显示各中间节点的连接状态（响应时间）。对于无法响应的节点，连接状态将显示为“*”。例如，通过以下操作结果可以看出，从本机到目标主机 192.168.7.7 之间，中间需跨越一个路由器 192.168.4.1。

```
[root@localhost ~]# traceroute 192.168.7.7
traceroute to 192.168.7.7 (192.168.7.7), 30 hops max, 40 byte packets
 1  (192.168.4.1)  7.740 ms  15.581 ms  15.881 ms
 2  (192.168.7.7)  19.652 ms  19.995 ms  19.942 ms
```


traceroute 命令能够比 ping 命令更加准确地定位网络连接的故障点（中断点），执行速度也因此会比 ping 命令稍慢。在网络测试与排错过程中，通常会先使用 ping 命令测试与目的主机的网络连接，如果发现网络连接有故障，再使用 traceroute 命令跟踪查看是在哪个中间节点存在故障。

3. 使用 nslookup 命令测试 DNS 域名解析

当域名解析出现异常时，将无法使用域名的形式访问网络中的 Web 站点、电子邮件系统等服务。nslookup 命令是用来测试域名解析的专用工具，使用时只要指定要解析的目标域名作为参数即可。例如，执行“nslookup www.google.com”命令后，nslookup 程序将提交查询请求，询问站点 www.google.com 对应的 IP 地址是多少。

```
[root@localhost ~]# nslookup www.google.com
Server:        202.106.0.20                    // 所使用的 DNS 服务器
Address:       202.106.0.20#53

Non-authoritative answer:                      // 以下为 DNS 解析的反馈结果
Name:   www.google.com
Address: 173.194.127.51
……                                             // 省略部分内容
```

若能够成功反馈要查询域名的 IP 地址，则表示域名解析没有问题，否则需要根据实际反馈情况来判断故障原因。例如，若出现“…… no servers could be reached”的信息，表示不能连接到指定的 DNS 服务器；若出现“…… can't find xxx.yyy.zzz: NXDOMAIN”的信息，表示要查询的域名不存在。

```
[root@localhost ~]# nslookup www.google.com
;; connection timed out; trying next origin
;; connection timed out; no servers could be reached
```

1.2 设置网络地址参数

从本节开始将学习如何来修改 Linux 主机的各种网络地址参数。在 Linux 主机中，