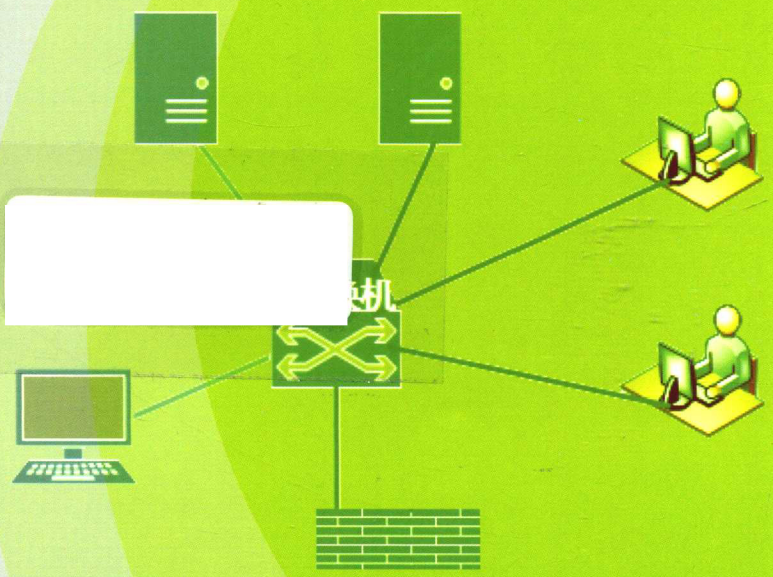
国家示范性高等职业院校建设规划教材

网络安全实训教程

WANGLUO ANQUAN SHIXUN JIAOCHENG

朱　俊　主编
丁亚明　钱　锋　主审



黄河水利出版社

国家示范性高等职业院校建设规划教材

网络安全实训教程

主　编　朱　俊
副主编　王　伟　周　曦
主　审　丁亚明　钱　锋

黄河水利出版社
·郑州·

内 容 提 要

本书是国家示范性高等职业院校建设规划教材，是用安徽省财政安排的“支持高等职业学校提升专业服务产业发展能力”项目经费组织编写的。本书是根据教育部国家示范性高等职业院校建设计划电子信息类专业群人才培养方案要求，按照计算机网络技术应用型人才培养标准编写完成的。本书共分三个项目，从主机安全、应用安全、网络安全等角度，介绍了一些常见的网络安全的实训实例。

本书可作为高等职业学校、高等专科学校及各类成人高校计算机类相关专业的实训教材，也可作为网络安全和网络运行维护技术人员的参考书或对网络安全技术感兴趣人士的自学教材。

图书在版编目(CIP)数据

网络安全实训教程/朱俊主编. —郑州：黄河水利出版社，2015. 12

国家示范性高等职业院校建设规划教材

ISBN 978-7-5509-1299-1

Ⅰ. ①网… Ⅱ. ①朱… Ⅲ. ①计算机网络-安全技术-高等职业教育-教材 Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字(2015)第 296002 号

组稿编辑：王路平 电话：0371-66022212 E-mail：hhslwlp@163. com

出 版 社：黄河水利出版社

地址：河南省郑州市顺河路黄委会综合楼 14 层 邮政编码：450003

发行单位：黄河水利出版社

发行部电话：0371-66026940、66020550、66028024、66022620(传真)

E-mail：hhslcbs@126. com

承印单位：郑州龙洋印务有限公司

开本：787 mm×1 092 mm 1/16

印张：14

字数：320 千字 印数：1—1 000

版次：2015 年 12 月第 1 版 印次：2015 年 12 月第 1 次印刷

定价：32. 00 元

前 言

本书是根据《教育部关于全面提高高等职业教育教学质量的若干意见》(教高〔2006〕16号)、《教育部关于推进高等职业教育改革创新引领职业教育科学发展的若干意见》(教职成〔2011〕12号)等文件精神,用安徽省财政安排的"支持高等职业学校提升专业服务产业发展能力"项目经费组织编写的教材。

本套教材以学生能力培养为主线,着重基本概念和基本原理的阐述,注重理论知识的应用,注重加强学生工程技术能力的训练,突出应用能力和创新能力的培养,体现出实用性、实践性、创新性的教材特色,是一套紧密联系工程实际、教学面向生产的高职高专教育精品规划教材。

21世纪已进入计算机网络时代。计算机网络极大普及,计算机应用已进入更高层次,计算机网络成了计算机行业的一部分。随着通信和计算机技术紧密结合与同步发展,我国计算机网络技术飞速发展。在计算机网络得到广泛应用的同时,网络安全问题也越来越突出。为了满足社会对计算机网络安全技术应用人才的培养需求、实现高职高专人才培养目标、提高学生的实践和创新能力,编者在多年教学实践的基础上结合最新教学成果编写了本书。

本书共分三个项目,从主机安全、应用安全、网络安全等角度,介绍了一些常见的网络安全的实训实例,涉及加密与解密、主机加固、安全策略配置、常用扫描软件使用、数据备份与恢复、防病毒软件的使用、浏览器安全设置、拒绝服务攻击、SQL Server应用安全等内容。

本书具有言简意赅、图文并茂、重点突出、实例紧贴实际、重视先进技术等特点。本书内容丰富、实用性强,以计算机网络工程项目建设为背景,取材新颖实用。本书配有大量操作应用图例,易学易懂。为了加强学生的实际应用技能的培养,本书注重强调计算机网络安全技术的应用,有大量实训项目指导学习者的实训,提高其专业与职业技能。

本书由安徽水利水电职业技术学院承担编写工作,编写人员及编写分工如下:由朱俊担任主编并负责全书统稿;由王伟、周曦担任副主编;余强、方跃胜、李翠梅、田芳参编部分内容;由丁亚明教授、钱锋副教授担任主审。

在编写过程中,安徽水利水电职业技术学院电子系领导及同志们给予了极大的支持。借此,向对本书给予帮助的同仁表示衷心感谢!

由于编写时间仓促,参编人员水平有限,书中难免会出现疏漏之处,欢迎广大师生及读者批评指正。

编 者

2015年8月

目 录

项目一　主机安全

实训一　常用网络测试命令的应用

一、实训目的

(1)了解系统网络命令及其代表的含义,以及其能对网络进行的操作。

(2)通过网络命令了解网络状态,并利用网络命令对网络进行简单的操作。

二、实训设备

实验机房,计算机安装的是 Windows 98/2000/XP 操作系统。

三、实训内容和要求

(1)利用 ping 命令检测网络连通性。

(2)利用 ipconfig 命令查看本机的网络配置信息。

(3)利用 arp 命令检验 MAC 地址解析。

(4)熟练使用 tracert、netstat、ftp 等网络命令。

四、背景知识

Windows 操作系统本身带有多种网络命令,利用这些网络命令可以对网络进行简单的操作。需要注意的是,这些命令均是在 DOS 命令行下执行的。本次实验学习 6 个最常用的网络命令。

(1)ping 命令(见图 1-1)。

```
C:\Documents and Settings\ibm>ping www.163.com

Pinging www.cache.split.netease.com [202.108.9.37] with 32 bytes of data:

Reply from 202.108.9.37: bytes=32 time=42ms TTL=47
Reply from 202.108.9.37: bytes=32 time=40ms TTL=47
Reply from 202.108.9.37: bytes=32 time=42ms TTL=47
Reply from 202.108.9.37: bytes=32 time=41ms TTL=47

Ping statistics for 202.108.9.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 42ms, Average = 41ms
```

图 1-1　ping 命令

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list

参数：

-t ping 指定的计算机直到中断。

-a 将地址解析为计算机名。

-n count 发送 count 指定的 ECHO 数据包数，默认值为 4 。

-l length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节；最大值是 65 527。

-f 在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。

-i ttl 将“生存时间”字段设置为 ttl 指定的值。

-v tos 将“服务类型”字段设置为 tos 指定的值。

-r count 在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台、最多 9 台计算机。

-s count 指定 count 指定的跃点数的时间戳。

-j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)，IP 允许的最大数量为 9。

-k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)，IP 允许的最大数量为 9。

-w timeout 指定超时间隔，单位为 ms。

destination-list 指定要 ping 的远程计算机。

查看 ping 的相关帮助信息“ping/?”

(2)ipconfig 命令(见图 1-2)。

ipconfig 是 Windows 操作系统中用于查看主机的 IP 配置命令，其显示信息中还包括主机网卡的 MAC 地址信息。该命令还可释放动态获得的 IP 地址并启动新一次的动态 IP 分配请求。

(3)arp 命令(见图 1-3)。

显示和修改 IP 地址与物理地址之间的转换表。

arp -s inet_addr eth_addr [if_addr]

arp -d inet_addr [if_addr]

arp -a [inet_addr] [-N if_addr]

-a 显示当前的 arp 信息，可以指定网络地址，不指定显示所有的表项。

-g 与 -a 一样。

-d 删除由 inet_addr 指定的主机，可以使用 * 来删除所有主机。

-s 添加主机，并将网络地址跟物理地址相对应，这一项是永久生效的。

eth_addr 物理地址。

if_addr 网卡的 IP 地址。

inet_addr 代表指定的 IP 地址。

(4)tracert 命令(见图 1-4)：判断数据包到达目的主机所经过的路径，显示数据包经过的中继节点的清单和到达时间。

(5)netstat 命令：让用户了解到自己的主机是怎样与 Internet 连接的，显示当前正在

```
C:\Documents and Settings\ibm>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : LENOVO-6D16351E
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 无线网络连接:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 3945ABG Net
k Connection
        Physical Address. . . . . . . . . : 00-1B-77-A4-51-69

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/1000 PL Network Conn
ion
        Physical Address. . . . . . . . . : 00-16-D3-BE-AC-89
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 202.115.6.179
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 202.115.6.1
        DNS Servers . . . . . . . . . . . : 202.112.14.151
                                            202.112.14.161
                                            202.112.14.161
```

图 1-2　ipconfig 命令

```
C:\>arp -a 202.115.6.1

Interface: 202.115.6.179 on Interface 0x1000003
  Internet Address      Physical Address      Type
  202.115.6.1           00-e0-7b-c0-b2-04     static
```

图 1-3　arp 命令

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert www.163.com

Tracing route to 163.xdwscache.glb0.lxdns.com [60.174.232.174]
over a maximum of 30 hops:

  1    <1 ms     1 ms     1 ms  192.168.0.1
  2    31 ms    43 ms    58 ms  117.64.80.1
  3     4 ms     3 ms     4 ms  61.190.245.213
  4     2 ms     3 ms     3 ms  61.190.245.150
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     2 ms     3 ms     2 ms  60.174.232.174

Trace complete.

C:\Documents and Settings\Administrator>

C:\Documents and Settings\Administrator>
```

图 1-4　tracert 命令

活动的网络连接。

netstat －r：显示路由表信息(见图 1-5)。

netstat －s：显示每个协议的状态，包括 TCP\UDP\ICMP 等(见图 1-6)。

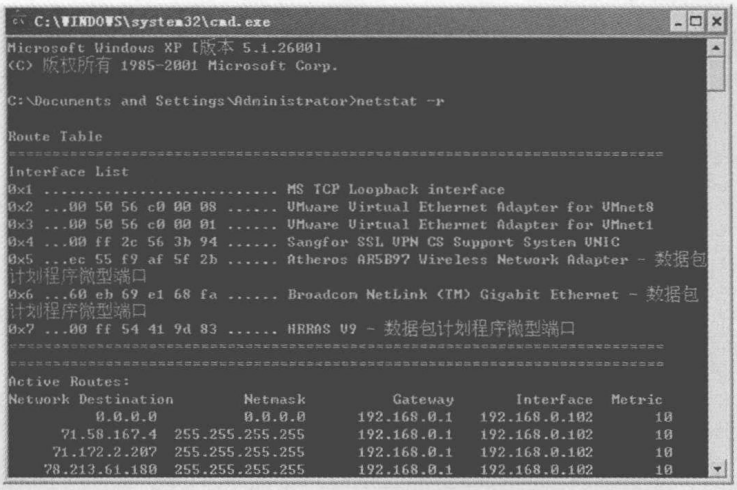


图 1-5　netstat - r 命令

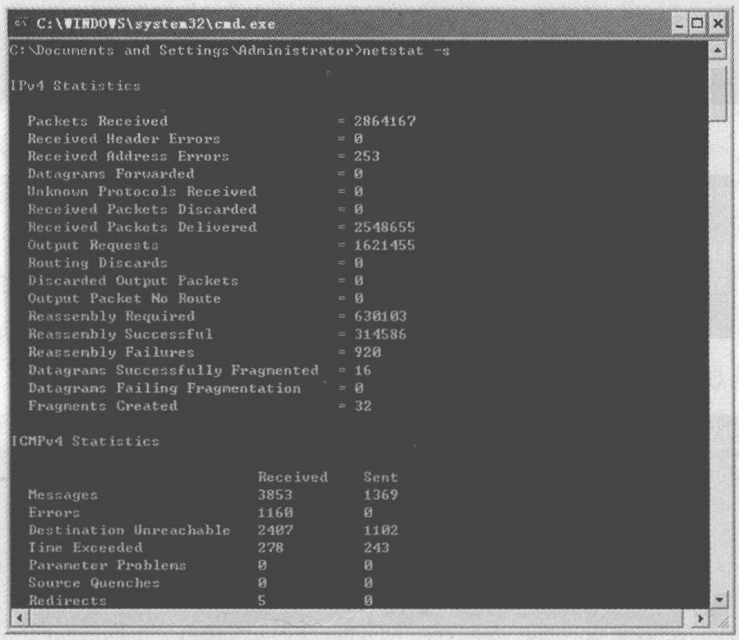


图 1-6　netstat - s 命令

netstat - n：以数字表格形式显示已经建立连接的 IP 地址和端口(见图 1-7)。

netstat - a：查看所有的连接(见图 1-8)。

(6)ftp：用于文件传输(需要存在文件传输服务器 FTP)(见图 1-9、图 1-10)。

ls：浏览目录。

put 文件名：上传文件。

get 文件名：下载文件。

quit/bye：退出命令。

五、实训步骤

(1)记录本机的主机名、MAC 地址、IP 地址、DNS、网关等信息。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

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

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.102:1306     220.181.132.158:80     ESTABLISHED
  TCP    192.168.0.102:1349     81.9.202.203:4600      ESTABLISHED
  TCP    192.168.0.102:1352     151.27.194.75:4662     TIME_WAIT
  TCP    192.168.0.102:1353     118.18.188.10:48999    TIME_WAIT
  TCP    192.168.0.102:1354     222.213.68.247:39895   ESTABLISHED
  TCP    192.168.0.102:1355     121.247.231.112:30089  SYN_SENT
  TCP    192.168.0.102:4442     88.191.221.121:7111    ESTABLISHED
  TCP    192.168.0.102:49373    1.202.103.123:40562    ESTABLISHED
  TCP    192.168.0.102:49373    27.24.213.52:4258      TIME_WAIT
  TCP    192.168.0.102:49373    49.115.224.28:7813     TIME_WAIT
  TCP    192.168.0.102:49373    50.53.25.118:51894     ESTABLISHED
  TCP    192.168.0.102:49373    62.83.201.137:56767    TIME_WAIT
  TCP    192.168.0.102:49373    71.177.169.78:53025    ESTABLISHED
  TCP    192.168.0.102:49373    77.225.212.202:54615   TIME_WAIT
  TCP    192.168.0.102:49373    77.250.103.139:54819   TIME_WAIT
  TCP    192.168.0.102:49373    78.159.199.60:50132    TIME_WAIT
  TCP    192.168.0.102:49373    78.213.61.180:53984    ESTABLISHED
```

图 1-7　netstat - n 命令

```
C:\Documents and Settings\ibm>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    LENOVO-6D16351E:echo   LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:discard  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:daytime  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:qotd   LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:chargen  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:microsoft-ds  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:30601  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:30606  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:31038  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:netbios-ssn  LENOVO-6D16351E:0      LISTENING
  TCP    LENOVO-6D16351E:2208   220.181.38.110:http    ESTABLISHED
  UDP    LENOVO-6D16351E:echo   *:*
  UDP    LENOVO-6D16351E:discard  *:*
  UDP    LENOVO-6D16351E:daytime  *:*
  UDP    LENOVO-6D16351E:qotd   *:*
  UDP    LENOVO-6D16351E:chargen  *:*
  UDP    LENOVO-6D16351E:microsoft-ds  *:*
  UDP    LENOVO-6D16351E:isakmp  *:*
  UDP    LENOVO-6D16351E:4500   *:*
  UDP    LENOVO-6D16351E:61440  *:*
  UDP    LENOVO-6D16351E:ntp    *:*
  UDP    LENOVO-6D16351E:1030   *:*
  UDP    LENOVO-6D16351E:1068   *:*
  UDP    LENOVO-6D16351E:2154   *:*
  UDP    LENOVO-6D16351E:2193   *:*
  UDP    LENOVO-6D16351E:ntp    *:*
  UDP    LENOVO-6D16351E:netbios-ns  *:*
  UDP    LENOVO-6D16351E:netbios-dgm  *:*
```

图 1-8　netstat - a 命令

```
C:\Documents and Settings\ibm>ftp /?
Unknown host /?.
ftp> ?
Commands may be abbreviated.  Commands are:

!               delete          literal         prompt          send
?               debug           ls              put             status
append          dir             mdelete         pwd             trace
ascii           disconnect      mdir            quit            type
bell            get             mget            quote           user
binary          glob            mkdir           recv            verbose
bye             hash            mls             remotehelp
cd              help            mput            rename
close           lcd             open            rmdir
ftp> _
```

图 1-9　ftp 命令

```
close           lcd             open            rmdir
ftp> o 192.168.1.3
Connected to 192.168.1.3.
220 hkzjz-109054c5c Microsoft FTP Service (Version 5.0).
User (192.168.1.3:(none)): adminstrator
331 Password required for adminstrator.
Password:
530 User adminstrator cannot log in.
Login failed.
ftp> o 192.168.1.3
Already connected to 192.168.1.3, use disconnect first.
ftp> _
```

图 1-10　建立 ftp 链接

ipconfig - all

命令描述：_____

执行结果：_____

(2)利用 ping 工具检测网络连通性。

①当一台计算机不能和网络中其他计算机进行通信时,可以按照如下步骤进行检测。在 DOS 窗口下输入“ping 127.0.0.1” 命令,用于检查本机的 TCP/IP 协议安装是否正确(注:凡是以 127 开头的 IP 地址都代表本机)。

②在 DOS 窗口下输入“ping 本机 IP 地址”命令,用于检查本机的服务和网络适配器的绑定是否正确(注:这里的服务一般是指“Microsoft 网络客户端”和“Microsoft 网络的文件和打印机共享”)。

③在 DOS 窗口下输入 “ping 网关 IP 地址” 命令,用来检查本机和网关的连接是否正常。

④在 DOS 窗口下输入 “ping 远程主机 IP 地址” 命令,用来检查网关能否将数据包转发出去。

⑤利用 ping 命令还可以来检测其他的一些配置是否正确。在 DOS 窗口下输入 “ping 主机名” 命令,用来检测 DNS 服务器能否进行主机名称解析。

⑥在 DOS 窗口下输入“ping 远程主机 IP 地址”命令,如果显示的信息为 “Destination host unreachable ”(目标主机不可达),说明这台计算机没有配置网关地址。运行 “ipconfig/all” 命令进行查看,网关地址为空。

⑦在配置网关地址后再次运行同样命令,信息变为“ Request timed out ”(请求时间超时)。此信息表示网关已经接到请求,只是找不到 IP 地址为“远程主机”的这台计算机。

命令描述：_____

执行结果：_____

ping 命令的其他用法：

连续发送 ping 探测报文：如 ping -t 202.102.192.68(这个地址需要根据具体的实验环境来搭配,见图 1-11),Ctrl + Break 查看统计信息,Ctrl + C 结束命令。

命令描述：_____

执行结果：_____

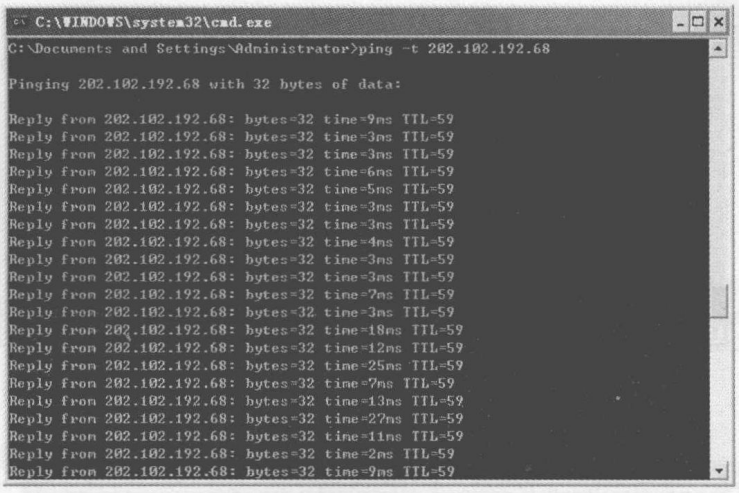


图 1-11

自选数据长度的 ping 探测报文：ping 目的主机 IP 地址 -l size，见图 1-12。

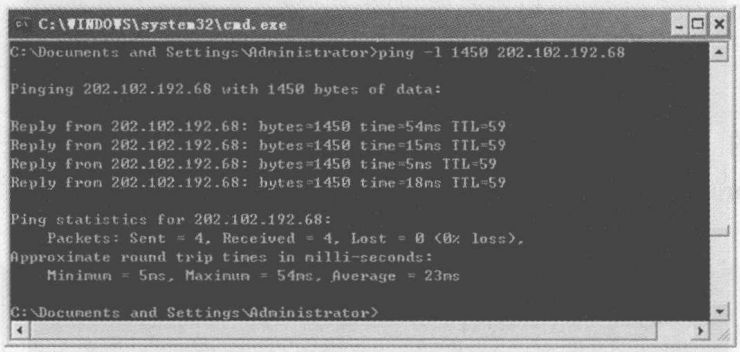


图 1-12

⑧不允许对 ping 探测报文分片：ping 目的主机 IP 地址 -f(见图 1-13)，在禁止分片的情况下，探测报文过长造成目的地不可达。

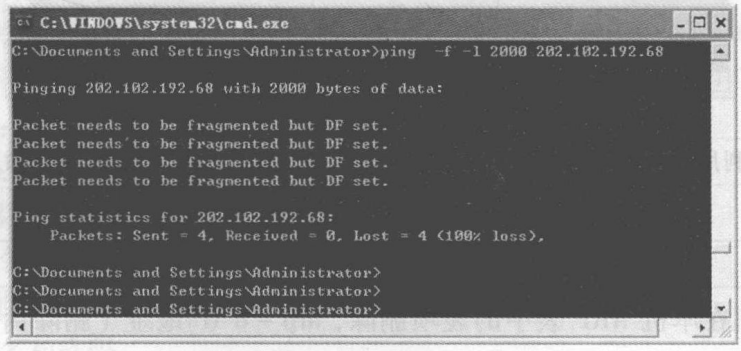


图 1-13

命令描述：_____

执行结果：_____

⑨修改“ping”命令的请求超时时间：ping 目的主机 IP 地址 -w time(见图 1-14)，指定等待每个回送应答的超时时间，单位为 ms，默认值为 1 000 ms。

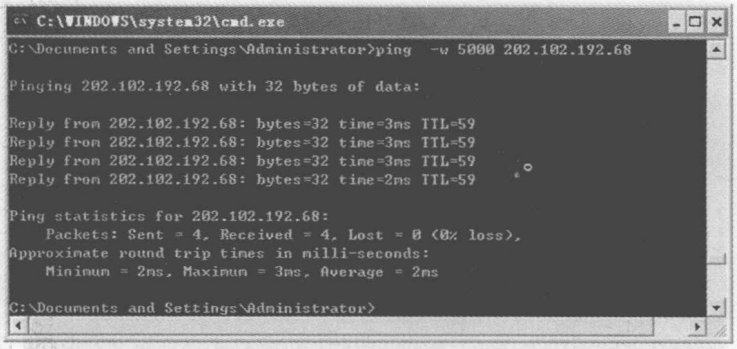


图 1-14　利用“-w”选项指定超时时间

命令描述：_____

执行结果：_____

(3)利用 arp 工具检验 MAC 地址解析。

①输入“arp -a”命令,可以查看本机的 arp 缓存内容。

命令描述：_____

执行结果：_____

②如本机的 ARP 表是空的,则 ping 本组相邻机的 IP 地址(要能 ping 通,见图 1-15),再查看本机的 arp 缓存内容,此时是否还是空的?

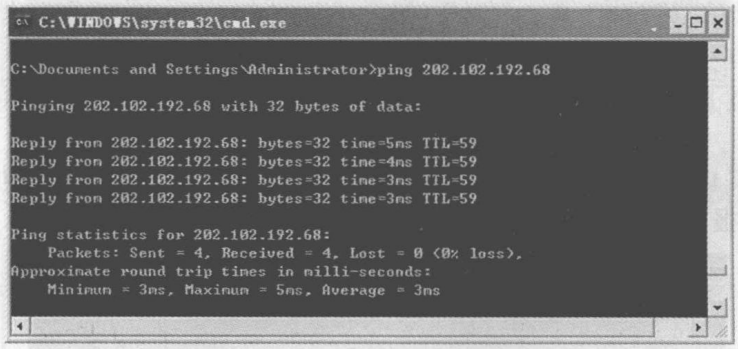


图 1-15　利用“ping”命令将一个站点的 IP 地址与 MAC 地址的映射关系加入 ARP 表

命令描述：_____

执行结果：_____

③将相邻机在本机 ARP 表中的表项删除，arp -d IP 地址（删除由 IP 地址指定的项,见图 1-16）。

命令描述：_____

执行结果：_____

④给相邻机的 IP 添加一个静止的错误的 MAC 地址对应项,再 ping 相邻机,此时是否能 ping 通?

arp -s IP 地址 MAC 地址(见图 1-17)。

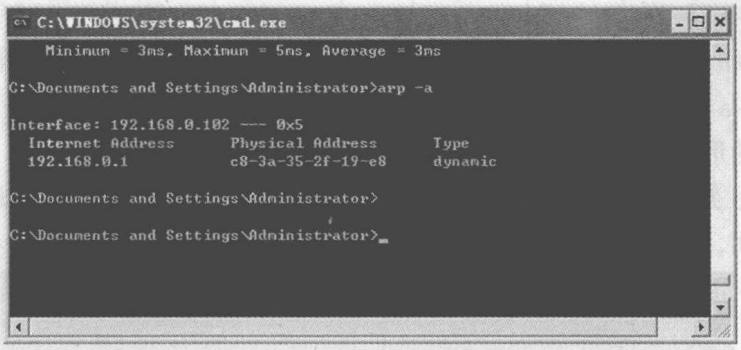


图 1-16　利用“arp - d”命令删除 ARP 表项

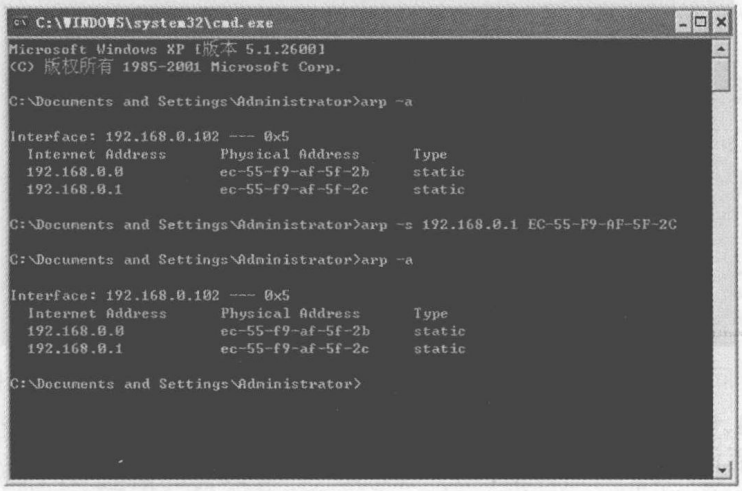


图 1-17　利用“arp - s”命令添加静态表项

在 ARP 缓存中添加项,将 IP 地址和物理地址关联,例如:

arp　- s 192.168.0.1 EC - 55 - F9 - AF - 5F - 2C 添加 IP 为 192.168.0.100 与其对应的 MAC 为 EC - 55 - F9 - AF - 5F - 2C 的表项。

命令描述:_____

执行结果:_____

熟练练习以下命令:

(1)ftp 命令。

ftp://IP 地址

输入用户名和密码

get 文件名

put 文件名

通过截图的形式记录实验结果。

(2)netstat。

①netstat　- r

②netstat －s

③netstat －n

④netstat －a

通过截图的形式记录实验结果。

(3)tracert。判断数据包到达目的主机所经过的路径,显示数据包经过的中继节点的清单和到达时间,见图 1-18。

```
C:\Documents and Settings\ibm>tracert www.163.com

Tracing route to www.cache.split.netease.com [202.108.9.38]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  202.115.6.1
  2    <1 ms    <1 ms    <1 ms  202.115.0.117
  3    <1 ms    <1 ms    <1 ms  202.115.255.242
  4    <1 ms    <1 ms    <1 ms  202.115.255.253
  5    <1 ms    <1 ms    <1 ms  202.112.53.145
  6    22 ms    21 ms    22 ms  202.112.36.114
  7    39 ms    39 ms    39 ms  202.112.36.113
  8    39 ms    38 ms    38 ms  202.112.53.178
  9    39 ms    39 ms    39 ms  58.68.255.13
 10    39 ms    39 ms    39 ms  61.135.207.169
 11    44 ms    41 ms    44 ms  58.68.132.1
 12    39 ms    40 ms    40 ms  61.49.39.65
 13    41 ms    40 ms    40 ms  61.148.5.133
 14    40 ms    42 ms    41 ms  bt-228-105.bta.net.cn [202.106.228.105]
 15    40 ms    40 ms    40 ms  bt-229-053.bta.net.cn [202.106.229.53]
 16    40 ms    40 ms    40 ms  61.148.143.30
 17    41 ms    41 ms    40 ms  210.74.176.194
 18    42 ms    41 ms    40 ms  202.108.9.38

Trace complete.
```

图 1-18　tracert 命令

六、实训结论

用户可以通过这些 DOS 命令,实现对网络状态的检查。利用 ipconfig 命令可以检查 TCP/IP 的相关配置;利用 ping 命令测试网络的物理连接是否正确、网卡驱动是否正常等;利用 arp 命令可以对本机上的 arp 缓存进行操作;利用 netstat 命令可以显示协议的统计信息和当前网络的连接状况;tracert 命令多用于显示和跟踪网关及路由信息;netstat 命令让用户了解到自己的主机是怎样与 Internet 连接的,并显示当前正在活动的网络连接。

实训二　关闭端口、服务

一、实训目的

掌握关闭服务器端口的基本方法。

二、实训设备

实验机房,计算机安装的是 Windows 操作系统。

三、实训内容和要求

(1)关闭端口的方法。

(2)停止服务的相关操作。

(3)IP 安全策略的创建及使用。

四、具体步骤

关闭服务器端口的常用方法:通过修改注册表;通过停止并禁用相关系统服务;通过配置本地 IP 安全策略实现端口的关闭。

(一)通过修改注册表关闭相关端口

通过以下的事例说明如何操作注册表来关闭 Windows 下的 445 端口。

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters 下建 DWORD 类型,键值设为 SMBDeviceEnabled = 0

(二)通过停止并禁用相关系统服务关闭端口

通过“开始”→“程序”→“管理工具”→“服务”,启动服务窗口,选中相应服务即可设置停止。

(1)关闭 79 等端口:关闭 Simple TCP/IP Service,支持以下 TCP/IP 服务:Character Generator, Daytime, Discard, Echo, 以及 Quote of the Day。

(2)关闭 25 端口:关闭 Simple Mail Transport Protocol (SMTP)服务,它提供的功能是跨网传送电子邮件。关闭 80 端口:关掉 WWW 服务。在“服务”中显示名称为 World Wide Web Publishing Service,通过 Internet 信息服务的管理单元提供 Web 连接和管理。

(3)关闭 21 端口:关闭 FTP Publishing Service,它提供的服务是通过 Internet 信息服务的管理单元提供 FTP 连接和管理。

(4)关闭 23 端口:关闭 Telnet 服务,它允许远程用户登录到系统并且使用命令行运行控制台程序。

(5)关闭 server 服务,此服务提供 RPC 支持、文件、打印以及命名管道共享。关闭它就关闭了 Windows 的默认共享,比如 ipc $、c $、admin $等,此服务关闭不影响其他操作。

(三)配置本地 IP 安全策略关闭端口

创建 IP 安全策略来屏蔽端口:

IP 安全性(Internet Protocol Security)是 Windows Sever 2000/2003 中提供的一种安全技术,它是一种基于点到点的安全模型,可以实现更高层次的局域网数据安全性。

图 1-19

在网络上传输数据的时候,通过创建 IP 安全策略,利用点到点的安全模型,能够安全有效地把源计算机的数据传输到目标计算机。

下面就详细介绍创建 IP 安全策略的步骤。

(1)单击“开始”→“控制面板”→“管理工具”,见图 1-19。

(2)在“管理工具”页面,选择“本地安全策略”,双击打开,见图 1-20。

图 1-20