《网络与通信》课程实验报告

实验 1：网络命令与网络工具使用实验

姓名	李昀哲	院系	计算机学院	学号	20123101
任课教师	刘通		指导教师	刘通	
实验地点	计 708		实验时间	2022.9.9	
实验课表现	出勤、表现得分(10)		实验报告得分(40)		实验总分	
	操作结果得分(50)					

实验目的：

1. 掌握 Windows 系统常用网络服务的配置方法
2. 掌握常用的 TCP/IP 网络中网络测试和网络诊断命令的使用方法

实验内容：

1. 使用 Windows 操作系统，了解 Telnet、FTP、WEB 服务等网络服务的配置方法；
2. 使用 Windows 操作系统，掌握常用网络测试命令的使用方法。

实验要求：（学生对预习要求的回答）（10 分）　　得分：

- 简要说明Telnet的主要命令与作用

1. 主要命令如图1所示，开启windows的telnet功能后，输入'?'命令即可查询主要命令。

```
c     - close                   关闭当前连接
d     - display                 显示操作参数
o     - open hostname [port]    连接到主机(默认端口 23)。
q     - quit                    退出 telnet
set   - set                     设置选项(键入 'set ?' 获得列表)
sen   - send                    将字符串发送到服务器
st    - status                  打印状态信息
u     - unset                   解除设置选项(键入 'set ?' 获得列表)
?/h   - help                    打印帮助信息
```

图1 telnet主要命令

close 为终止当前已经建立的联接或正在进行的联接。自动将本地系统与远程系统切断；
display 为展示当前的各类操作参数，例如，在紧急状态下是否发送中断字符等；
open 为与指定的这台主机建立 Telnet 联接，同“telnet 主机名”命令的意义相同；
quit 为退出 Telnet 应用进程，回到本地系统，任何 Telnet 命令不再起作用；
set 为设置所有可以用 display 命令显示的操作参数；
send 为已经登录到某台主机后，可以通过 send 命令发送一些信息到远程系统上；
status 为显示当前状态信息。该命令只有已经登录到某一台主机后才有效；
unset 为取消已设置的用 display 命令显示的操作参数。它与 set 命令功能刚好相反。

2. Telnet包括客户端和服务器端，客户端是Telnet客户机，服务器端是提供Telnet网络服务的系统。通过telnet命令，远程设备可以作为一个虚拟终端进行远程登录，还可以检查源站点和目的站点的应用层软件的可用性。

客户机的作用是：建立链接 -> 接收输入 -> 传送给服务器 -> 接受服务器输出

图2为分析www.microsoft.com应用层协议

图2 telnet命令分析微软官网HTTP协议

- 简要说明Ftp主要命令与作用

ftp全称为File Transfer Protocol 文件传输协议，顾名思义主要作用就是用来远程文件传输，命令主要包括：

open [IP]：用于连接一个ip地址，通常用于连接服务器；

put: 用于上传单个文件，从本地到服务器；

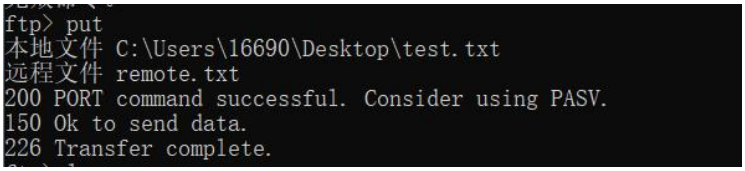

图3 put命令实验

mput：和put类似，但用于上传多个文件；

get：单个文件下载；

mget：多个文件下载；

bye：退出ftp环境

- 你所熟悉的网络测试命令有哪些

ipconfig：显示所有当前的TCP/IP网络配置值；

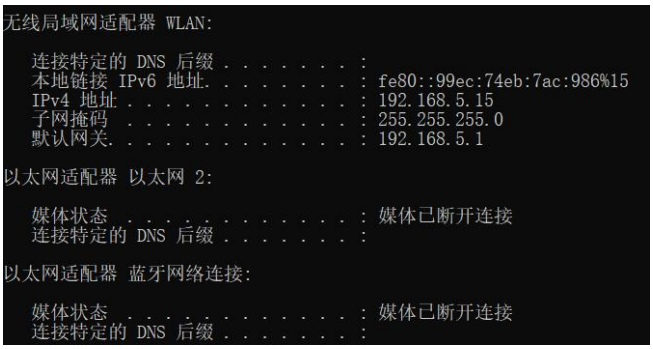

图4 ipconfig

Ping: 127.0.0.1 -> 本机IP地址 -> 默认网关 -> 目标IP地址 -> 目标主机名

图5 ping虚拟机上的ip地址

ARP：显示和修改“地址解析协议 (ARP)”缓存中的项目

```
C:\Users\16690>arp

显示和修改地址解析协议(ARP)使用的“IP 到物理”地址转换表。

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            通过询问当前协议数据，显示当前 ARP 项。
                如果指定 inet_addr，则只显示指定计算机
                的 IP 地址和物理地址。如果不止一个网络
                接口使用 ARP，则显示每个 ARP 表的项。
  -g            与 -a 相同。
  -v            在详细模式下显示当前 ARP 项。所有无效项
                和环回接口上的项都将显示。
  inet_addr     指定 Internet 地址。
  -N if_addr    显示 if_addr 指定的网络接口的 ARP 项。
  -d            删除 inet_addr 指定的主机。inet_addr 可
                以是通配符 *，以删除所有主机。
  -s            添加主机并且将 Internet 地址 inet_addr
                与物理地址 eth_addr 相关联。物理地址是用
                连字符分隔的 6 个十六进制字节。该项是永久的。
  eth_addr      指定物理地址。
  if_addr       如果存在，此项指定地址转换表应修改的接口
                的 Internet 地址。如果不存在，则使用第一
                个适用的接口。
示例:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09.... 添加静态项。
  > arp -a                                .... 显示 ARP 表。
```

图6 ARP

Netstat：显示连接统计信息

```
C:\Users\16690>netstat

活动连接

  协议  本地地址          外部地址        状态
  TCP    127.0.0.1:53496        LAPTOP-L433KM8V:54533  ESTABLISHED
  TCP    127.0.0.1:53497        LAPTOP-L433KM8V:53498  ESTABLISHED
  TCP    127.0.0.1:53498        LAPTOP-L433KM8V:53497  ESTABLISHED
  TCP    127.0.0.1:54533        LAPTOP-L433KM8V:53496  ESTABLISHED
  TCP    127.0.0.1:58747        LAPTOP-L433KM8V:58748  ESTABLISHED
  TCP    127.0.0.1:58748        LAPTOP-L433KM8V:58747  ESTABLISHED
  TCP    127.0.0.1:58749        LAPTOP-L433KM8V:58750  ESTABLISHED
  TCP    127.0.0.1:58750        LAPTOP-L433KM8V:58749  ESTABLISHED
  TCP    127.0.0.1:58751        LAPTOP-L433KM8V:58752  ESTABLISHED
  TCP    127.0.0.1:58752        LAPTOP-L433KM8V:58751  ESTABLISHED
  TCP    127.0.0.1:58774        LAPTOP-L433KM8V:58775  ESTABLISHED
  TCP    127.0.0.1:58775        LAPTOP-L433KM8V:58774  ESTABLISHED
  TCP    192.168.5.15:53431     49.7.240.75:https      ESTABLISHED
```

图7 netstat命令信息

Tracert：路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间(TTL)字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

```
C:\Users\16690>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [180.101.49.11] 的路由:

  1     1 ms    <1 毫秒     1 ms  192.168.5.1
  2     2 ms     1 ms     1 ms  192.168.1.1
  3     9 ms    18 ms     4 ms  100.65.0.1
  4     9 ms    12 ms     5 ms  61.152.49.177
  5     *        *        *     请求超时。
  6     8 ms     7 ms     7 ms  202.97.101.46
  7     *        *       11 ms  58.213.94.146
```

图 8 tracert 跟踪百度

Nslookup：通过查询 DNS 服务器检查记录、域主机别名、域主机服务和操作系统信息。

```
C:\Users\16690>nslookup www.baidu.com
服务器:  UnKnown
Address:  192.168.5.1

非权威应答:
名称:    www.a.shifen.com
Addresses:  180.101.49.12
          180.101.49.11
Aliases:  www.baidu.com
```

图 9 nslookup 查询百度的服务器信息

Net 系列命令：

```
C:\Users\16690>net share

共享名       资源                            注解

-------------------------------------------------------------------------------
C$           C:\                             默认共享
D$           D:\                             默认共享
E$           E:\                             默认共享
IPC$                                         远程 IPC
ADMIN$       C:\WINDOWS                      远程管理
命令成功完成。
```

图 10 查看本机共享

实验过程中遇到的问题如何解决的？（10 分）	得分：

问题 1：terminal 中输入 telnet 抛出“不是内部指令”的错误。

A: 在控制面板/程序和功能/启用或关闭 Windows 功能/Telnet 客户端中，打开功能选项即可正常使用。

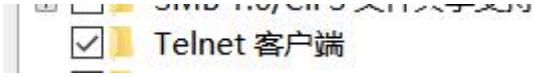

图 11 telnet 客户端选项

问题 2：win10 剔除了 telnet 服务端的功能，无法使用服务端。

A: 在 http://www.goodtechsys.com 上下载 telnet server 端，安装即可使用。

```
Welcome to GoodTech Systems Telnet Server for Windows NT/2000/XP/2003 (Evaluation Copy)

(C) Copyright 1996-2010 GoodTech Systems, Inc.

Login username:
```

图 12 telnet 服务端

问题 3：无法使用 ftp 将本地文件上传至服务端。

A: 首先使用虚拟机，在 linux 下安装 vsftpd 作为 ftp 服务器，再用 ifconfig 查看服务器 ip；本地进入 ftp 环境，open 服务器 ip，使用账号密码登录，登陆后进入需要传输的路径（当然也可以在传输时再指定）。

使用 put 命令后发现错误信息为：550 Permission denied 很明显的权限问题，但尝试一般解决方法，加入 sudo 后并未成功，故查询了解到，ftp 若想实现文件读写，必须打开权限。因此，在服务端 sudo gedit /etc/vsftpd.conf 文件中修改图中的权限，保存后成功。

```
write command.
31 write_enable=YES
```

图 13 打开“写允许”权限

问题 4：ping 不通 www.google.com
A: 首先检查 ping 127.0.0.1 是否有效，检查有效后尝试 ping www.baidu.com，同样得到反馈，之后发现时 google 是受限制的无法访问的域名，同我们直接访问一样，无法成功。
尝试中发现 ping 的次数在 windows 下默认只会有 4 次，MacOS 和 linux 下会无限重复。

问题 5：tracert www.baidu.com 的过程中，不明白为什么卡在 7 个跃点时不动了。
尚未解决

```
C:\Users\16690>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [180.101.49.11] 的路由:

  1     1 ms    <1 毫秒     1 ms  192.168.5.1
  2     2 ms     1 ms     1 ms  192.168.1.1
  3     9 ms    18 ms     4 ms  100.65.0.1
  4     9 ms    12 ms     5 ms  61.152.49.177
  5     *        *        *     请求超时。
  6     8 ms     7 ms     7 ms  202.97.101.46
  7     *        *       11 ms  58.213.94.146
```

图 14 第七个跃点时停止

本次实验的体会（结论）（10 分）	得分：

本次实验中对常用的 TCP/IP 网络测试和故障诊断命令进行了实验，观察机器的输出并检索相关输出结果的缘由，并针对部分出现的错误，进行了分析，对于无法连接、无法访问、权限不够等问题进行了解决。学会了如何利用 telnet 连接远程终端，并利用 ftp 进行文件传输操作。

但对于部分网络命令仅是进行了实验，其背后的原理还并不十分了解，还需要通过后续的课程不断加强自己的理论基础，才能更好的解决和发现网络中出现错误时的问题。

思考题：（10 分）

思考题 1：（4 分）	得分：

介绍四个以上你在实验中用到的网络命令，参数如何？表示什么含义？

Ipconfig 主要用于显示当前的网络 TCP/IP 的配置值，参数如下图所示：

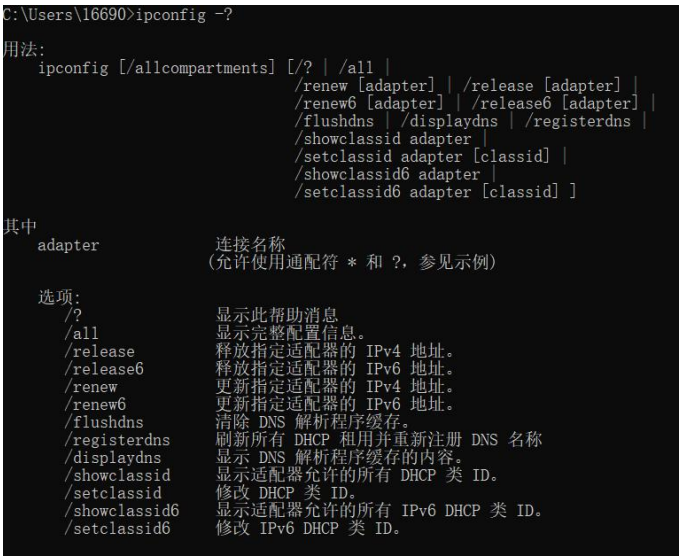

图 15 ipconfig 网络命令参数及其解释

Ping 命令：

较常用的参数为-n count 返回请求数，-u ttl 返回生存时间，-w timeout 设置每次等待的回复时间等，这些都是在处理 ping 事件时，有效的工具参数。

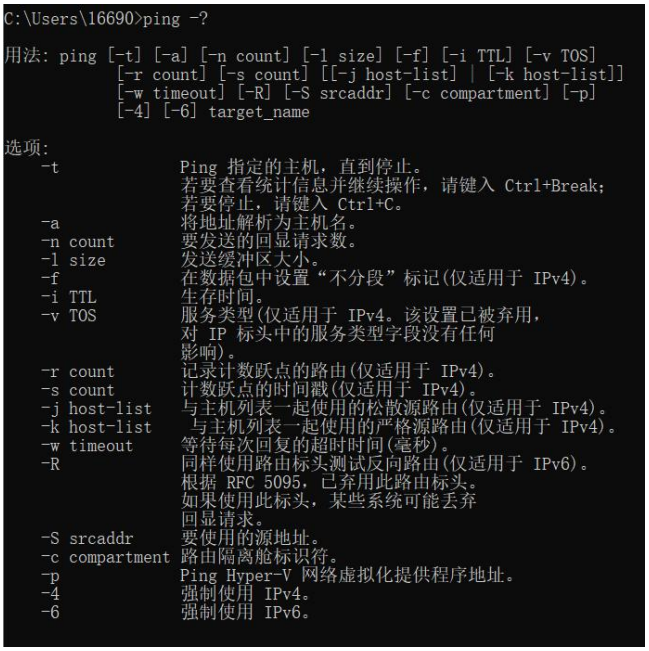

图 16 ping 命令

Netstat：显示协议统计信息和当前 TCP/IP 的网络连接

```
C:\Users\16690>netstat -?

显示协议统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            显示所有连接和侦听端口。
  -b            显示在创建每个连接或侦听端口时涉及的
                可执行文件。在某些情况下，已知可执行文件托管
                多个独立的组件，此时会
                显示创建连接或侦听端口时
                涉及的组件序列。在此情况下，可执行文件的
                名称位于底部 [] 中，它调用的组件位于顶部，
                直至达到 TCP/IP。注意，此选项
                可能很耗时，并且可能因为你没有足够的
                权限而失败。
  -e            显示以太网统计信息。此选项可以与 -s 选项
                结合使用。
  -f            显示外部地址的完全限定
                域名(FQDN)。
  -n            以数字形式显示地址和端口号。
  -o            显示拥有的与每个连接关联的进程 ID。
  -p proto      显示 proto 指定的协议的连接；proto
                可以是下列任何一个：TCP、UDP、TCPv6 或 UDPv6。如果与 -s
                选项一起用来显示每个协议的统计信息，proto 可以是下列任何一个：
                IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。
  -q            显示所有连接、侦听端口和绑定的
                非侦听 TCP 端口。绑定的非侦听端口
                不一定与活动连接相关联。
  -r            显示路由表。
  -s            显示每个协议的统计信息。默认情况下，
                显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；
                -p 选项可用于指定默认的子网。
  -t            显示当前连接卸载状态。
  -x            显示 NetworkDirect 连接、侦听器和共享
                终结点。
  -y            显示所有连接的 TCP 连接模板。
                无法与其他选项结合使用。
  interval      重新显示选定的统计信息，各个显示间暂停的
                间隔秒数。按 CTRL+C 停止重新显示
                统计信息。如果省略，则 netstat 将打印当前的
                配置信息一次。
```

图 17 netstat

Tracert：

```
C:\Users\16690>tracert -?

用法: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

选项:
    -d                  不将地址解析成主机名。
    -h maximum_hops     搜索目标的最大跃点数。
    -j host-list        与主机列表一起的松散源路由(仅适用于 IPv4)。
    -w timeout          等待每个回复的超时时间(以毫秒为单位)。
    -R                  跟踪往返行程路径(仅适用于 IPv6)。
    -S srcaddr          要使用的源地址(仅适用于 IPv6)。
    -4                  强制使用 IPv4。
    -6                  强制使用 IPv6。
```

图 18 tracert

思考题 2：（6 分）　　得分：

说明利用 Telnet 进行应用层协议（HTTP 或 SMTP 或 POP3）实验过程。

1. 打开命令行
2. 输入 telnet www.microsoft.com 80
3. 打开本地回显，输入 set localecho 并回车，再输入 GET / HTTP/1.1，换行继续输入 Host:www.microsoft.com 并回车两次

```
欢迎使用 Microsoft Telnet Client

Escape 字符为 'CTRL+]'


Microsoft Telnet> set localecho
```


GET / HTTP/1.1
Host:www.microsoft.com


GET / HTTP/1.1
Host:www.microsoft.com
HTTP/1.0 400 Bad Request
Server: GHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 208
Expires: Fri, 09 Sep 2022 00:26:10 GMT
Date: Fri, 09 Sep 2022 00:26:10 GMT
Connection: close
<HTML><HEAD>
<TITLE>Invalid URL</TITLE>
</HEAD><BODY>
<H1>Invalid URL</H1>
The requested URL "[no URL]", is invalid.<p>
Reference #9.951c3f3b.1662683170.e422d17
</BODY></HTML>

指导教师评语：

日期：