计算机网络实验报告

警示

1. **实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。**
2. **当次小组成员成绩只计学号、姓名登录在下表中的。**
3. **在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。**
4. **实验报告文件以 PDF 格式提交。**

专业	计算机科学与技术（超算）	班 级	行政 3 班
学号	19335074		
学生	黄玟瑜		

基本命令与操作

实验内容

实验 1~7

- **ping 命令**
  - 网络连通性 echo
  - 最常用形式：“ping IP 地址”或“ping 域名”

```
C:\>ping/?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

实例：

```
C:\>ping www.sohu.com

Pinging fgzyd.a.sohu.com [183.240.112.16] with 32 bytes of data:
Reply from 183.240.112.16: bytes=32 time=10ms TTL=52
Reply from 183.240.112.16: bytes=32 time=18ms TTL=52
Reply from 183.240.112.16: bytes=32 time=18ms TTL=52
Reply from 183.240.112.16: bytes=32 time=19ms TTL=52

Ping statistics for 183.240.112.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 19ms, Average = 16ms
```

```
C:\>ping 183.240.112.16

Pinging 183.240.112.16 with 32 bytes of data:
Reply from 183.240.112.16: bytes=32 time=9ms TTL=52
Reply from 183.240.112.16: bytes=32 time=10ms TTL=52
Reply from 183.240.112.16: bytes=32 time=9ms TTL=52
Reply from 183.240.112.16: bytes=32 time=9ms TTL=52

Ping statistics for 183.240.112.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms
```

bytes 值：数据包大小，也就是字节。

time 值：响应时间，这个时间越小，说明你连接这个地址速度越快。

TTL 值：Time To Live,表示 DNS 记录在 DNS 服务器上存在的时间，它是 IP 协议包的一个值，告诉路由器该数据包何时需要被丢弃。

```
C:\>ping www.sysu.edu.cn -t

Pinging pisces-1.sysu.edu.cn [2001:250:3002:10::8] with 32 bytes of data:
Reply from 2001:250:3002:10::8: time=3ms
Reply from 2001:250:3002:10::8: time=2ms
Reply from 2001:250:3002:10::8: time=4ms
Reply from 2001:250:3002:10::8: time=4ms
Reply from 2001:250:3002:10::8: time=8ms
Reply from 2001:250:3002:10::8: time=5ms
Reply from 2001:250:3002:10::8: time=5ms
Reply from 2001:250:3002:10::8: time=15ms
Reply from 2001:250:3002:10::8: time=5ms
Reply from 2001:250:3002:10::8: time=9ms
Reply from 2001:250:3002:10::8: time=4ms
Reply from 2001:250:3002:10::8: time=7ms
Reply from 2001:250:3002:10::8: time=4ms
Reply from 2001:250:3002:10::8: time=5ms
Reply from 2001:250:3002:10::8: time=6ms
Reply from 2001:250:3002:10::8: time=6ms
Reply from 2001:250:3002:10::8: time=3ms

2001:250:3002:10::8 的 Ping 统计信息:
    数据包: 已发送 = 17, 已接收 = 17, 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 = 15ms, 平均 = 5ms
Control-C
```

ping-t 的使用：不间断地 ping 指定计算机，知道管理员中断，按住键盘的 Ctrl+c 终止它继续 ping 下去，这说明电脑连接路由器是通的，网络效果好。

```
C:\>ping -r 6 -l 200 172.18.187.254

Pinging 172.18.187.254 with 200 bytes of data:
Reply from 172.18.187.254: bytes=200 time=13ms TTL=252
    Route: 10.44.36.202 ->
           10.44.32.201 ->
           10.44.185.201 ->
           172.18.187.254 ->
           10.44.32.202 ->
           10.44.36.201
Reply from 172.18.187.254: bytes=200 time=9ms TTL=252
    Route: 10.44.36.202 ->
           10.44.32.201 ->
           10.44.185.201 ->
           172.18.187.254 ->
           10.44.32.202 ->
           10.44.36.201
Reply from 172.18.187.254: bytes=200 time=9ms TTL=252
    Route: 10.44.36.202 ->
           10.44.32.201 ->
           10.44.185.201 ->
           172.18.187.254 ->
           10.44.32.202 ->
           10.44.36.201
Reply from 172.18.187.254: bytes=200 time=80ms TTL=252
    Route: 10.44.36.202 ->
           10.44.32.201 ->
           10.44.185.201 ->
           172.18.187.254 ->
           10.44.32.202 ->
           10.44.36.201

Ping statistics for 172.18.187.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 80ms, Average = 27ms
```

-r count：Record route for count hops (IPv4-only).

-l size：发送 size 指定大小的到目标主机的数据包。

记录下所经过的 6 个路由器的线路。发送大小为 200 的数据包到目标主机。

```
C:\>ping -s 4 -l 200 172.18.187.254

Pinging 172.18.187.254 with 200 bytes of data:
Reply from 172.18.187.254: bytes=200 time=71ms TTL=252
    Timestamp: 172.19.63.254 : 39687054 ->
               10.44.36.201 : 68486235 ->
               10.44.32.202 : 68486231 ->
               10.44.185.202 : 39686230
Reply from 172.18.187.254: bytes=200 time=55ms TTL=252
    Timestamp: 172.19.63.254 : 39688052 ->
               10.44.36.201 : 68487235 ->
               10.44.32.202 : 68487231 ->
               10.44.185.202 : 39687230
Reply from 172.18.187.254: bytes=200 time=8ms TTL=252
    Timestamp: 172.19.63.254 : 39689055 ->
               10.44.36.201 : 68488235 ->
               10.44.32.202 : 68488231 ->
               10.44.185.202 : 39688230
Reply from 172.18.187.254: bytes=200 time=11ms TTL=252
    Timestamp: 172.19.63.254 : 39690076 ->
               10.44.36.201 : 68489255 ->
               10.44.32.202 : 68489251 ->
               10.44.185.202 : 39689250

Ping statistics for 172.18.187.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 71ms, Average = 36ms
```

发送大小为 200 的数据包到目标主机，同时记录下 4 个路由器的时间戳。

- **tracert 命令**

  - tracert（跟踪路由）是路由跟踪实用程序

  - 用于获得 IP 数据报访问目标时从本地计算机到目的主机的路径信息。

  - 最常用形式：“tracert IP 地址”或“tracert 域名”

```
C:\>tracert/?

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

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

```
C:\>tracert www.sina.com

Tracing route to spool.grid.sinaedge.com [2409:8c34:2000:2::17:73]
over a maximum of 30 hops:

  1    13 ms    11 ms    10 ms  2001:250:3002:4240::1
  2     4 ms     2 ms     4 ms  fd44:1024::ff01
  3     5 ms     4 ms     5 ms  fd04:110::ff01
  4     6 ms     6 ms     5 ms  fd00:110::ff02
  5     8 ms     8 ms     8 ms  cernet2.net [2001:da8:a2:102::1]
  6     5 ms    11 ms     3 ms  cernet2.net [2001:da8:a2:11::1]
  7     6 ms     4 ms     4 ms  2001:da8:2:104::1
  8    17 ms    15 ms    16 ms  2001:da8:2:17::2
  9    34 ms    31 ms    62 ms  2001:da8:2:2b::1
 10    38 ms    38 ms    39 ms  2001:da8:2:13::1
 11    53 ms    52 ms    51 ms  2001:da8:2:703::2
 12    52 ms    49 ms    53 ms  2409:8080:0:3:2e1:283::
 13    52 ms    49 ms    50 ms  2409:8080:0:1:204:2e1:1:0
 14    62 ms    52 ms    62 ms  2409:8080:1:2:204:204:0:1
 15    97 ms   175 ms   162 ms  2409:8080:1:2:204:1002:1:1
 16   167 ms    90 ms   136 ms  2409:8080:1:2:1002:1072:0:1
 17    99 ms   153 ms    89 ms  2409:8034:0:263::1
 18    97 ms   103 ms   103 ms  2409:8034:3002:101::1
 19   217 ms   202 ms   207 ms  2409:8034:3012:501::1
 20   185 ms   141 ms   192 ms  2409:8c34:2000:2::17:73

Trace complete.
```

从左到右的 5 条信息分别代表了“生存时间”(每途经一个路由器结点自增 1)、“三次发送的 ICMP 包返回时间”（共计 3 个，单位为毫秒 ms）和“途经路由器的 IP 地址”（如果有主机名，还会包含主机名)。

```
C:\>tracert -d 172.16.0.88

Tracing route to 172.16.0.88 over a maximum of 30 hops

  1     *        *        *     Request timed out.
  2     3 ms     7 ms     4 ms  10.44.36.201
  3     5 ms     7 ms     3 ms  10.44.16.201
  4    18 ms    25 ms     9 ms  10.10.1.142
  5     9 ms     7 ms     9 ms  10.20.30.10
  6    10 ms     7 ms     8 ms  10.33.67.201
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
```

-d：不将地址解析为主机名。

➢ ipconfig 命令

- ipconfig 命令可以显示所有当前的 TCP/IP 网络配置值（如 IP 地址、网关、子网掩码）
  - 刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。
- 最常用形式：“ipconfig”或“ipconfig /all”

```
C:\>ipconfig

Windows IP Configuration


Wireless LAN adapter 本地连接* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter 本地连接* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d024:63da:9140:105e%7
   IPv4 Address. . . . . . . . . . . : 192.168.157.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2473:7526:1379:67c2%19
   IPv4 Address. . . . . . . . . . . : 192.168.136.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter WLAN:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:250:3002:4240:64:9f67:2fa8:ef03
   Temporary IPv6 Address. . . . . . : 2001:250:3002:4240:d973:aebd:45e5:202e
   Link-local IPv6 Address . . . . . : fe80::64:9f67:2fa8:ef03%10
   IPv4 Address. . . . . . . . . . . : 172.19.8.183
   Subnet Mask . . . . . . . . . . . : 255.255.192.0
   Default Gateway . . . . . . . . . : fe80::a68:8dff:fea5:1e01%10
                                       172.19.63.254

Ethernet adapter 蓝牙网络连接:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

显示所有适配器的基本 TCP/IP 配置，它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。

```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-KKCUJPTB
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter 本地连接* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3

   Physical Address. . . . . . . . . : 0C-DD-24-1E-9C-46
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter 本地连接* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4

   Physical Address. . . . . . . . . : 0E-DD-24-1E-9C-45
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet
1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d024:63da:9140:105e%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.157.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 2021年3月9日 18:52:44
   Lease Expires . . . . . . . . . . : 2021年3月9日 19:52:44
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.157.254
   DHCPv6 IAID . . . . . . . . . . . : 671109206
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-E1-7D-1E-0C-DD-24-1E-9C-45
```

显示所有适配器的完整 TCP/IP 配置，为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等）。

- **netstat 命令**

netstat 命令可以显示：

1. 当前活动的 TCP 连接
2. 计算机侦听的端口
3. 以太网统计信息
4. IP 路由表
5. IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议）
6. IPv6 统计信息

```
C:\>netstat/?

Displays protocol statistics and current TCP/IP network connections.

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

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:6646           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4301         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:28317        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:44440        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:44440        127.0.0.1:55421        ESTABLISHED
  TCP    127.0.0.1:49669        127.0.0.1:49674        ESTABLISHED
  TCP    127.0.0.1:49674        127.0.0.1:49669        ESTABLISHED
  TCP    127.0.0.1:50041        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:50041        127.0.0.1:55721        ESTABLISHED
  TCP    127.0.0.1:55421        127.0.0.1:44440        ESTABLISHED
  TCP    127.0.0.1:55721        127.0.0.1:50041        ESTABLISHED
  TCP    127.0.0.1:61978        0.0.0.0:0              LISTENING
  TCP    172.19.8.183:139       0.0.0.0:0              LISTENING
  TCP    172.19.8.183:53576     121.46.19.36:443       ESTABLISHED
  TCP    172.19.8.183:53626     120.204.10.154:443     CLOSE_WAIT
  TCP    172.19.8.183:60376     120.226.1.140:443      CLOSE_WAIT
  TCP    172.19.8.183:60626     36.152.44.205:443      CLOSE_WAIT
  TCP    172.19.8.183:60632     120.241.147.161:443    TIME_WAIT
  TCP    172.19.8.183:60633     54.186.175.197:443     CLOSE_WAIT
  TCP    172.19.8.183:60634     168.62.200.169:443     TIME_WAIT
  TCP    172.19.8.183:60643     104.208.16.0:443       ESTABLISHED
  TCP    172.19.8.183:60646     36.152.44.205:443      ESTABLISHED
  TCP    172.19.8.183:64420     117.184.242.106:8080   ESTABLISHED
  TCP    172.19.8.183:64426     40.119.211.203:443     ESTABLISHED
  TCP    172.19.8.183:64431     40.119.211.203:443     ESTABLISHED
```

显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。

```
C:\>netstat -e -s
Interface Statistics

                           Received            Sent

Bytes                    2637990532       131515618
Unicast packets             2971192          842614
Non-unicast packets         1412352           60996
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

IPv4 Statistics

  Packets Received                   = 447579
  Received Header Errors             = 0
  Received Address Errors            = 33
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 3158
  Received Packets Delivered         = 469670
  Output Requests                    = 123506
  Routing Discards                   = 0
  Discarded Output Packets           = 3098
  Output Packet No Route             = 118
  Reassembly Required                = 2
  Reassembly Successful              = 1
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

IPv6 Statistics

  Packets Received                   = 57991
  Received Header Errors             = 0
  Received Address Errors            = 11
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 71102
  Output Requests                    = 54075
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 9
```

显示以太网统计信息，如发送和接收的字节数、数据包数。

```
C:\>netstat -ano -p tcp | find "3389" >nul 2>nul && echo 3389端口已开启 || echo 3389未开启
3389未开启
```

由查询结果可知 3389 未开启

- **arp 命令**

ARP 把 IP 地址解析成 LAN 硬件使用的媒体访问控制地址，用于显示和修改“地址解析协议（ARP）”缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则 ARP 命令将显示帮助信息。

```
C:\>arp/?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

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

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

```
C:\>arp -a

Interface: 192.168.157.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.157.254       00-50-56-f1-02-d2     dynamic
  192.168.157.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.19.8.183 --- 0xa
  Internet Address      Physical Address      Type
  172.19.63.254         08-68-8d-a5-1e-01     dynamic
  172.19.63.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.136.1 --- 0x13
  Internet Address      Physical Address      Type
  192.168.136.254       00-50-56-ee-f9-8a     dynamic
  192.168.136.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

所有接口的 ARP 缓存表

```
C:\>arp -a -N 172.19.8.183

Interface: 172.19.8.183 --- 0xa
  Internet Address      Physical Address      Type
  172.19.63.254         08-68-8d-a5-1e-01     dynamic
  172.19.63.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

显示 IP 地址为 172.19.8.183 的接口 ARP 缓存表，该表和上图中的对应信息一致。

```
C:\>arp -s 172.19.63.254 08-68-8d-a5-1e-01
```

将 IP 地址 172.19.63.254 与物理地址 08-68-8d-a5-1e-01 绑定(静态 ARP 缓存项)，此项操

作需要管理员权限。

- **route 命令**

Route 命令可以在数据包没有有效传递的情况下，利用 route 命令查看路由表

```
C:\>route print
===========================================================================
Interface List
  4...0c dd 24 1e 9c 46 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 15...0e dd 24 1e 9c 45 ......Microsoft Wi-Fi Direct Virtual Adapter #4
  7...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 19...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 10...0c dd 24 1e 9c 45 ......Intel(R) Wireless-AC 9560 160MHz
  3...0c dd 24 1e 9c 49 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.19.63.254     172.19.8.183     45
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
       172.19.0.0    255.255.192.0         On-link      172.19.8.183    301
     172.19.8.183  255.255.255.255         On-link      172.19.8.183    301
    172.19.63.255  255.255.255.255         On-link      172.19.8.183    301
    192.168.136.0    255.255.255.0         On-link     192.168.136.1    291
    192.168.136.1  255.255.255.255         On-link     192.168.136.1    291
  192.168.136.255  255.255.255.255         On-link     192.168.136.1    291
    192.168.157.0    255.255.255.0         On-link     192.168.157.1    291
    192.168.157.1  255.255.255.255         On-link     192.168.157.1    291
  192.168.157.255  255.255.255.255         On-link     192.168.157.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.19.8.183    301
        224.0.0.0        240.0.0.0         On-link     192.168.157.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.136.1    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.19.8.183    301
  255.255.255.255  255.255.255.255         On-link     192.168.157.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.136.1    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 10    301 ::/0                     fe80::a68:8dff:fea5:1e01
  1    331 ::1/128                  On-link
 10    301 2001:250:3002:4240::/64  On-link
 10    301 2001:250:3002:4240:64:9f67:2fa8:ef03/128
```

```
                                    On-link
 10    301 2001:250:3002:4240:d973:aebd:45e5:202e/128
                                    On-link
 10    301 fe80::/64                 On-link
  7    291 fe80::/64                 On-link
 19    291 fe80::/64                 On-link
 10    301 fe80::64:9f67:2fa8:ef03/128
                                    On-link
 19    291 fe80::2473:7526:1379:67c2/128
                                    On-link
  7    291 fe80::d024:63da:9140:105e/128
                                    On-link
  1    331 ff00::/8                  On-link
 10    301 ff00::/8                  On-link
  7    291 ff00::/8                  On-link
 19    291 ff00::/8                  On-link
===========================================================================
Persistent Routes:
  None
```

以上为 IP 路由表的完整内容。

```
C:\>route print 10.*
===========================================================================
Interface List
  4...0c dd 24 1e 9c 46 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 15...0e dd 24 1e 9c 45 ......Microsoft Wi-Fi Direct Virtual Adapter #4
  7...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 19...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 10...0c dd 24 1e 9c 45 ......Intel(R) Wireless-AC 9560 160MHz
  3...0c dd 24 1e 9c 49 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
  None
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
  None
Persistent Routes:
  None
```

以上为 IP 路由表中以 10. 开始的路由，该表和上图中的对应信息一致。

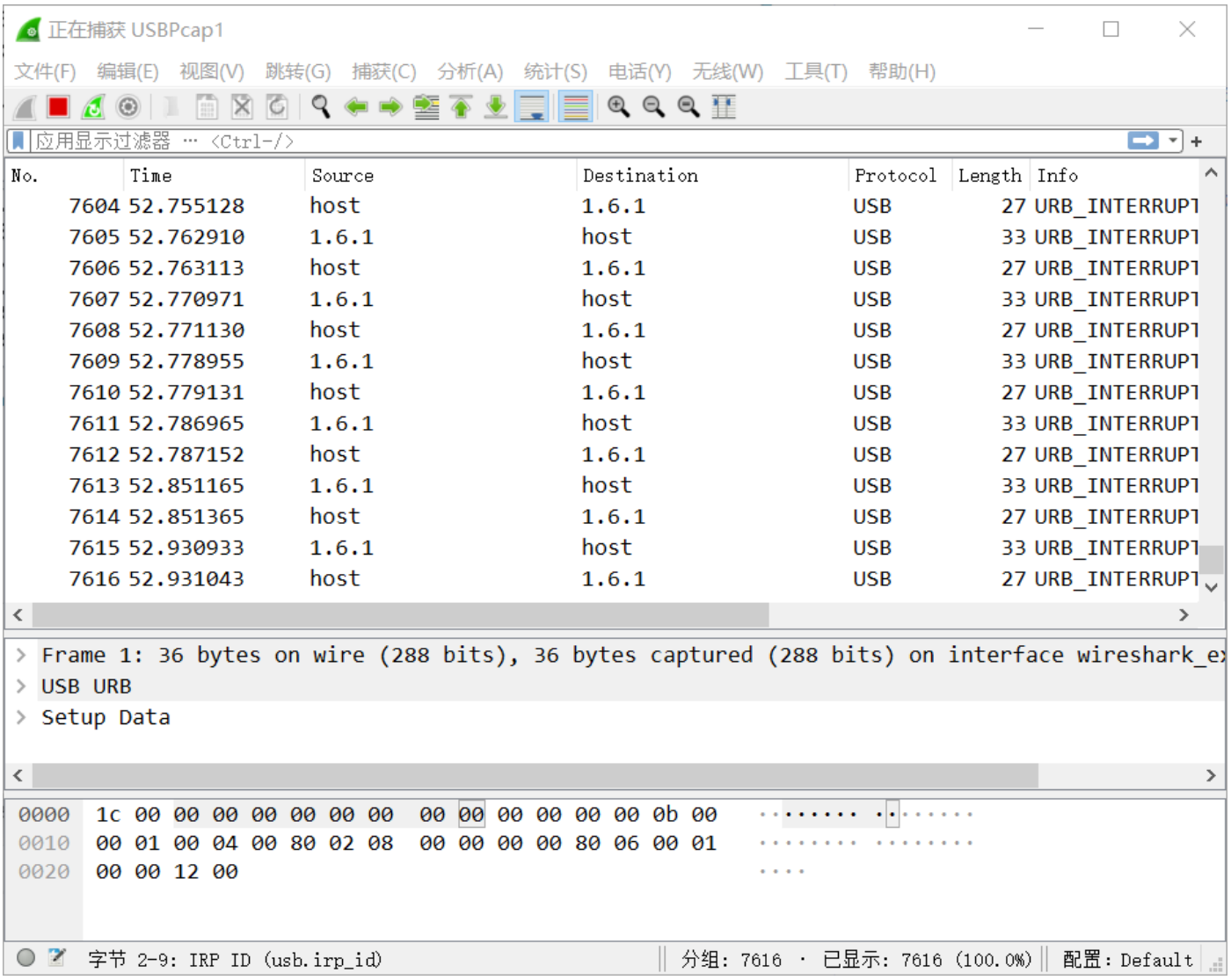
计算机网络实验报告

实验 9

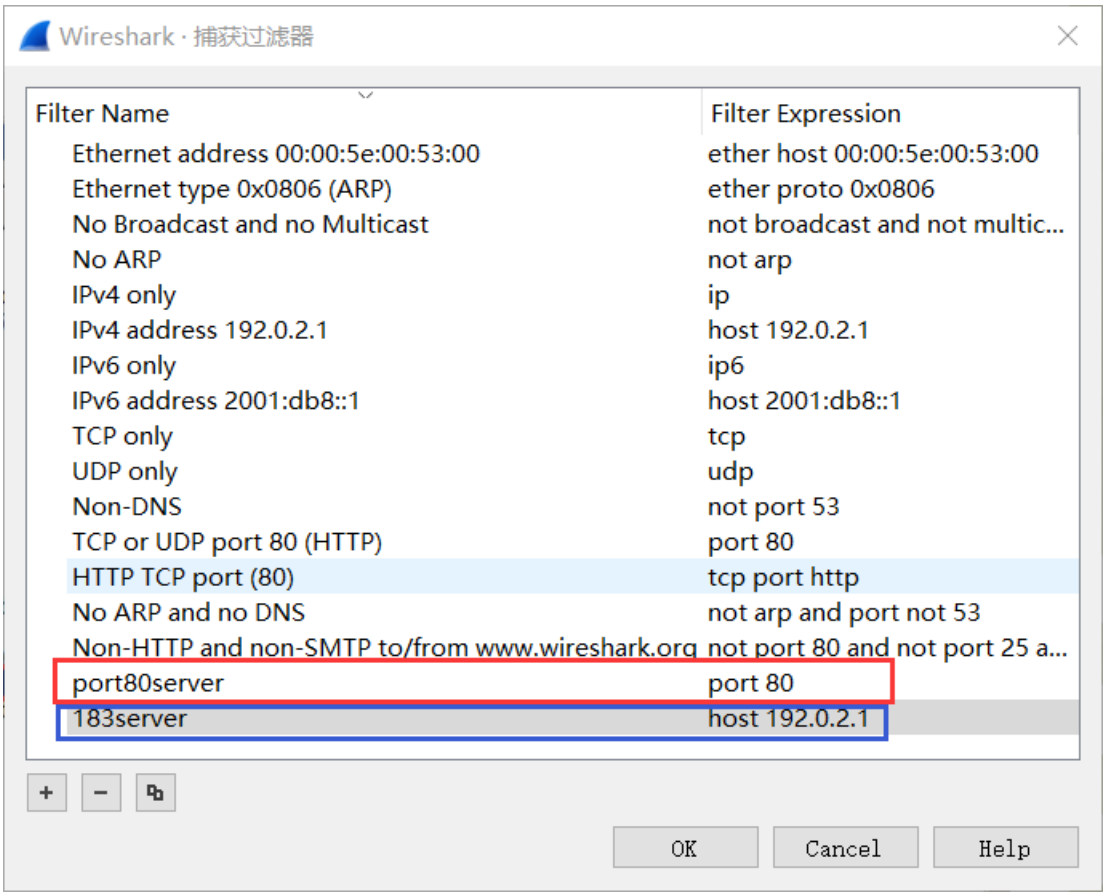
网络协议分析软件

使用 wireshark 捕获数据

数据包捕获实例：



分为七列，分别表示：编号（编号不会发生改变）、时间戳、源 IP、目的 IP、最高层协议、分组长度、附加信息。



左边是捕获过滤器名称，右边是捕获过滤器规则，图中过滤规则分别为：

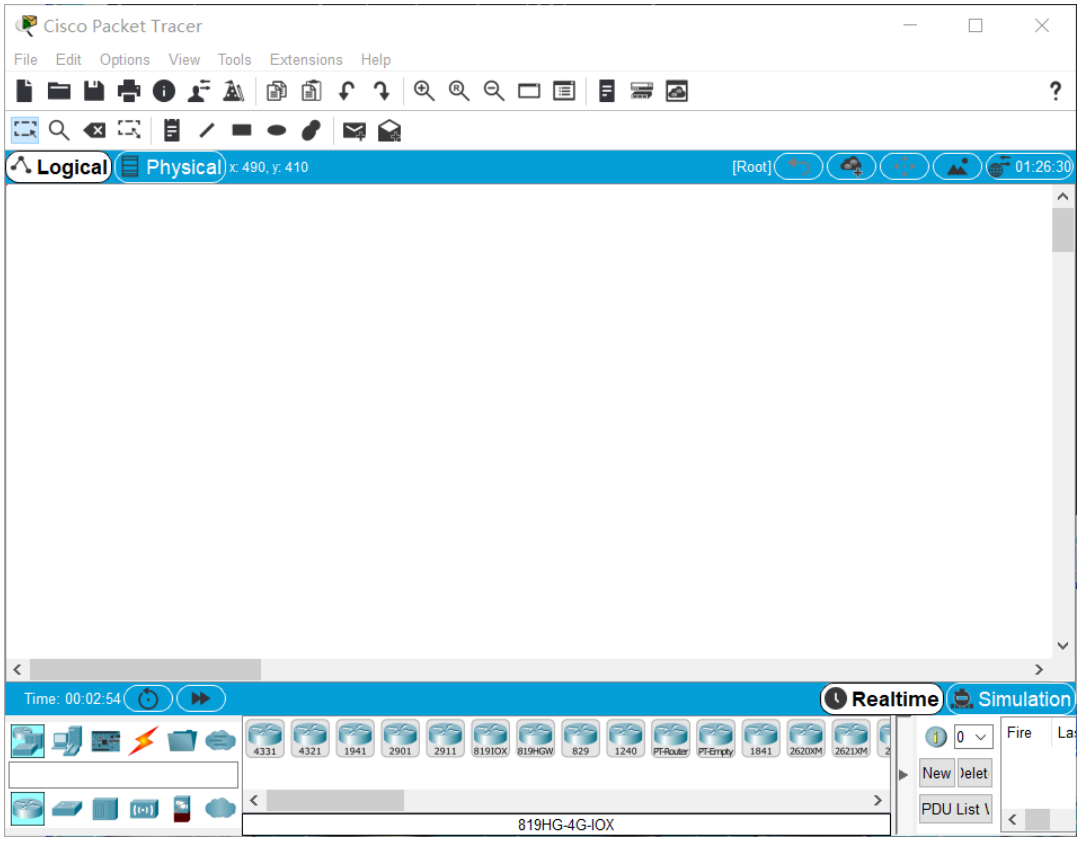
1、根据端口号去过滤：port 80

2、根据 ip 去过滤：host 192.0.2.1

网络模拟软件

使用 Packet Tracer 实时、仿真两个操作模式呈现网络的行为

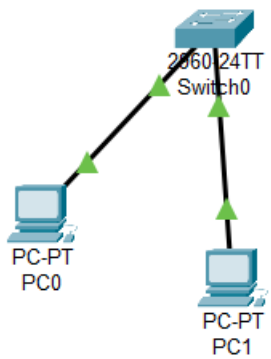
计算机网络实验报告



Packet Tracer 页面

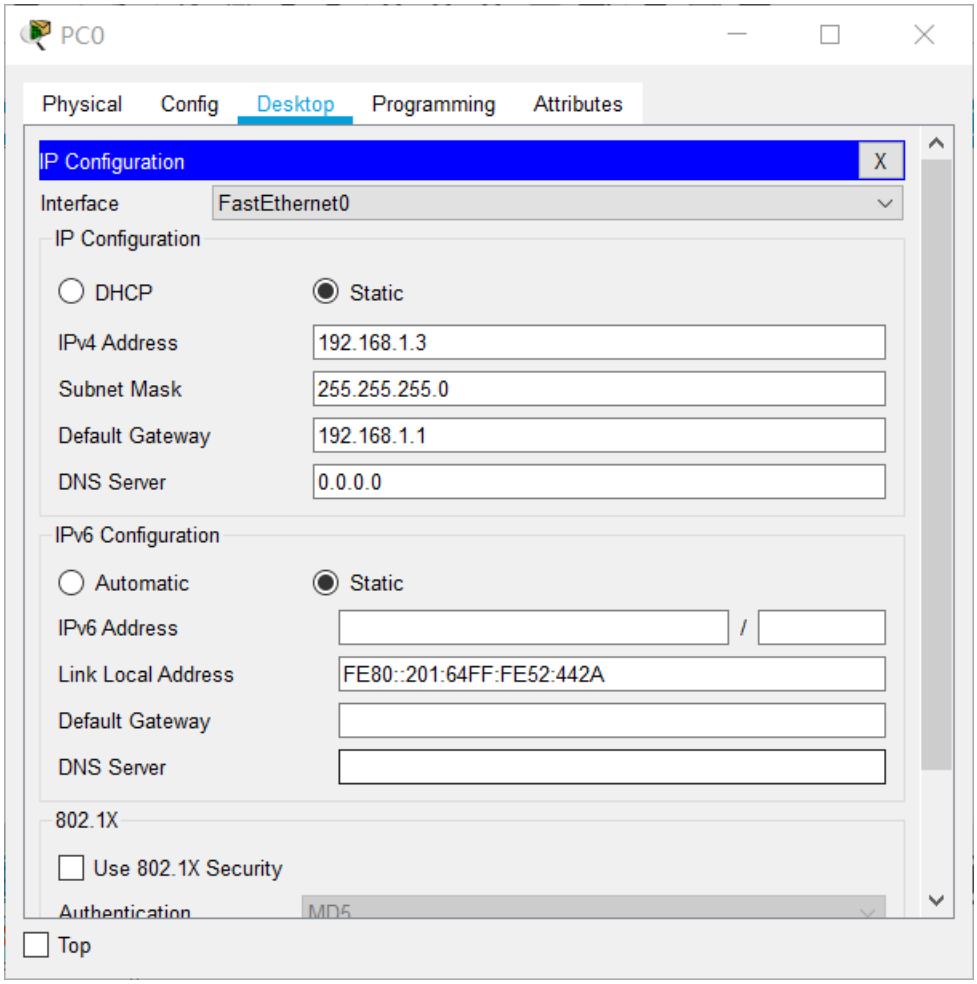
实时模式

1.选择交换机和端设备，一台交换机和两台 PC：Switch0 和 PC0、PC1，并选择连接选项，将端设备和交换机相连



2. 配置相关参数

点击 PC0，进入 PC0 窗口，选择 Desktop 选项卡，选择 IP Configuration，设置参数如下：



PC1 同理，参数如下：

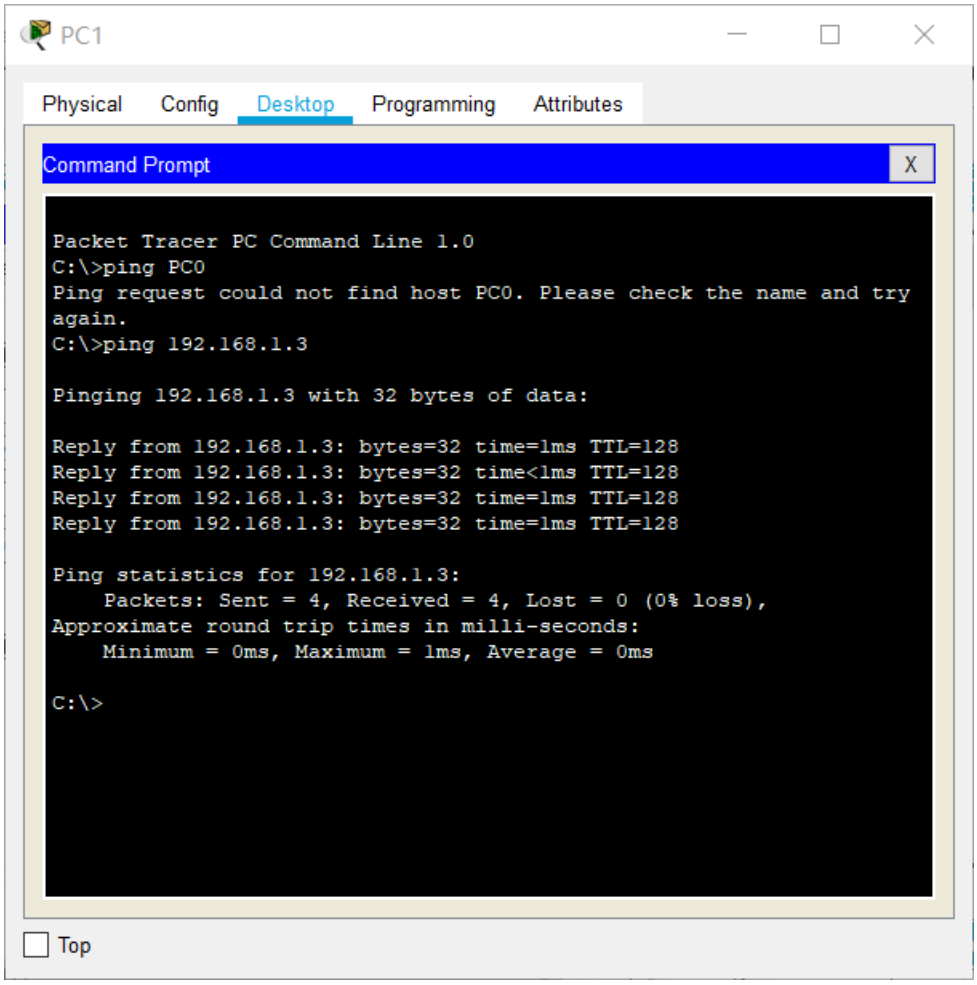
IP: 192.168.1.2

Submask: 255.255.255.0

Gateway: 192.168.1.1

3.使用 PC1 ping PC0

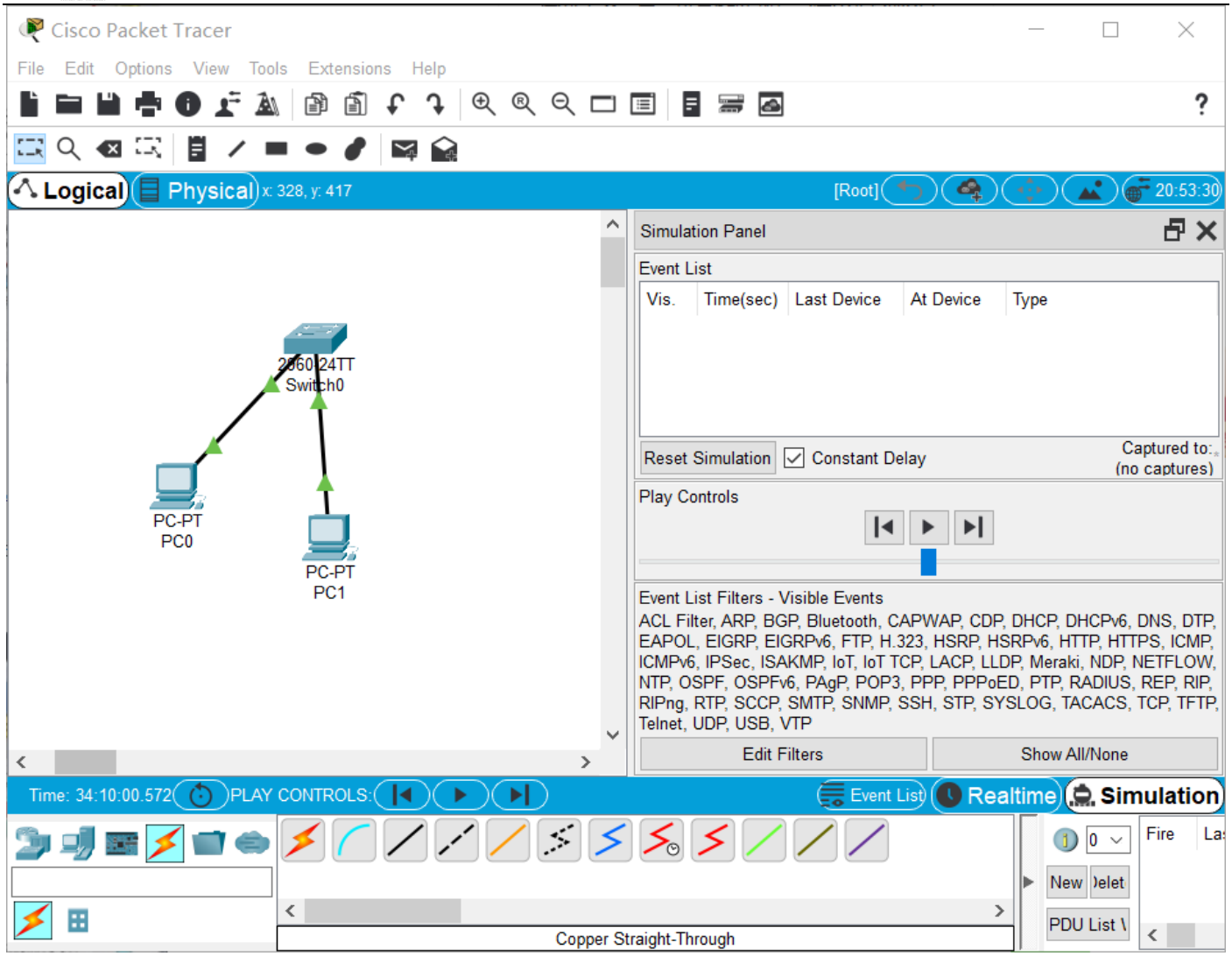
点击 PC1，进入 PC1 窗口，选择 Desktop 选项卡，选择 Command Prompt，输入命令：



仿真模式

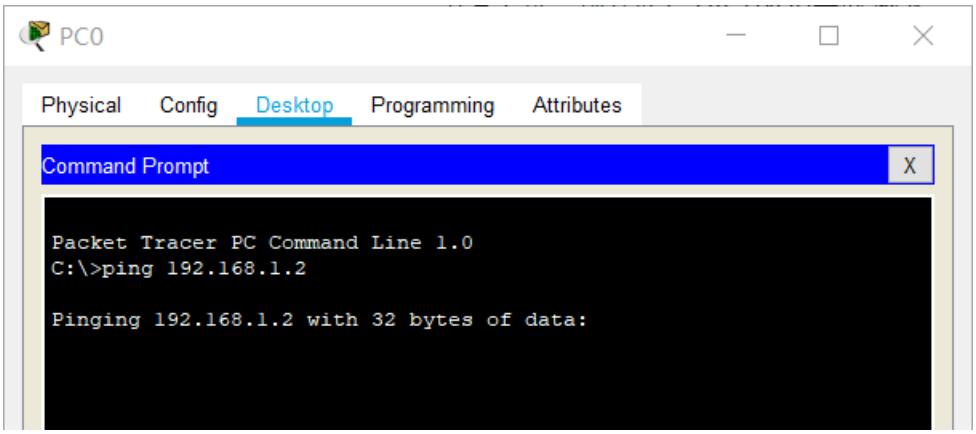
4. 注意到软件界面的右下角有两个按钮，分别是 Realtime mode(实时模式)和 Simulation mode（仿真模式）的切换按钮。将模式切换到仿真模式

计算机网络实验报告



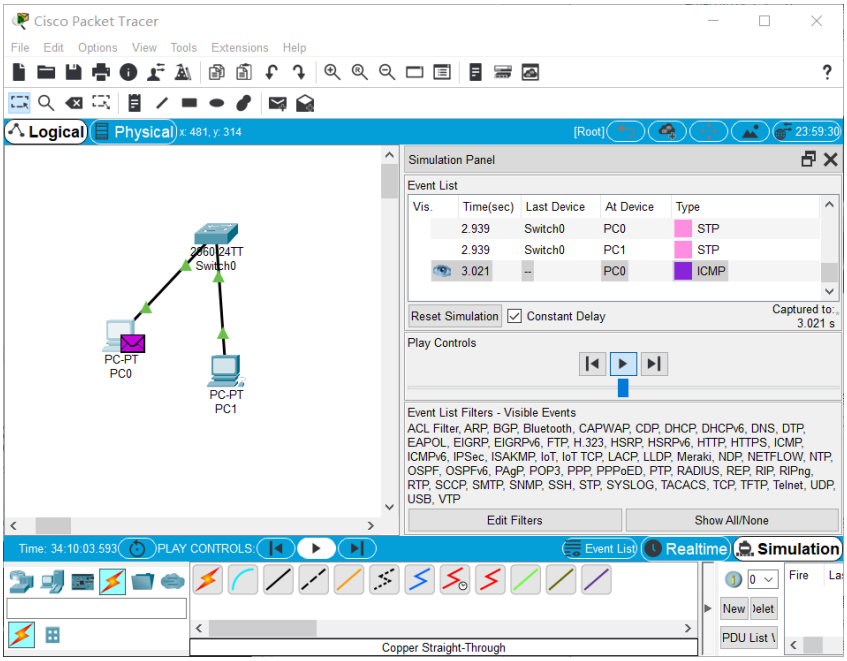
5.在仿真模式下使用 PC0 ping PC1

可以看到输入命令后 ping 包在命令窗口静止不动，需要在操作窗口点击 Auto Capture / Paly (自动捕获)。



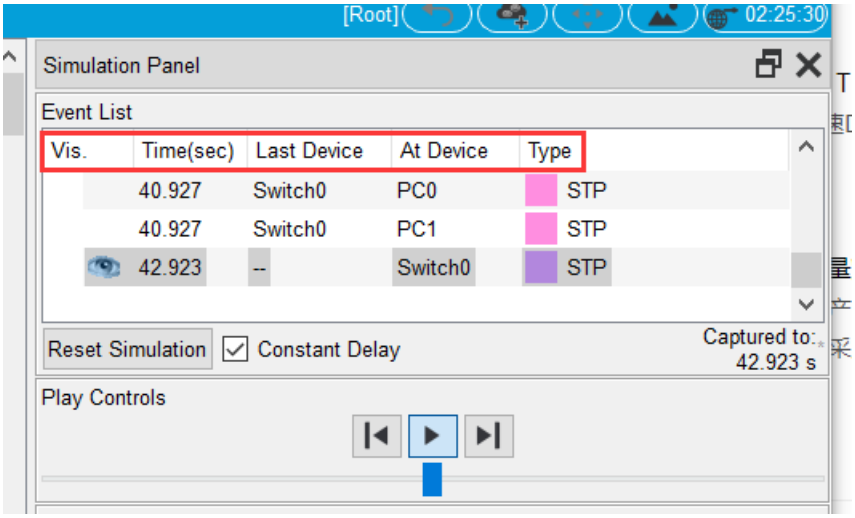
- 看到在拓扑图上有一个信封样子的数据包，以动画的形式传输

1615337246515.mp4



过程截图

图中，5 个选项依次表示在图中运动的可视数据包、所用时间、数据包路过的上一个设备、数据包现所在的设备和数据包类型。



计算机网络实验报告

实验感想

在本次实验中，我学会了一些基本指令于操作，还对 Wireshark 和 Packet Tracer 的使用有了大致的了解。在前 7 个实验中，对 ping 命令、tracert 命令、ipconfig 命令、netstat 命令 、arp 命令和 route 命令分别进行了了解和使用，了解了各条指令的功能，通过帮助功能查询到各个参数的功能和设置的格式，并通过实践调用各个命令进一步熟悉，同时分析结果，相信这些知识对以后的实验会有帮助。

通过教材和互联网上的资料，我对 Wireshark 的使用方法有了基本的了解，学会了用 Wireshark 来抓取数据包，包括一些过滤条件的设置、如何分析各个信息栏所表示的内容等等；通过对 Cisco Packet Tracer 的使用，我学会了如何在实时模式下和仿真模式下进行网络模拟，学会了选择设备、设备间连线的方法、设备的参数设置（如 IP Configuration 的设置）等等；对这些工具的使用有了基本的了解，相信在以后的实验中会进一步熟悉，并能够熟练运用。