# 计算机网络及应用 实验一

# 基本网络操作命令

姓名：钟清扬

学号：2016011481

班级：自 65

# 目录

计算机网络及应用 实验一 ..... 1
基本网络操作命令 ..... 1
实验目的 ..... 3
实验环境 ..... 3
实验内容 ..... 3
ipconfig ..... 3
nbstat ..... 3
netstat ..... 5
arp ..... 8
ping ..... 9
tracert ..... 11
实验思考 ..... 11
实验总结 ..... 13

# 实验目的

练习使用网络常用命令，进一步了解网络地址、子网掩码、域名、网关、路由、地址解析、协议和端口等基本概念；通过查看和测试网络状态，发现和解决网络可能存在的问题。

# 实验环境

微机环境：win10 操作系统
网络环境：Tsinghua 无线局域网（紫荆公寓 8 号楼）

# 实验内容

## ipconfig

练习使用 ipconfig 工具,检测网络配置查看并记录本地微机的 IP(V4)地址、子网掩码、DNS 服务器地址、默认网关地址、网卡物理地址等；

使用 ipconfig/all 指令：

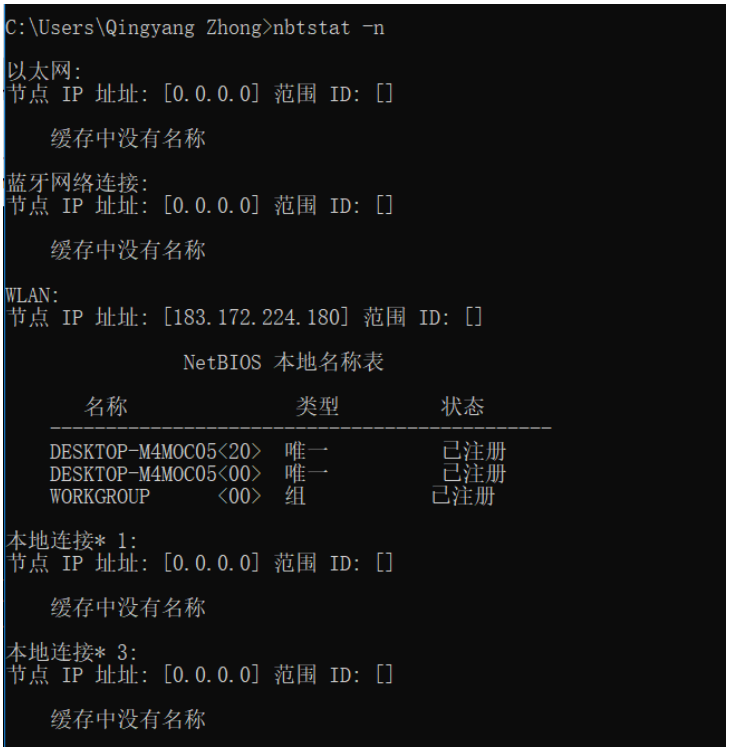
```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . : tsinghua.edu.cn
   描述. . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   物理地址. . . . . . . . . . . . . : 18-5E-0F-7C-BB-CC
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : 2402:f000:2:e001:f96d:fd96:66d8:b6b(首选)
   临时 IPv6 地址. . . . . . . . . . : 2402:f000:2:e001:9c46:d266:775b:6802(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::f96d:fd96:66d8:b6b%13(首选)
   IPv4 地址 . . . . . . . . . . . . : 183.172.224.180(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.248.0
   获得租约的时间  . . . . . . . . . : 2018年10月5日 19:39:05
   租约过期的时间  . . . . . . . . . : 2018年10月5日 21:09:05
   默认网关. . . . . . . . . . . . . : fe80::9203:25ff:feb9:7f05%13
                                       183.172.224.1
   DHCP 服务器 . . . . . . . . . . . : 172.17.3.150
   DHCPv6 IAID . . . . . . . . . . . : 85483023
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-22-22-93-E5-18-5E-0F-7C-BB-CC
   DNS 服务器  . . . . . . . . . . . : 166.111.8.28
                                       166.111.8.29
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

可知本地微机的基本信息：
IP(V4)地址：183.172.224.180
子网掩码：255.255.248.0
DNS 服务器地址：166.111.8.28
默认网关地址：183.172.224.1
网卡物理地址：18-5E-0F-7C-BB-CC

## nbstat

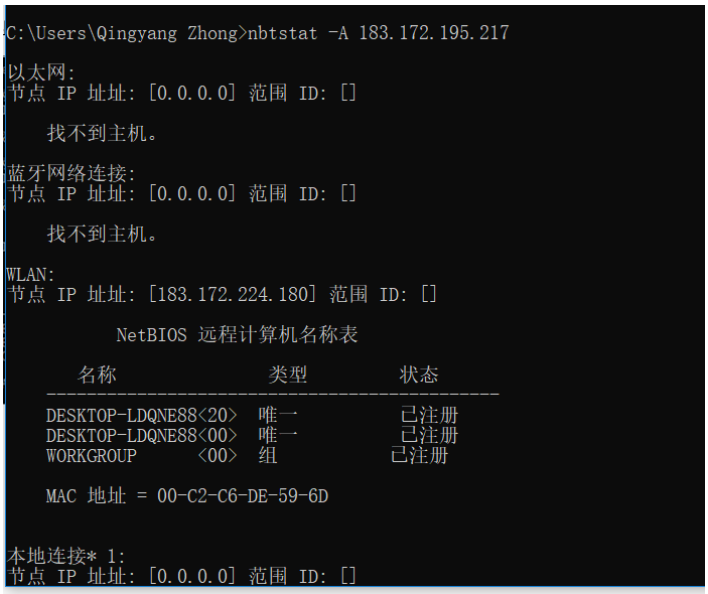
使用 nbtstat 工具，确定本机和相邻微机的 NetBIOS 信息

使用 nbtstat –n 命令,获得本地 NetBIOS 名称:




本地 NetBIOS 名称为 DESKTOP-M4M0C05

使用 nbtstat -A 命令,获得指定 IP 地址的远程主机的 NetBIOS 信息，并获得远程主机的 MAC 地址:



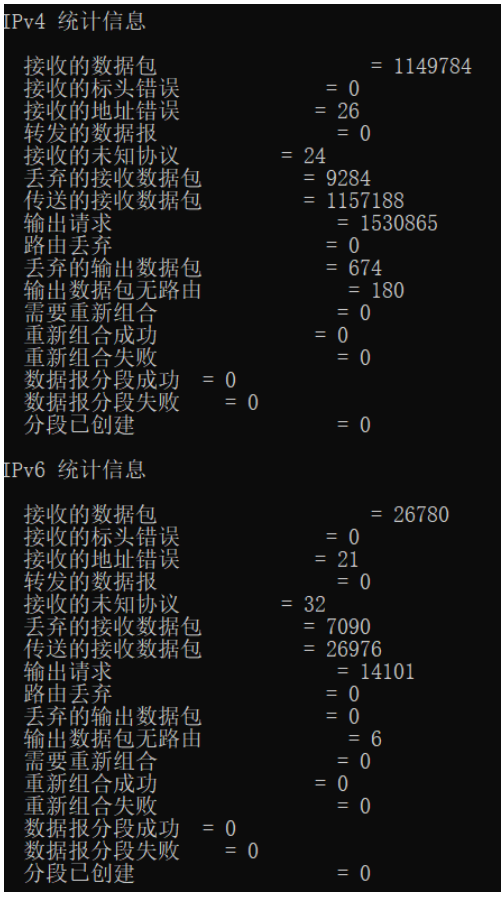

搜寻同样连接 Tsinghua 无线局域网的室友的 IP 地址，可得到相邻微机的名称为 DESKTOP-LDQNE88，MAC 地址为 00-C2-C6-DE-59-6D

# netstat

使用 netstat 工具，查看并记录本机传输层协议统计信息和协议端口

使用 netstat -s 命令,按协议显示统计信息，默认情况下显示 TCP、UDP、ICMP 和 IP 协议的统计信息：

IP 协议统计信息：




TCP 协议统计信息：

UDP 协议统计信息：

```
IPv4 的 UDP 统计信息

  接收的数据报     = 94102
  无端口           = 2291
  接收错误         = 7373
  发送的数据报     = 130537

IPv6 的 UDP 统计信息

  接收的数据报     = 8724
  无端口           = 671
  接收错误         = 6393
  发送的数据报     = 2085
```

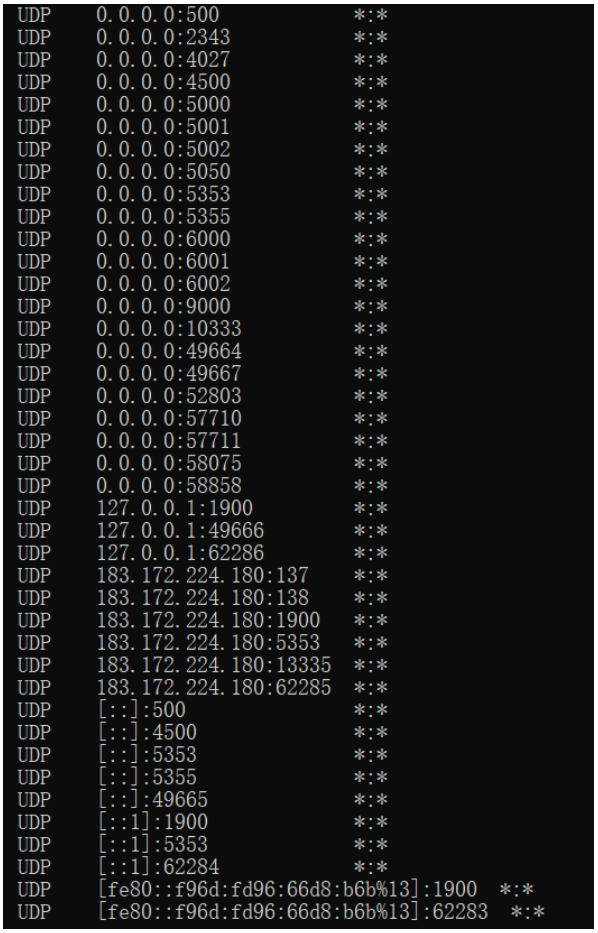
ICMP 协议统计信息：

```
ICMPv4 统计信息

                          已接收    已发送
  消息                    1131      913
  错误                    0         0
  目标不可达    56        730
  超时          34        0
  参数问题      0         0
  源抑制        0         0
  重定向        0         0
  回显回复      1021      2
  回显          20        181
  时间戳        0         0
  时间戳回复    0         0
  地址掩码      0         0
  地址掩码回复  0         0
  路由器请求    0         0
  路由器播发    0         0

ICMPv6 统计信息

                          已接收    已发送
  消息                    3710      299
  错误                    0         0
  目标不可达    0         11
  数据包太大    0         0
  超时          0         0
  参数问题      0         0
  回显          1         0
  回显回复      0         0
  MLD 查询      2         0
  MLD 报告      219       0
  MLD 已完成    33        0
  路由器请求    0         90
  路由器播发    3372      0
  邻居请求      25        119
  邻居播发      58        79
  重定向        0         0
  路由器重新编号  0       0
```

使用 netstat -a 命令,可显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口，本机的协议端口如图所示

```
C:\Users\Qingyang Zhong>netstat -a

活动连接

  协议   本地地址           外部地址        状态
  TCP    0.0.0.0:135            DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:2343           DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:3580           DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:3582           DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:8080           DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49189          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49690          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:49700          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:58185          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:59110          DESKTOP-M4MOC05:0      LISTENING
  TCP    0.0.0.0:59111          DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:4000         DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:4300         DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:4301         DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:10000        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:15292        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:21440        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:21441        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:48303        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:48303        DESKTOP-M4MOC05:49725  ESTABLISHED
  TCP    127.0.0.1:49682        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:49682        DESKTOP-M4MOC05:49688  ESTABLISHED
  TCP    127.0.0.1:49688        DESKTOP-M4MOC05:49682  ESTABLISHED
  TCP    127.0.0.1:49725        DESKTOP-M4MOC05:48303  ESTABLISHED
  TCP    127.0.0.1:51280        DESKTOP-M4MOC05:51279  TIME_WAIT
  TCP    127.0.0.1:51282        DESKTOP-M4MOC05:51281  TIME_WAIT
  TCP    127.0.0.1:51286        DESKTOP-M4MOC05:51285  TIME_WAIT
  TCP    127.0.0.1:51288        DESKTOP-M4MOC05:51287  TIME_WAIT
  TCP    127.0.0.1:58969        DESKTOP-M4MOC05:62522  ESTABLISHED
  TCP    127.0.0.1:59076        DESKTOP-M4MOC05:59077  ESTABLISHED
  TCP    127.0.0.1:59077        DESKTOP-M4MOC05:59076  ESTABLISHED
  TCP    127.0.0.1:59078        DESKTOP-M4MOC05:59079  ESTABLISHED
  TCP    127.0.0.1:59079        DESKTOP-M4MOC05:59078  ESTABLISHED
  TCP    127.0.0.1:59136        DESKTOP-M4MOC05:59137  ESTABLISHED
```

```
  TCP    127.0.0.1:59138        DESKTOP-M4MOC05:59139  ESTABLISHED
  TCP    127.0.0.1:59139        DESKTOP-M4MOC05:59138  ESTABLISHED
  TCP    127.0.0.1:61158        DESKTOP-M4MOC05:61159  ESTABLISHED
  TCP    127.0.0.1:61159        DESKTOP-M4MOC05:61158  ESTABLISHED
  TCP    127.0.0.1:61160        DESKTOP-M4MOC05:61161  ESTABLISHED
  TCP    127.0.0.1:61161        DESKTOP-M4MOC05:61160  ESTABLISHED
  TCP    127.0.0.1:62522        DESKTOP-M4MOC05:0      LISTENING
  TCP    127.0.0.1:62522        DESKTOP-M4MOC05:58969  ESTABLISHED
  TCP    183.172.224.180:139    DESKTOP-M4MOC05:0      LISTENING
  TCP    183.172.224.180:49728  .:http                 CLOSE_WAIT
  TCP    183.172.224.180:51270  52.229.168.53:https    TIME_WAIT
  TCP    183.172.224.180:51271  52.229.170.171:https   TIME_WAIT
  TCP    183.172.224.180:51277  52.229.170.171:https   ESTABLISHED
  TCP    183.172.224.180:51278  ec2-54-222-183-226:http  CLOSE_WAIT
  TCP    183.172.224.180:51283  smtp96:69              TIME_WAIT
  TCP    183.172.224.180:51284  182.254.48.91:https    TIME_WAIT
  TCP    183.172.224.180:51289  smtp96:69              TIME_WAIT
  TCP    183.172.224.180:61183  52.230.84.0:https      ESTABLISHED
  TCP    183.172.224.180:62213  182.254.78.139:https   ESTABLISHED
  TCP    [::]:135               DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:445               DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:7680              DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49189             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49664             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49665             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49666             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49667             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49690             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:49700             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::]:58185             DESKTOP-M4MOC05:0      LISTENING
  TCP    [::1]:49670            DESKTOP-M4MOC05:49671  ESTABLISHED
  TCP    [::1]:49671            DESKTOP-M4MOC05:49670  ESTABLISHED
  TCP    [::1]:49676            DESKTOP-M4MOC05:49677  ESTABLISHED
  TCP    [::1]:49677            DESKTOP-M4MOC05:49676  ESTABLISHED
  TCP    [::1]:49678            DESKTOP-M4MOC05:49679  ESTABLISHED
  TCP    [::1]:49679            DESKTOP-M4MOC05:49678  ESTABLISHED
  TCP    [::1]:49680            DESKTOP-M4MOC05:49681  ESTABLISHED
  TCP    [::1]:49681            DESKTOP-M4MOC05:49680  ESTABLISHED
  TCP    [2402:f000:2:e001:9c46:d266:775b:6802]:51292  g2600-1406-c800-038a-0000-0000-0000-11e2:https  ESTABLISHED
  TCP    [2402:f000:2:e001:9c46:d266:775b:6802]:61979  ti-in-x6c:imaps        ESTABLISHED
```



```
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:2343           *:*
UDP    0.0.0.0:4027           *:*
UDP    0.0.0.0:4500           *:*
UDP    0.0.0.0:5000           *:*
UDP    0.0.0.0:5001           *:*
UDP    0.0.0.0:5002           *:*
UDP    0.0.0.0:5050           *:*
UDP    0.0.0.0:5353           *:*
UDP    0.0.0.0:5355           *:*
UDP    0.0.0.0:6000           *:*
UDP    0.0.0.0:6001           *:*
UDP    0.0.0.0:6002           *:*
UDP    0.0.0.0:9000           *:*
UDP    0.0.0.0:10333          *:*
UDP    0.0.0.0:49664          *:*
UDP    0.0.0.0:49667          *:*
UDP    0.0.0.0:52803          *:*
UDP    0.0.0.0:57710          *:*
UDP    0.0.0.0:57711          *:*
UDP    0.0.0.0:58075          *:*
UDP    0.0.0.0:58858          *:*
UDP    127.0.0.1:1900         *:*
UDP    127.0.0.1:49666        *:*
UDP    127.0.0.1:62286        *:*
UDP    183.172.224.180:137    *:*
UDP    183.172.224.180:138    *:*
UDP    183.172.224.180:1900   *:*
UDP    183.172.224.180:5353   *:*
UDP    183.172.224.180:13335  *:*
UDP    183.172.224.180:62285  *:*
UDP    [::]:500               *:*
UDP    [::]:4500              *:*
UDP    [::]:5353              *:*
UDP    [::]:5355              *:*
UDP    [::]:49665             *:*
UDP    [::1]:1900             *:*
UDP    [::1]:5353             *:*
UDP    [::1]:62284            *:*
UDP    [fe80::f96d:fd96:66d8:b6b%13]:1900  *:*
UDP    [fe80::f96d:fd96:66d8:b6b%13]:62283  *:*
```

## arp

熟悉 arp 命令的基本用法，了解 IP 地址与物理地址之间的映射关系，查看本机、相邻主机或网关的 IP 地址和物理地址的映射关系

ARP 是一个地址解析协议，其作用是根据 B 的 IP 地址去获取其 MAC 地址。

网络互连首先要解决网络地址到物理地址的映射问题。TCP/IP 协议中，当 A 要向 B 发 IP 包时，需要填写 B 的 IP 为目标地址，但包含 IP 地址的包在以太网传输时还需要进行以太网的包装，由于以太网接口分配的是 48 位的物理地址，不能识别 32 位的 IP 地址，故在以太包中，目标地址为 B 的 MAC 地址。

ARP cache 是用来储存（IP,MAC）地址的缓存区。当主机 A 要与主机 B 通信时，首先根据主机 A 上的路由表内容确定访问主机 B 的 IP 地址 BP，然后 A 主机在自己的本地 ARP 缓存中检查主机 B 的匹配 MAC 地址。如果主机 A 在 ARP 缓存中没有找到映射，它将发送 ARP request 向局域网查询。由于以太网具备广播能力、物理地址固定，主机 A 将包括源主机 AIP 地址和 MAC 地址的 ARP 请求帧广播到本地网络上的所有主机，请求 IP 地址为 BP 的主机回答其物理地址。本地网络上的每台主机都接收到 ARP 请求并且检查是否与自己的 IP 地址匹配。如果主机发现请求的 IP 地址与自己的 IP 地址不匹配，则将丢弃 ARP 请求；若主机 B 确定 ARP 请求中的 IP 地址与自己的 IP 地址匹配，则将主机 A 的 IP 地址和 MAC 地址映射添加到本地 ARP 缓存中，并将包含自身 MAC 地址的 ARP 回复消息直接发送回主机 A。主机 A 收到主机 B 发来的 ARP 回复消息时，用主机 B 的 IP 和 MAC 地址映射更新 ARP 缓存，以备

下次使用。

本机缓存有生存期，生存期结束后会再次重复以上过程。储存在高速 cache 中的 ARP 表，既可以有动态表项，也可以有静态表项，可以通过 arp –s 指令将 IP 地址与 MAC 地址的映射关系手动添加到 ARP 表中。ARP 表在手工配置前通常为动态 ARP 表项，因此表项变动较大，通过该命令加入的是静态表项，系统不会自动删除。使用 arp –d 命令可以删除动态表项与静态表项。

使用 arp –a 命令显示高速 cache 中的 ARP 表：

```
C:\Users\Qingyang Zhong>arp -a

接口: 183.172.225.15 --- 0xd
  Internet 地址         物理地址              类型
  183.172.224.1         90-03-25-b9-7f-05     动态
  183.172.231.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

已知默认网关地址为 183.172.224.1，可见网关的物理地址为 90-03-25-b9-7f-05

# ping

练习使用 ping 命令，测试网络连通性，要求随机测试本机、邻居微机、默认网关、域名服务器、远程网络地址等

ping 127.0.0.1 检测本机的 TCP/IP 协议安装是否正确

```
C:\Users\Qingyang Zhong>ping 127.0.0.1

正在 Ping 127.0.0.1 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128

127.0.0.1 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 = 0ms，最长 = 0ms，平均 = 0ms
```

ping 183.172.225.15（本机 IP）检测本机的服务和网络适配器绑定是否正确

```
C:\Users\Qingyang Zhong>ping 183.172.225.15

正在 Ping 183.172.225.15 具有 32 字节的数据:
来自 183.172.225.15 的回复: 字节=32 时间<1ms TTL=128
来自 183.172.225.15 的回复: 字节=32 时间<1ms TTL=128
来自 183.172.225.15 的回复: 字节=32 时间<1ms TTL=128
来自 183.172.225.15 的回复: 字节=32 时间<1ms TTL=128

183.172.225.15 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 = 0ms，最长 = 0ms，平均 = 0ms
```

ping 183.172.224.1（网关 IP）检测本机和网关连接是否正常

```
C:\Users\Qingyang Zhong>ping 183.172.224.1

正在 Ping 183.172.224.1 具有 32 字节的数据:
来自 183.172.224.1 的回复: 字节=32 时间=1ms TTL=254
来自 183.172.224.1 的回复: 字节=32 时间=1ms TTL=254
来自 183.172.224.1 的回复: 字节=32 时间=1ms TTL=254
来自 183.172.224.1 的回复: 字节=32 时间=1ms TTL=254

183.172.224.1 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 = 1ms, 最长 = 1ms, 平均 = 1ms
```

ping 183.172.195.217（邻居微机 IP）检测能否与邻居微机间传送数据包

```
C:\Users\Qingyang Zhong>ping 183.172.195.217

正在 Ping 183.172.195.217 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

邻居微机无法 ping 通，可能是由于对方主机做了限制，如安装了防火墙等。将双方防火墙关闭，数据包接收成功:

```
C:\Users\Qingyang Zhong>ping 183.172.195.217

正在 Ping 183.172.195.217 具有 32 字节的数据:
来自 183.172.195.217 的回复: 字节=32 时间=82ms TTL=63
来自 183.172.195.217 的回复: 字节=32 时间=92ms TTL=63
来自 183.172.195.217 的回复: 字节=32 时间=110ms TTL=63
来自 183.172.195.217 的回复: 字节=32 时间=22ms TTL=63

183.172.195.217 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 = 22ms, 最长 = 110ms, 平均 = 76ms
```

ping 101.6.244.4（远程主机 IP）检测网关是否能转发数据包

```
C:\Users\Qingyang Zhong>ping 101.6.244.4

正在 Ping 101.6.244.4 具有 32 字节的数据:
来自 101.6.244.4 的回复: 字节=32 时间=3ms TTL=60
来自 101.6.244.4 的回复: 字节=32 时间=2ms TTL=60
来自 101.6.244.4 的回复: 字节=32 时间=1ms TTL=60
来自 101.6.244.4 的回复: 字节=32 时间=2ms TTL=60

101.6.244.4 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 = 1ms, 最长 = 3ms, 平均 = 2ms
```

ping www.bv2008.cn（志愿北京域名）检测 DNS 服务器是否能正常解释

```
C:\Users\Qingyang Zhong>ping www.bv2008.cn

正在 Ping www.bv2008.cn [220.194.54.25] 具有 32 字节的数据:
来自 220.194.54.25 的回复: 字节=32 时间=3ms TTL=52
来自 220.194.54.25 的回复: 字节=32 时间=2ms TTL=52
来自 220.194.54.25 的回复: 字节=32 时间=2ms TTL=52
来自 220.194.54.25 的回复: 字节=32 时间=5ms TTL=52

220.194.54.25 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 = 5ms, 平均 = 3ms
```

所有数据包均接收成功，说明网络连通，网络状况正常。

## tracert

练习使用 tracert 命令,检测到达目的地址 166.111.8.28 所经过的路由器的 IP 地址

从紫荆 8#Tsinghua 无线局域网到 166.111.8.28 所经过的路由器的 IP 地址如下:

```
C:\Users\Qingyang Zhong>tracert 166.111.8.28

通过最多 30 个跃点跟踪
到 dns-a.tsinghua.edu.cn [166.111.8.28] 的路由:

  1     5 ms     2 ms     2 ms  183.172.224.1
  2     1 ms     1 ms     1 ms  172.17.2.25
  3     1 ms     1 ms     1 ms  118.229.2.218
  4     1 ms     1 ms     1 ms  dns-a.tsinghua.edu.cn [166.111.8.28]
```

# 实验思考

1. 在 Internet 上进行网络通信，主机必须包含的基本网络配置有哪些？必须具有哪些地址？

   主机需要包含网络协议、网络服务和网络客户等基本网络配置，必须具有 IP 地址、子网掩码、默认网关地址、DNS 服务器地址和网卡物理地址等地址。

2. 在使用 tracert 命令时，在路由检测的过程中可能会出现“*”，是否一定代表路由不可到达？为什么？

   不一定。tracert 提供从源点到目标点的沿端到端因特网路径的时延测量。从原理上看，源向网络发送 N 个特殊的分组，其中每个分组指向最终目的地。Tracert 利用 ICMP 数据报和 IP 数据报头部中的 TTL 值进行路由检测。TTL 是一个 IP 数据报的生存时间，当每个 IP 数据报经过路由器的时候 TTL 值都会减去 1；当路由器接收到一个 TTL 为 0 或者 1 的 IP 数据报的时候，路由器就将这个数据直接丢弃，并且发送一个 ICMP“超时”信息给源主机，从而使源记录从它发送一个分组到它接收到对应返回报文所经受的时间，与返回该报文的路由器（或目的地主机）的名字和地址。

   若某些路由器不经询问直接自动处理 TTL 过期的数据包，或某些路由器出于安全问题没有返回报文，或分组所选路径出现拥塞产生丢包现象等都可能导致出现“*”结果，若报文在有限时间内没有返回，即使分组没有被丢失，也可能出现“*”结果，因此路由检测的过程中出现“*”，不一定代表路由不可到达。

3. 分别使用 ping -r 和 tracert 检验到 166.111.8.28 所通过的路径，分析到达该目标地址的相关路由，获得的路由信息有何不同？并画出到达目的地址的路径示意图。

   使用 tracert 得到的路径如下:

```
C:\Users\Qingyang Zhong>tracert 166.111.8.28

通过最多 30 个跃点跟踪
到 dns-a.tsinghua.edu.cn [166.111.8.28] 的路由:

  1     4 ms     2 ms     5 ms  183.172.224.1
  2     1 ms     1 ms     1 ms  172.17.2.25
  3     1 ms     1 ms     1 ms  118.229.2.218
  4     1 ms     1 ms     1 ms  dns-a.tsinghua.edu.cn [166.111.8.28]

跟踪完成。
```

使用 ping –r 得到的路径如下（设定记录路由的 count 值为 9）：

```
C:\Users\Qingyang Zhong>ping -r 9 166.111.8.28

正在 Ping 166.111.8.28 具有 32 字节的数据:
来自 166.111.8.28 的回复: 字节=32 时间=10ms TTL=61
    路由: 172.17.2.26 ->
          118.229.2.217 ->
          166.111.8.1 ->
          166.111.8.28 ->
          166.111.8.28 ->
          118.229.2.218 ->
          172.17.2.25 ->
          183.172.224.1
来自 166.111.8.28 的回复: 字节=32 时间=11ms TTL=61
    路由: 172.17.2.26 ->
          118.229.2.217 ->
          166.111.8.1 ->
          166.111.8.28 ->
          166.111.8.28 ->
          118.229.2.218 ->
          172.17.2.25 ->
          183.172.224.1
来自 166.111.8.28 的回复: 字节=32 时间=5ms TTL=61
    路由: 172.17.2.26 ->
          118.229.2.217 ->
          166.111.8.1 ->
          166.111.8.28 ->
          166.111.8.28 ->
          118.229.2.218 ->
          172.17.2.25 ->
          183.172.224.1
来自 166.111.8.28 的回复: 字节=32 时间=8ms TTL=61
    路由: 172.17.2.26 ->
          118.229.2.217 ->
          166.111.8.1 ->
          166.111.8.28 ->
          166.111.8.28 ->
          118.229.2.218 ->
          172.17.2.25 ->
          183.172.224.1

166.111.8.28 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 = 5ms, 最长 = 11ms, 平均 = 8ms
```

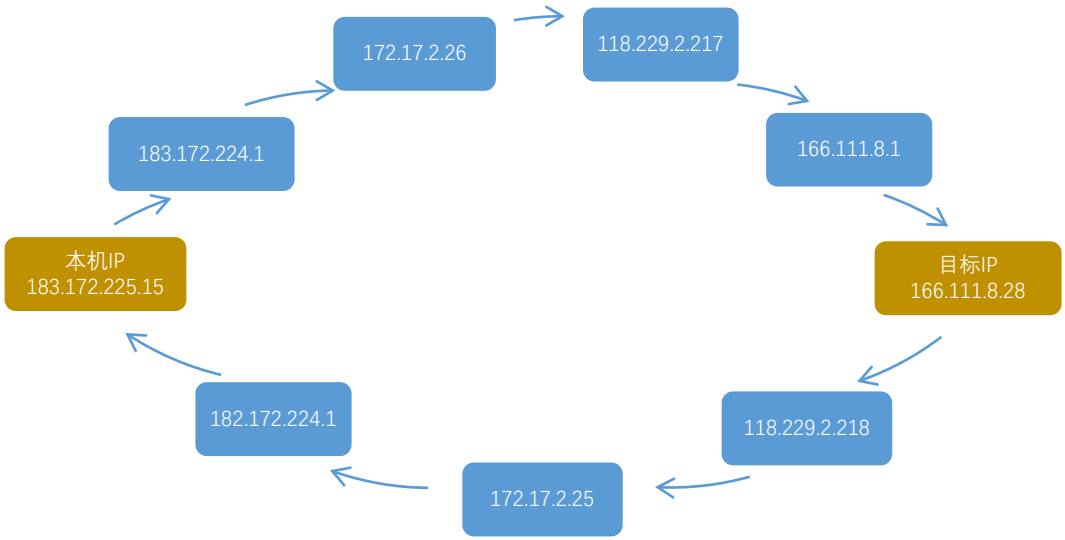
tracert 用于探测路由的程序，利用 ICMP 数据报和 IP 数据报头部中的 TTL 值进行路由检测。获得的路由信息是源从每次发送 3 组报文到接收对应返回报文所各自经受的时间与 IP 数据报到达目的地经过的路由。

ping 用于检测目标主机是否可连通。工作原理上，ping 发送一个 ICMP 回显请求报文给目的主机，等待回显的 ICMP 应答并打印回显的报文。获得的路由信息包括字节数、反应时间、以及生存时间。ping –r count 在“记录路由”的字段中记录发出报文和返回报文的路由。

不同点在于 ping 获得的路由信息包括发出报文和返回报文的路由；ping 与 tracert 中 ICMP 数据包所走的线路可能不完全相同。

tracert 到达目的地址的路径示意图如下：


ping-r 到达目的地址的路径示意图如下：




4. 实验中还出现了哪些你认为不该出现的或不能解释的现象，你是如何分析和理解的？

1） ping 过程中追踪的路由 IP 中 166.111.8.28 出现两次

对比路由器地址发现，重复的路由器地址是目标地址，结合 tracert 得到的路由信息可以看出 ping 返回路径中经过的路由器与 tracert 经过的路由器重叠。由于 ping –r count 在“记录路由”的字段中记录发出报文和返回报文的全部路由，因而目标 IP 理应出现两次。

2）tracert 的追踪过程中 TTL=n 分组返回报文用时比 TTL=n+1 分组用时更长

```
C:\Users\Qingyang Zhong>tracert 166.111.8.28

通过最多 30 个跃点跟踪
到 dns-a.tsinghua.edu.cn [166.111.8.28] 的路由:

  1     4 ms     2 ms     5 ms  183.172.224.1
  2     1 ms     1 ms     1 ms  172.17.2.25
  3     1 ms     1 ms     1 ms  118.229.2.218
  4     1 ms     1 ms     1 ms  dns-a.tsinghua.edu.cn [166.111.8.28]

跟踪完成。
```

由于 tracert 提供的是因特网路径的实时时延测量，不同分组间存在时间间隔且所走路径也可能完全不同，选择不同路径、网络状况不稳定时即会存在该现象。

# 实验总结

通过本次实验，我练习了网络常用命令，学会了使用 ipconfig、ping、tracert、arp、netstat、nbtstat 等工具，对网络地址、子网掩码、域名、网关、路由、地址解析、协议和端口等基本概念有了更深入的理解；通过查看和测试网络状态，掌握了发现和解决网络可能存在的问题的基本方法，为今后计算机网络课程的学习打下了良好基础。