

广州大学学生实验报告

开课学院及实验室：计算机科学与工程实验室 518

2019 年 10 月 21 日

学院	计算机科学与 教育软件学院	年级/专 业/班	软件 171	姓名	谢金宏	学号	1706300001
实验课 程名称	计算机网络实验					成绩	
实验项 目名称	Windows 网络测试工具					指导老师	唐琳

一、实验目的

理解 Windows 上实用的网络工具（Ping, netstat, ipconfig, arp, tracert, route, nbtstat, net）所涉及的基本概念并学会使用这些工具测试网络的状态及从网上获取信息。

二、实验环境

安装有 TCP/IP 协议的 Windows 计算机。

三、实验内容

- 1、检测本机的 MAC 地址。
- 2、检测本机网关的 MAC 地址。
- 3、检测本地域名服务器的 IP 地址。
- 4、检测 DHCP 服务器的 MAC 地址(考虑两种网络环境:实验室网络环境和宿舍网络环境)。
- 5、检测去往 www.gzhu.edu.cn 的路径 MTU。
- 6、检测本机的路由表。
- 7、检测去往 www.gzhu.edu.cn 网络的可用性、回程响应时间及经过的路由器个数。
- 8、检测本机的所有有效连接，及各连接的端口号。
- 9、往路由表添加一条路由，去往主机 www.gzhu.edu.cn 的路由，经过邻居同学的主机转发。
- 10、（选做）课后实验并写入实验报告：
 - a) 为了确定你所在组织的路由是否稳定，使用路由跟踪程序来找到去往每一网络中的一条路由，重复测试一次，再连续测试几天，看看路由有变化吗？
 - b) 挑选 10 个 Internet 中较远的目的地，进行前一练习中的实验，看看路由变化的频度。
 - c) 上网收集网络测试工具并测试使用方法。

四、实验步骤、记录和结果

- 1、检测本机的 MAC 地址。

使用 ipconfig -all 命令可以查看本机的 MAC 地址。下图中橙色框选位置为以太网卡的物理地址。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ipconfig -all

Windows IP 配置

主机名 . . . . . : 518-01
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否

以太网适配器 本地连接 3:

    连接特定的 DNS 后缀 . . . . . :
    描述. . . . . : Realtek PCIe GBE Family Controller #2
    物理地址. . . . . : C0-3F-D5-F5-EE-5D
    DHCP 已启用 . . . . . : 是
    自动配置已启用 . . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::b948:1143:e0b5:2a67%17<首选>
    IPv4 地址 . . . . . : 202.192.34.70<首选>
    子网掩码 . . . . . : 255.255.255.0
    获得租约的时间 . . . . . : 2019年10月21日 8:21:40
    租约过期的时间 . . . . . : 2019年10月22日 8:21:36
    默认网关 . . . . . : 202.192.34.254
    DHCP 服务器 . . . . . : 202.192.34.254
    DHCPv6 IAID . . . . . : 448806869
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-22-C7-56-FC-00-98-99-00-BC-17

    DNS 服务器 . . . . . : 202.192.18.1
                           202.96.128.86
                           61.144.56.100
                           202.96.128.166
                           202.192.31.248
                           202.192.31.250
                           202.192.31.252

    TCP/IP 上的 NetBIOS . . . . . : 已启用
```

2、检测本机网关的 MAC 地址。

从步骤 1 中 config -all 命令的输出可以看出网默认网关的 IP 地址为 202.192.34.254（绿色框选位置）。使用 arp -a 202.192.34.254 即可查询默认网关的 MAC 地址。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>arp -a 202.192.34.254

接口: 202.192.34.70 --- 0x11
Internet 地址      物理地址      类型
202.192.34.254     00-0f-e2-19-00-dc 动态

C:\Users\Administrator>
```

3、检测本地域名服务器的 IP 地址。

从步骤 1 中 config -all 命令的输出可以看出本地域名服务器中的首选服务器的 IP 地址

为 202.192.18.1（蓝色框选位置）。

4、检测 DHCP 服务器的 MAC 地址(考虑两种网络环境:实验室网络环境和宿舍网络环境)。

在实验室网络环境下，从步骤 1 可知 DHCP 服务器的 IP 地址为 202.192.34.254（灰色框选位置）。使用 `arp -a 202.192.34.254` 可查询 DHCP 服务器的 MAC 地址。

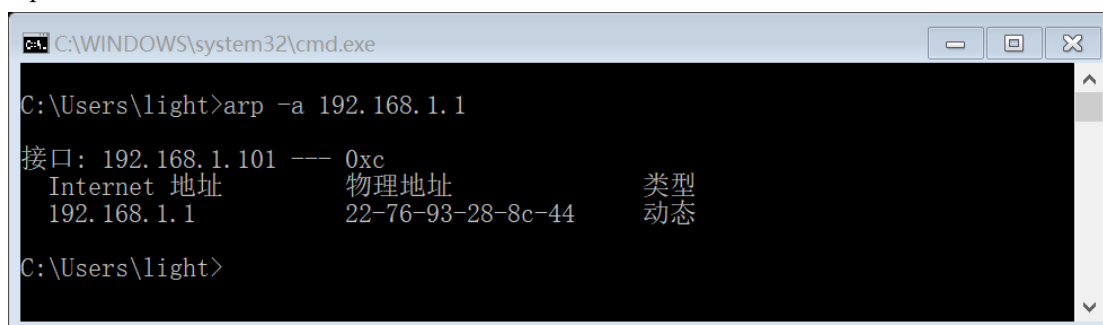


```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>arp -a 202.192.34.254

接口: 202.192.34.70 --- 0x11
Internet 地址      物理地址      类型
202.192.34.254    00-0f-e2-19-00-dc  动态

C:\Users\Administrator>
```

在寝室网络环境下，由 `ipconfig -all` 查询得 DHCP 服务器的 IP 地址为 192.168.1.1，使用 `arp -a 192.168.1.1` 查询的结果为：



```
C:\WINDOWS\system32\cmd.exe
C:\Users\light>arp -a 192.168.1.1

接口: 192.168.1.101 --- 0xc
Internet 地址      物理地址      类型
192.168.1.1        22-76-93-28-8c-44  动态

C:\Users\light>
```

5、检测去往 `www.gzhu.edu.cn` 的路径 MTU。

分别使用 `ping -l 1372 -f www.gzhu.edu.cn` 和 `ping -l 1372 -f www.gzhu.edu.cn` 得到：

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping -l 1472 -f www.gzhu.edu.cn

正在 Ping gdedu.cache.dbappwaf.cn [58.205.213.52] 具有 1472 字节的数据:
来自 58.205.213.52 的回复: 字节=1472 时间=2ms TTL=56
来自 58.205.213.52 的回复: 字节=1472 时间=7ms TTL=56
来自 58.205.213.52 的回复: 字节=1472 时间=3ms TTL=56
来自 58.205.213.52 的回复: 字节=1472 时间=2ms TTL=56

58.205.213.52 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 7ms, 平均 = 3ms

C:\Users\Administrator>ping -l 1473 -f www.gzhu.edu.cn

正在 Ping gdedu.cache.dbappwaf.cn [58.205.213.52] 具有 1473 字节的数据:
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。

58.205.213.52 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Administrator>
```

可知去往 www.gzhu.edu.cn 的 MTU 为 $1372+20+8=1500$ 。(其中 20 为 IP 数据报首部长度, 8 为 ICMP 报文首部长度。)

6、检测本机的路由表。

使用 route print 显示本机的路由表。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>route print

=====
接口列表
17...c0 3f d5 f5 ee 5d .....Realtek PCIe GBE Family Controller #2
11...00 89 98 80 cf 3f .....Realtek RTL8139/810x Family Fast Ethernet NIC
15...0a 00 27 00 00 0f .....VirtualBox Host-Only Ethernet Adapter
1.....Software Loopback Interface 1
21...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
14...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
16...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 路由表
=====
活动路由:
网络目标          网络掩码          网关          接口          跃点数
0.0.0.0            0.0.0.0            0.0.0.0        202.192.34.254  202.192.34.70    10
127.0.0.0          255.0.0.0
127.0.0.1          255.255.255.255
127.255.255.255    255.255.255.255
192.168.56.0       255.255.255.0
192.168.56.1       255.255.255.255
192.168.56.255     255.255.255.255
202.192.34.0       255.255.255.0
202.192.34.70      255.255.255.255
202.192.34.255     255.255.255.255
224.0.0.0          240.0.0.0
224.0.0.0          240.0.0.0
224.0.0.0          240.0.0.0
255.255.255.255    255.255.255.255
255.255.255.255    255.255.255.255
255.255.255.255    255.255.255.255
在链路上          127.0.0.1        306
在链路上          127.0.0.1        306
在链路上          127.0.0.1        306
在链路上          192.168.56.1     266
在链路上          192.168.56.1     266
在链路上          192.168.56.1     266
在链路上          202.192.34.70    266
在链路上          202.192.34.70    266
在链路上          202.192.34.70    266
在链路上          127.0.0.1        306
在链路上          202.192.34.70    266
在链路上          192.168.56.1     266
在链路上          127.0.0.1        306
在链路上          202.192.34.70    266
在链路上          192.168.56.1     266
=====

永久路由:
无

IPv6 路由表
=====
活动路由:
如果跃点数网络目标          网关
12  1110 ::/0                2002:c058:6301::c058:6301
1   306  ::1/128                在链路上
12  1010 2002::/16            在链路上
12  266  2002:cac0:2246::cac0:2246/128 在链路上
17  266  fe80::/64                在链路上
15  266  fe80::/64                在链路上
15  266  fe80::9b7:65dd:84c3:7f03/128 在链路上
```

7、检测去往 www.gzhu.edu.cn 网络的可用性、回程响应时间及经过的路由器个数。

使用 `ping -n www.gzhu.edu.cn` 来检测网络可用性和回程响应时间。

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping -n 10 www.gzhu.edu.cn

正在 Ping gdedu.cache.dbappwaf.cn [58.205.213.52] 具有 32 字节的数据:
来自 58.205.213.52 的回复: 字节=32 时间=1ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=2ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=2ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=3ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=1ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=2ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=1ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=1ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=1ms TTL=56
来自 58.205.213.52 的回复: 字节=32 时间=1ms TTL=56

58.205.213.52 的 Ping 统计信息:
    数据包: 已发送 = 10, 已接收 = 10, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 1ms, 最长 = 3ms, 平均 = 1ms

C:\Users\Administrator>
```

使用 tracert www.gzhu.edu.cn 来检测经过路由器的个数。

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>tracert www.gzhu.edu.cn

通过最多 30 个跃点跟踪
到 gdedu.cache.dbappwaf.cn [58.205.213.52] 的路由:

 1  1 ms    2 ms    1 ms    202.192.34.254
 2  <1 毫秒 <1 毫秒 <1 毫秒 202.192.31.245
 3  2 ms    2 ms    3 ms    172.22.72.254
 4  2 ms    2 ms    2 ms    10.254.0.121
 5  1 ms    *        1 ms    10.211.211.13
 6  *        *        *        请求超时。
 7  *        29 ms   37 ms    202.112.19.10
 8  106 ms   2 ms     2 ms    scn-rgw6.gznet.edu.cn [202.112.19.49]
 9  *        *        *        请求超时。
10  *        *        1 ms     58.205.213.52

跟踪完成。

C:\Users\Administrator>
```

如图可知，本机发送的数据包要经过 9 个中间路由器才能到达 www.gzhu.edu.cn。

8、检测本机的所有有效连接，及各连接的端口号。

使用 netstat -a -n 命令：

```

管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -a -n

活动连接

协议 本地地址 外部地址 状态
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49160 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1434 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5354 0.0.0.0:0 LISTENING
TCP 127.0.0.1:49169 127.0.0.1:49170 ESTABLISHED
TCP 127.0.0.1:49170 127.0.0.1:49169 ESTABLISHED
TCP 127.0.0.1:49173 127.0.0.1:49174 ESTABLISHED
TCP 127.0.0.1:49174 127.0.0.1:49173 ESTABLISHED
TCP 127.0.0.1:49175 127.0.0.1:49176 ESTABLISHED
TCP 127.0.0.1:49176 127.0.0.1:49175 ESTABLISHED
TCP 127.0.0.1:64678 127.0.0.1:64679 ESTABLISHED
TCP 127.0.0.1:64679 127.0.0.1:64678 ESTABLISHED
TCP 192.168.56.1:139 0.0.0.0:0 LISTENING
TCP 202.192.34.70:139 0.0.0.0:0 LISTENING
TCP 202.192.34.70:2388 0.0.0.0:0 LISTENING
TCP 202.192.34.70:64643 111.206.58.11:80 ESTABLISHED
TCP 202.192.34.70:64690 172.217.194.95:443 SYN_SENT
TCP 202.192.34.70:64691 172.217.194.95:443 SYN_SENT
TCP 202.192.34.70:64694 36.110.237.176:80 ESTABLISHED
TCP 202.192.34.70:64697 111.7.68.174:80 ESTABLISHED
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:1433 [::]:0 LISTENING
TCP [::]:49152 [::]:0 LISTENING
TCP [::]:49153 [::]:0 LISTENING
TCP [::]:49154 [::]:0 LISTENING
TCP [::]:49155 [::]:0 LISTENING
TCP [::]:49156 [::]:0 LISTENING
TCP [::]:49160 [::]:0 LISTENING
TCP [::]:1434 [::]:0 LISTENING
UDP 0.0.0.0:123 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 0.0.0.0:5355 *:*
UDP 0.0.0.0:50315 *:*
UDP 0.0.0.0:50605 *:*
UDP 0.0.0.0:52260 *:*
UDP 0.0.0.0:52297 *:*
UDP 0.0.0.0:52327 *:*

```

9、 往路由表添加一条路由，去往主机 www.gzhu.edu.cn 的路由，经过邻居同学的主机转发。

在寝室环境下进行实验，首先使用 `nslookup www.gzhu.edu.cn` 查询得主机的 IP 地址为 58.205.213.52。局域网内同学的主机的 IP 地址为 192.168.1.159。使用 `route add 58.205.213.52 192.168.1.159` 可以向路由表中添加一条由邻居同学的主机转发的路由规则。

使用 `route print -4` 可以看出路由表中确实存在这样的规则：

```
管理员: Windows PowerShell
PS C:\WINDOWS\system32> route add 58.205.213.52 192.168.1.159
操作完成!
PS C:\WINDOWS\system32> route print -4
=====
接口列表
22...68 f7 28 8d 96 1e .....Realtek PCIe GBE Family Controller
38...02 00 4c 4f 4f 50 .....Npcap Loopback Adapter
21...22 0d b0 31 73 f6 .....Microsoft Wi-Fi Direct Virtual Adapter #4
11...20 0d b0 31 73 f6 .....Microsoft Wi-Fi Direct Virtual Adapter #5
12...20 0d b0 31 73 f6 .....Realtek 8821CU Wireless LAN 802.11ac USB NIC
1.....Software Loopback Interface 1
16...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

IPv4 路由表
=====
活动路由:
网络目标      网络掩码      网关      接口      跃点数
0.0.0.0      0.0.0.0      192.168.1.1      192.168.1.101      55
58.205.213.52 255.255.255.255 192.168.1.159 192.168.1.101      56
127.0.0.0      255.0.0.0      在链路上      127.0.0.1      331
127.0.0.1      255.255.255.255 在链路上      127.0.0.1      331
127.255.255.255 255.255.255.255 在链路上      127.0.0.1      331
169.254.0.0      255.255.0.0      在链路上      169.254.135.94      281
169.254.135.94 255.255.255.255 在链路上      169.254.135.94      281
169.254.255.255 255.255.255.255 在链路上      169.254.135.94      281
192.168.1.0      255.255.255.0      在链路上      192.168.1.101      311
192.168.1.101 255.255.255.255 在链路上      192.168.1.101      311
192.168.1.255 255.255.255.255 在链路上      192.168.1.101      311
192.168.137.0 255.255.255.0      在链路上      192.168.137.1      281
192.168.137.1 255.255.255.255 在链路上      192.168.137.1      281
192.168.137.255 255.255.255.255 在链路上      192.168.137.1      281
224.0.0.0      240.0.0.0      在链路上      127.0.0.1      331
224.0.0.0      240.0.0.0      在链路上      169.254.135.94      281
224.0.0.0      240.0.0.0      在链路上      192.168.1.101      311
224.0.0.0      240.0.0.0      在链路上      192.168.137.1      281
255.255.255.255 255.255.255.255 在链路上      127.0.0.1      331
255.255.255.255 255.255.255.255 在链路上      169.254.135.94      281
255.255.255.255 255.255.255.255 在链路上      192.168.1.101      311
255.255.255.255 255.255.255.255 在链路上      192.168.137.1      281
=====
永久路由:
无
```

但实际上无法 ping 通，可能因为同学的主机拒绝转发这样的数据包。

10、上网收集网络测试工具并测试使用方法。

Windows 与 Linux 上的网络环境测试工具对照如下：

Windows 上的命令	Linux 上的命令
ping	ping, ping6
netstat	netstat
ipconfig	ifconfig
route	route, iptables
tracert	tracert
arp	arp
nbtstat	无
net	无

另一个常用的网络工具是 nmap，它是著名的端口扫描工具。例如，使用命令 nmap

-sn 192.168.1.0/24 可以 ping 192.168.1.0/24 上所有的主机并显示哪些主机回应了 ping 请求。

五、实验分析

进行计算机网络实验时，要注意融会贯通，否则容易只见现象不见原因，例如：

1. 在使用 ARP 命令查询 DHCP 服务器的 MAC 地址时，若服务器与主机不在同一网段中，则 ARP 协议不能获得 DHCP 服务器的 MAC 地址。因为 IP 数据包不是直接交付给服务器的，而是需要通过网关的转发，因此 ARP 协议只能获取到网关的 MAC 地址。
2. 使用 ipconfig 命令查询 MAC 地址时，每张网卡都可能有一个 MAC 地址。
3. 使用 ping 命令结合 -l <size> 开关可以检测链路的 MTU。注意链路的 MTU 是参数中的 size+20+8。因为 ICMP 报文首部长度 8 字节，并封装在 IP 数据报中。IP 数据报的首部长度为 20 字节。

六、练习与思考

1. 在 Windows2000 操作系统的客户端可以通过（ C ）命令查看 DHCP 服务器分配给本机的 IP 地址。（2006.5 网络管理员试题）
A.config B.ifconfig C.ipconfig D.route
2. 在 Windows2000 操作系统中，配置 IP 地址的命令是（① B ）。若用 ping 命令来测试本机是否安装了 TCP/IP 协议，则正确的命令是（② B ）。如果要列出本机当前建立的连接，可以使用的命令是（③ C ）。（2004.11 网络工程师试题）
①A.winipcfg B.ipconfig C.ipcfg D.winipconfig
②A.ping 127.0.0.0 B.ping 127.0.0.1 C.ping 127.0.1.1 D.ping 127.1.1.1
③A.netstat -s B.netstat -0 C.netstat -a D.netstat -r
3. 在 Windows 中，ping 命令的 -n 选项表示（ A ）。（2005.5 网络工程师试题）
A.ping 的次数 B.ping 的网络号
C.数字形式显示结果 D.不要重复，只 ping 一次
4. 在 Windows 中，tracert 命令的 -h 选项表示（ B ）。（2005.5 网络工程师试题）
A.指定主机名 B.指定最大跳步数
C.指定达到目标主机的时间 D.指定源路由
5. 某校园网用户无法访问外部站点 210.102.58.74，管理人员在 Windows 操作系统下可以使用（ B ）判断故障发生在校园网内还是校园网外。（2006.5 网络工程师试题）
A.ping 210.102.58.74 B.tracert 210.102.58.74
C.netstat 210.102.58.74 C.arp 210.102.58.74
6. 某人配置“Internet 协议（TCP/IP）属性”以后，使用 ipconfig 命令验证配置的选项，其结果如图 1.4 所示，IP 地址和子网掩码选项分别是 0.0.0.0。请分析可能导致这种情况

况的原因，并如何解决这个问题。

```
C:\WINDOWS\system32\cmd.exe

C:\>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : hr-75d67fa21b83
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . :
    Description . . . . . : Intel(R) PRO/100 VE Network Connection
    Physical Address. . . . . : 00-11-11-13-45-78
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :
    DNS Servers . . . . . : 172.16.2.1
                           202.96.68.128

C:\>
```

IP 地址和子网掩码分别为 0.0.0.0，说明该计算机没有分配到有效的 IP 地址。从截图中观察到该同学查询到了 DNS 服务器，因此该同学实际上能够连接到 TCP/IP 网络。并且从截图中观察到该同学的 DHCP 功能没有启用，尝试启用 DHCP 可能解决此问题。若还不能解决，可以考虑手动配置 IP 地址和掩码。