
实验一 网络服务与配置

1、实验目的

- (1) 了解 OSI 参考模型的层次结构和工作原理。
- (2) 了解 TCP/IP 协议簇的体系结构以及它和 OSI 参考模型的对应关系。
- (3) 了解 IP 协议的基本工作原理。
- (4) 了解 TCP 和 UDP 协议的基本工作原理。
- (5) 了解 ARP 和 ICMP 协议的基本原理。
- (6) 学习使用 netstat 命令查看 IP、TCP、UDP 和 ICMP 协议的统计信息。
- (7) 学习管理和维护本地 ARP 表。
- (8) 学习使用 ping 命令检测远程计算机的在线状态。

2、实验器材

装有系统的计算机；


3、实验内容

- (1) 掌握 ipconfig 命令的含义；
- (2) 掌握 ping 命令的含义；
- (3) 理解 Netstat 命令的含义与应用；
- (4) 理解 tracert 命令的含义与应用；
- (5) 理解 nslookup 命令的含义与应用；
- (6) 理解 ARP 命令的含义与应用；
- (7) 理解 Telnet 的含义与应用；

3.1 ipconfig/all命令的使用

注释：ipconfig 命令是我们经常使用的命令，它可以查看网络连接的情况，比如本机的 ip 地址，子网掩码，dns 配置，dhcp 配置等等 /all 参数就是显示所有配置的参数。

在“开始”——“运行”弹出的对话框中输入“cmd”回车，弹出

 C:\WINDOWS\system32\cmd.exe 窗口，然后输入“ipconfig/all”回车。

```
C:\WINDOWS\system32\cmd.exe
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : LUOB0-1598F5D24
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . :
    Description . . . . . : VIA Rhine II Fast Ethernet Adapter
    Physical Address. . . . . : 00-0D-87-14-76-3E
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.28.98
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 192.168.28.1
    DNS Servers . . . . . : 202.102.128.68
                           202.102.134.68

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

图 1 ipconfig /all 的显示结果
图 1 显示相应的地址例如 IP 地址子网掩码等等。

3.2 ping的使用

常用参数选项

ping IP -t--连续对 IP 地址执行 Ping 命令，直到被用户以 Ctrl+C 中断。

- a 以 IP 地址格式来显示目标主机的网络地址
- l 2000--指定 Ping 命令中的数据长度为 2000 字节，而不是缺省的 323 字节。
- n--执行特定次数的 Ping 命令
- f 在包中发送“不分段”标志。该包将不被路由上的网关分段。
- i ttl 将“生存时间”字段设置为 ttl 指定的数值。
- v tos 将“服务类型”字段设置为 tos 指定的数值。
- r count 在“记录路由”字段中记录发出报文和返回报文的路由。指定的 Count 值最小可以是 1，最大可 9 。
- s count 指定由 count 指定的转发次数的时间邮票。
- j computer-list 经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机（松散源路由）。允许的最大 IP 地址数目是 9 。
- k computer-list 经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机（严格源路由）。允许的最大 IP 地址数目是 9 。
- w timeout 以毫秒为单位指定超时间隔。
- destination-list 指定要校验连接的远程计算机。

在“开始”——“运行”弹出的对话框重输入”cmd“回车，弹出

C:\WINDOWS\system32\cmd.exe 窗口，然后输入“ping”回车，如图 2:

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.28.98

Pinging 192.168.28.98 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.28.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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

图 2 ping 命令

图 2 显示这些表明不能上网。数据报：发送=4 接受=0 丢失=4
输入 ping，显示 ping 命令的用法。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>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] 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.
    -i TTL     Time To Live.
    -v TOS     Type Of Service.
    -r count    Record route for count hops.
    -s count    Timestamp for count hops.
    -j host-list Loose source route along host-list.
    -k host-list Strict source route along host-list.
    -w timeout  Timeout in milliseconds to wait for each reply.

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

图 3 ping 相应的参数

(1) ping -t 的使用，如图 4 所示：

输入 ping IP -t

```
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>ping 192.168.28.98 -t

Pinging 192.168.28.98 with 32 bytes of data:

Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
Reply from 192.168.28.98: bytes=32 time<1ms TTL=128
极品五笔 半:
```

图 4 ping -t 运行结果

出现上面这些就显示可以正常访问 Internet，解释一下 TTL

TTL：生存时间 指定数据报被路由器丢失之前允许通过的网段数量。

TTL 是由发送主机设置的，以防止数据包不断在 IP 互联网络上永不终止地循环。转发 IP 数据包时，要求路由器至少将 TTL 减小 1。

注意：网速等于 \approx (发送的字节数/返回的时间[毫秒])K 字节；

注意：如果你的机器 TTL 是 251 的话,那说明你的机器的注册表被人修改了!

如图所示：

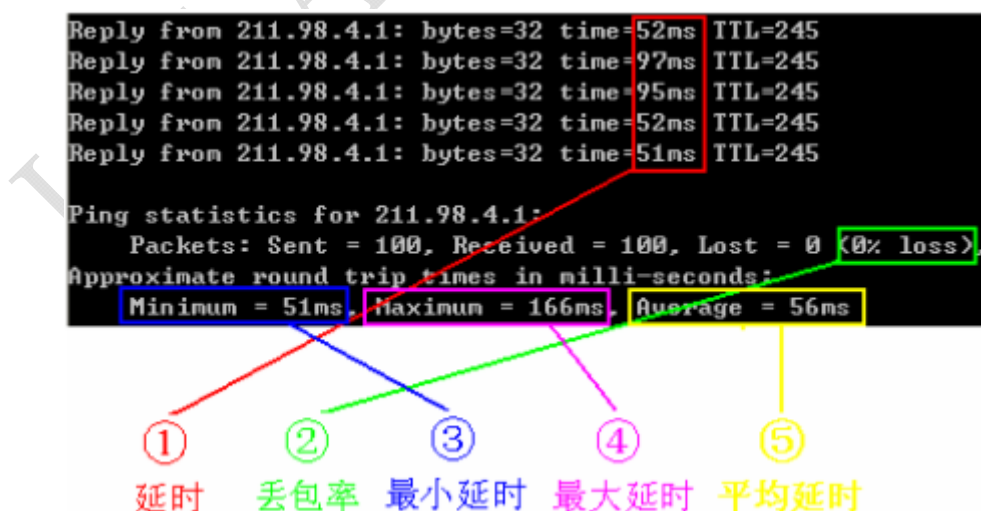


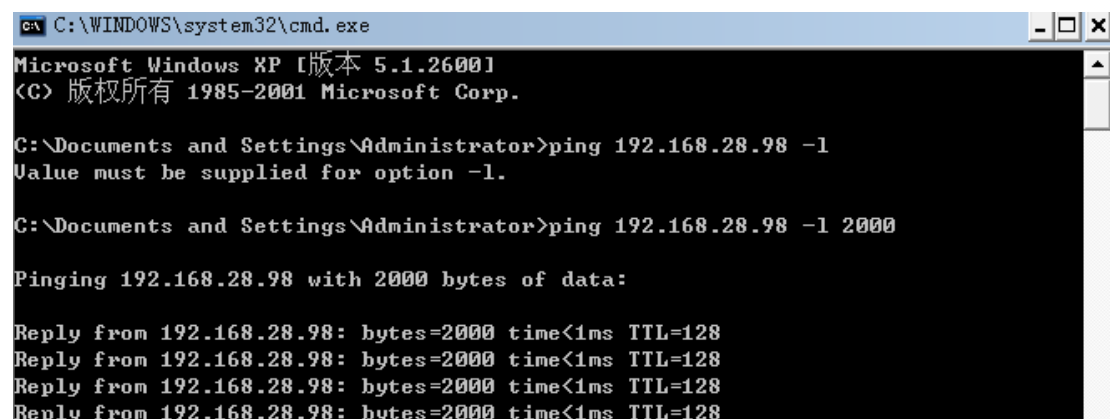
图 5 ping 运行结果解释

数据包：发送=100 接收=100；

(2) ping -n 的使用

例如: ping 192.168.28.101 -n 3 可以向这个 IP ping 三次才终止操作,n 代表次数;

(3) ping -l 的使用, 如图 6 所示:



```
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>ping 192.168.28.98 -l
Value must be supplied for option -l.

C:\Documents and Settings\Administrator>ping 192.168.28.98 -l 2000

Pinging 192.168.28.98 with 2000 bytes of data:

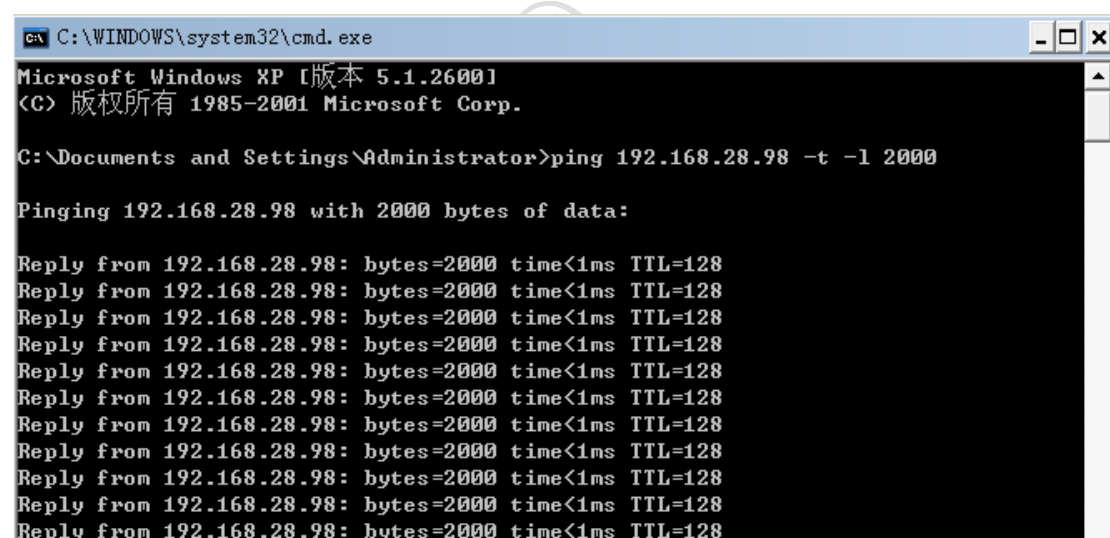
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
```

图 6 ping -l 运行结果解释

向这个 IP 用户发送 2000 字节;

如果你想终止的话可以按 “ctrl+c” 建终止操作;

(4) ping -l -t 的组和使用, 如图所示:



```
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>ping 192.168.28.98 -t -l 2000

Pinging 192.168.28.98 with 2000 bytes of data:

Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
Reply from 192.168.28.98: bytes=2000 time<1ms TTL=128
```

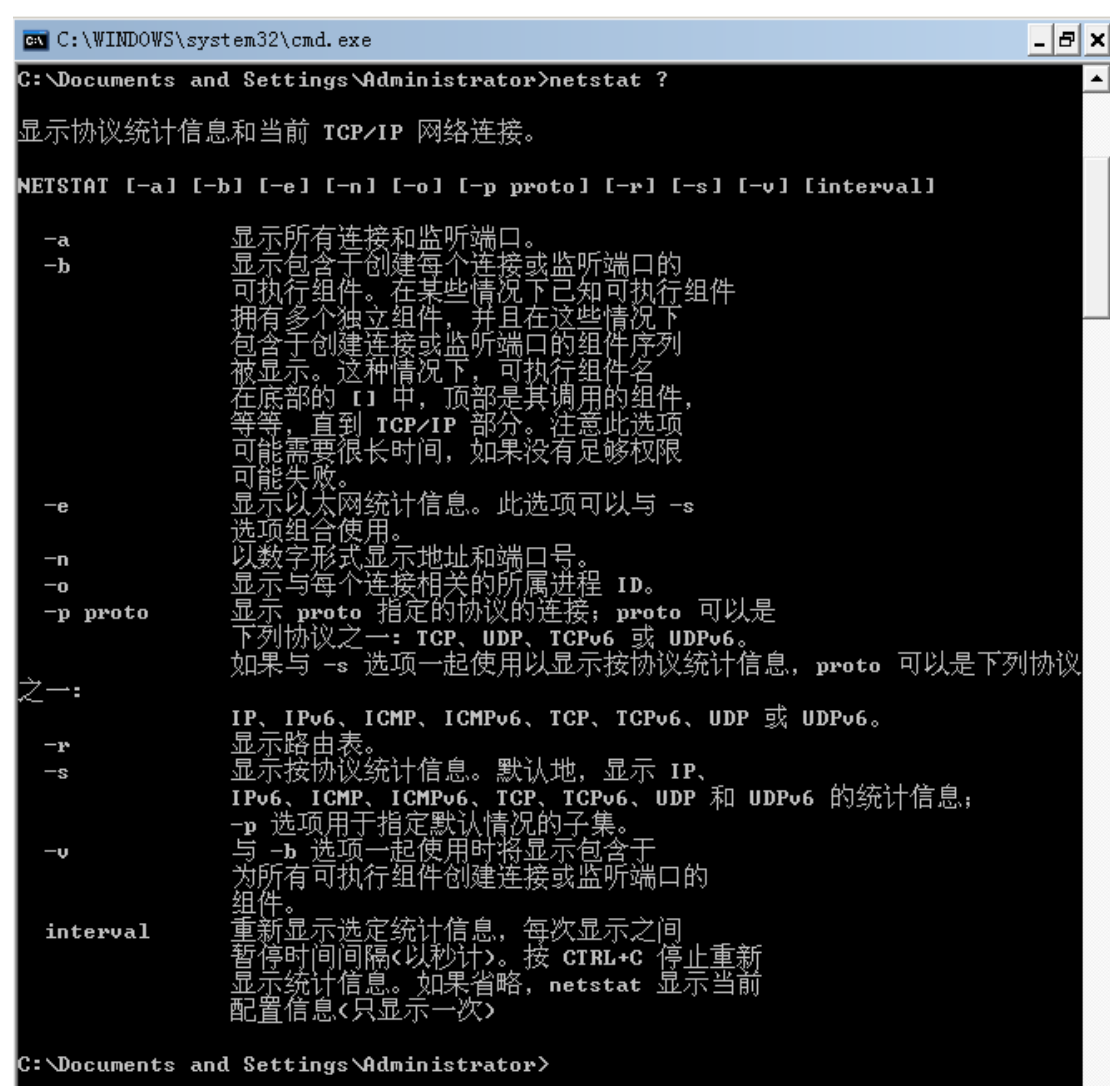
图 7 ping 运行结果解释

向这个 IP 用户连续的发送 2000 字节;

3.3、netstat命令的使用

netstat 是 DOS 命令, 是一个监控 TCP/IP 网络的非常有用的工具, 它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息. Netstat 用于显示与 IP、TCP、UDP 和

ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat ?

显示协议统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

-a          显示所有连接和监听端口。
-b          显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。这种情况下，可执行组件名在底部的 [ ] 中，顶部是其调用的组件，等等，直到 TCP/IP 部分。注意此选项可能需要很长时间，如果没有足够权限可能失败。
-e          显示以太网统计信息。此选项可以与 -s 选项组合使用。
-n          以数字形式显示地址和端口号。
-o          显示与每个连接相关的所属进程 ID。
-p proto    显示 proto 指定的协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。
            如果与 -s 选项一起使用以显示按协议统计信息，proto 可以是下列协议之一：
            IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。
-r          显示路由表。
-s          显示按协议统计信息。默认地，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；-p 选项用于指定默认情况的子集。
-v          与 -b 选项一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件。
interval    重新显示选定统计信息，每次显示之间暂停时间间隔<以秒计>。按 CTRL+C 停止重新显示统计信息。如果省略，netstat 显示当前配置信息<只显示一次>

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

图 8 netstat 命令

1. 使用netstat命令查看本机路由表

打开命令窗口，执行下面的命令。

```
netstat -r
```

运行结果如图 9 所示。

```
命令提示符
C:\Documents and Settings\Administrator>netstat -r

IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 26 18 0b 79 66 ..... Realtek RTL8102E Family PCI-E Fast Ethernet
NIC
=====
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
0.0.0.0                0.0.0.0          192.168.5.254    192.168.5.205    20
127.0.0.0              255.0.0.0        127.0.0.1        127.0.0.1        1
192.168.5.0            255.255.255.0    192.168.5.205    192.168.5.205    20
192.168.5.205          255.255.255.255  127.0.0.1        127.0.0.1        20
192.168.5.255          255.255.255.255  192.168.5.205    192.168.5.205    20
224.0.0.0              240.0.0.0        192.168.5.205    192.168.5.205    20
255.255.255.255        255.255.255.255  192.168.5.205    192.168.5.205    1
Default Gateway:       192.168.5.254
=====
Persistent Routes:
None

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

图 9 查看本地路由表

路由表中 Network Destination 表示要到达的目标网络的网络地址，Netmask 表示目标网络的子网掩码，Gateway 指定要到达目标网络需要经过的网关，Interface 指定网关的接口，Metric（度）指定指在路由选择协议算法完成计算后得到的一个变量值，如网络延迟，它的目的是确定最佳路由。

2. 使用netstat命令查看TCP/UDP连接情况

打开命令窗口，执行下面的命令。

```
netstat -na
```

运行结果如图 10 所示。

```
C:\命令提示符
C:\Documents and Settings\Administrator>netstat -na

Active Connections

Proto Local Address          Foreign Address         State
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING
TCP    0.0.0.0:1027            0.0.0.0:0               LISTENING
TCP    0.0.0.0:1081            0.0.0.0:0               LISTENING
TCP    0.0.0.0:1433            0.0.0.0:0               LISTENING
TCP    0.0.0.0:2880            0.0.0.0:0               LISTENING
TCP    0.0.0.0:3306            0.0.0.0:0               LISTENING
TCP    0.0.0.0:3389            0.0.0.0:0               LISTENING
TCP    0.0.0.0:8031            0.0.0.0:0               LISTENING
TCP    0.0.0.0:9901            0.0.0.0:0               LISTENING
TCP    0.0.0.0:10205           0.0.0.0:0               LISTENING
TCP    0.0.0.0:18386           0.0.0.0:0               LISTENING
TCP    0.0.0.0:20205           0.0.0.0:0               LISTENING
TCP    0.0.0.0:23141           0.0.0.0:0               LISTENING
TCP    127.0.0.1:445           127.0.0.1:1035          ESTABLISHED
TCP    127.0.0.1:1035         127.0.0.1:445          ESTABLISHED
TCP    127.0.0.1:1054          0.0.0.0:0               LISTENING
TCP    127.0.0.1:1434          0.0.0.0:0               LISTENING
TCP    127.0.0.1:8081          0.0.0.0:0               LISTENING
TCP    192.168.5.205:139       0.0.0.0:0               LISTENING
TCP    192.168.5.205:1043      110.75.161.77:16000      ESTABLISHED
TCP    192.168.5.205:2851      110.75.161.37:16000      ESTABLISHED
TCP    192.168.5.205:10509     61.135.189.6:80         CLOSE_WAIT
TCP    192.168.5.205:13417     61.135.189.6:80         CLOSE_WAIT
TCP    192.168.5.205:14349     61.135.189.6:80         CLOSE_WAIT
TCP    192.168.5.205:14369     61.135.189.6:80         CLOSE_WAIT
TCP    192.168.5.205:14373     61.135.189.6:80         CLOSE_WAIT
TCP    192.168.5.205:14397     61.135.189.6:80         CLOSE_WAIT
TCP    192.168.5.205:14416     61.135.189.6:80         ESTABLISHED
TCP    192.168.5.205:14495     60.2.251.10:80          CLOSE_WAIT
TCP    192.168.5.205:14545     61.139.219.152:80       TIME_WAIT
UDP    0.0.0.0:445             *:*:                     *:
UDP    0.0.0.0:500             *:*:                     *:
UDP    0.0.0.0:1028            *:*:                     *:
UDP    0.0.0.0:3601            *:*:                     *:
UDP    0.0.0.0:4500            *:*:                     *:
```

图 10 查看 TCP/UDP 连接情况

在 netstat 命令中使用 -o 参数可以查看该连接对应的进程编号 (PID)。在命令窗口执行下面的命令：

netstat -nao

运行结果如图 11 所示。

```
C:\命令提示符
C:\Documents and Settings\Administrator>netstat -nao

Active Connections

Proto Local Address          Foreign Address         State      PID
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING  792
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING  4
TCP    0.0.0.0:1027            0.0.0.0:0               LISTENING  532
TCP    0.0.0.0:1433            0.0.0.0:0               LISTENING  1724
TCP    0.0.0.0:3306            0.0.0.0:0               LISTENING  1780
TCP    0.0.0.0:3389            0.0.0.0:0               LISTENING  3612
TCP    0.0.0.0:8031            0.0.0.0:0               LISTENING  2908
TCP    0.0.0.0:9901            0.0.0.0:0               LISTENING  1352
TCP    0.0.0.0:10205           0.0.0.0:0               LISTENING  5396
TCP    0.0.0.0:20205           0.0.0.0:0               LISTENING  2908
TCP    127.0.0.1:445           127.0.0.1:1035          ESTABLISHED 4
TCP    127.0.0.1:1035         127.0.0.1:445          ESTABLISHED 4
TCP    127.0.0.1:1054          0.0.0.0:0               LISTENING  3824
TCP    127.0.0.1:1434          0.0.0.0:0               LISTENING  1724
TCP    127.0.0.1:8081          0.0.0.0:0               LISTENING  2908
TCP    192.168.5.205:139       0.0.0.0:0               LISTENING  4
TCP    192.168.5.205:10509     61.135.189.6:80         CLOSE_WAIT  5000
TCP    192.168.5.205:13417     61.135.189.6:80         CLOSE_WAIT  5648
```

图 11 查看 TCP/UDP 连接情况中的进程编号

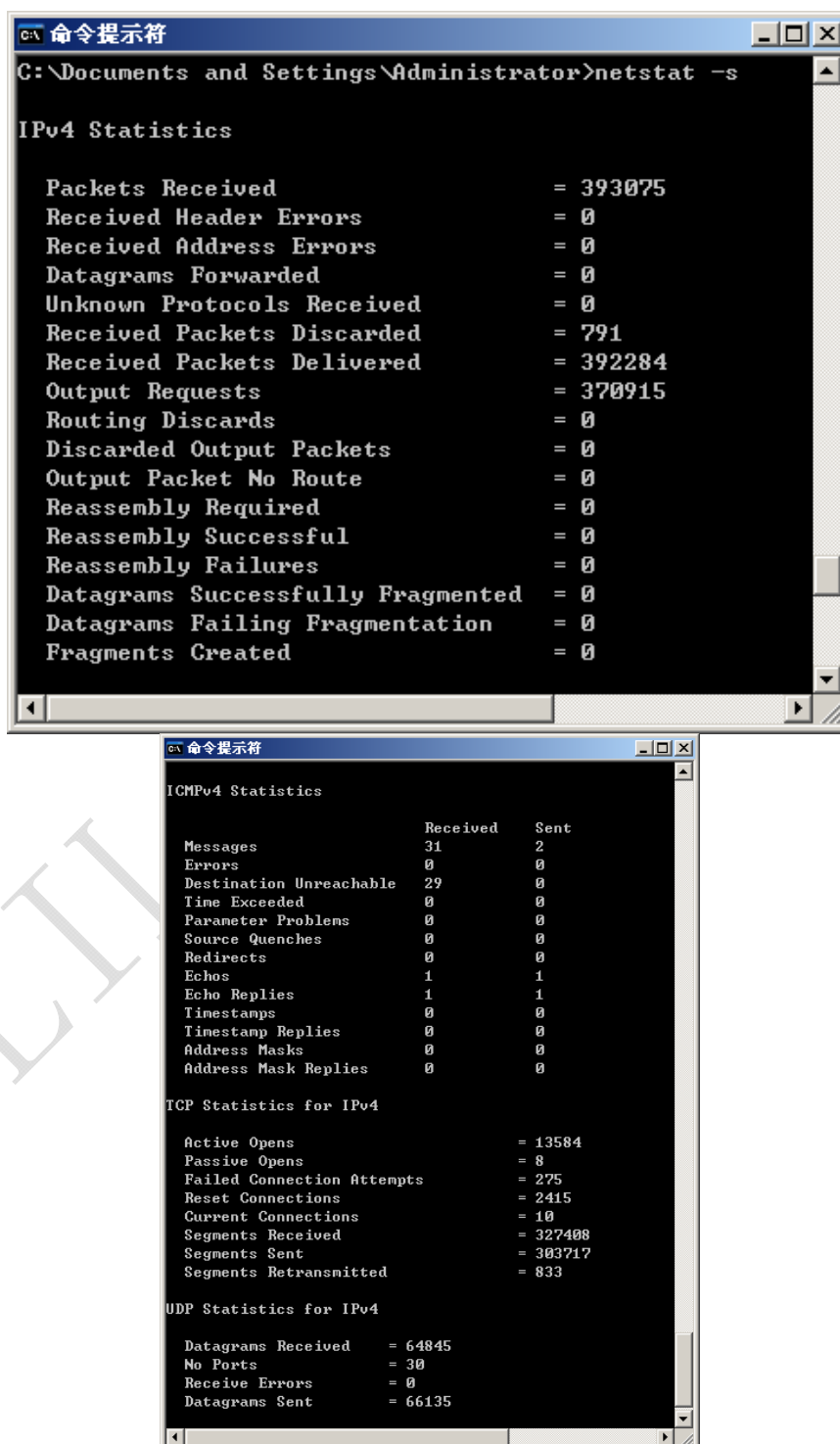
可以打开任务管理器，查看 PID 对应的进程信息。

3. 使用netstat命令查看IP、ICMP、TCP和UDP等协议的统计信息

打开命令窗口，执行下面的命令。

```
netstat -s
```

运行结果如图 12 所示。



```
C:\Documents and Settings\Administrator>netstat -s

IPv4 Statistics

Packets Received                = 393075
Received Header Errors          = 0
Received Address Errors         = 0
Datagrams Forwarded             = 0
Unknown Protocols Received      = 0
Received Packets Discarded      = 791
Received Packets Delivered      = 392284
Output Requests                 = 370915
Routing Discards                = 0
Discarded Output Packets        = 0
Output Packet No Route         = 0
Reassembly Required             = 0
Reassembly Successful           = 0
Reassembly Failures             = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created               = 0


ICMPv4 Statistics

          Received    Sent
Messages          31      2
Errors              0      0
Destination Unreachable 29      0
Time Exceeded      0      0
Parameter Problems  0      0
Source Quench      0      0
Redirects          0      0
Echoes             1      1
Echo Replies       1      1
Timestamps         0      0
Timestamp Replies  0      0
Address Masks      0      0
Address Mask Replies 0      0


TCP Statistics for IPv4

Active Opens                = 13584
Passive Opens               = 8
Failed Connection Attempts  = 275
Reset Connections           = 2415
Current Connections        = 10
Segments Received           = 327408
Segments Sent               = 303717
Segments Retransmitted     = 833


UDP Statistics for IPv4

Datagrams Received  = 64845
No Ports            = 30
Receive Errors      = 0
Datagrams Sent      = 66135
```

图 12 查看 IP、ICMP、TCP 和 UDP 等协议的统计信息

因为返回结果的内容很多，因此这里使用两个窗口来显示。在左侧的窗口中向下拉动滚动条，即可看到右侧窗口中的内容。

在 IPv4 的统计信息中，可以看到的项目如表 1 所示。

项 目 名 称	描 述 信 息
Packets Received	收到的数据包数量
Received Header Errors	收到的包头错误的数据包数量
Received Address Errors	收到的地址错误的数据包数量
Datagrams Forwarded	转发的数据包数量
Unknown Protocols Received	收到的协议未知的数据包数量
Received Packets Discarded	接收后被丢弃的数据包数量
Received Packets Delivered	接收后被转发的数据包数量
Output Requests	请求数量
Routing Discards	路由丢弃数
Discarded Output Packets	包丢弃数
Output Packet No Route	没有路由的请求包数量
Reassembly Required	重组的请求数
Reassembly Successful	重组成功的数量
Reassembly Failures	重组失败的数量
Datagrams Successfully Fragmented	分片成功的数据报数量
Datagrams Failing Fragmentation	分片失败的数据报数量
Fragments Created	建立的分片数量

在 ICMPv4 的统计信息中，可以看到的项目如表 2 所示。每个项目都拥有发送和接收两个数量。

项 目 名 称	描 述 信 息
Messages	消息数量
Errors	错误数量
Destination Unreachable	无法到达的主机数量
Time Exceeded	超时数量
Parameter Problems	参数错误数量
Source Quenches	源夭折数量
Redirects	重定向数量
Echos	回应数量
Echo Replies	回复回应数量
Timestamps	时间戳数
Timestamp Replies	时间戳回复数

Address Masks	地址掩码数
Address Mask Replies	地址掩码回复数

在 TCP 的统计信息中，可以看到的项目如表 3 所示。

表 3 TCP 的统计信息中的项目

项 目 名 称	描 述 信 息
Active Opens	主动打开的连接数
Passive Opens	被动打开的连接数
Failed Connection Attempts	尝试连接失败的数量
Reset Connections	重置连接的数量
Current Connections	当前连接数
Segments Received	已经收到的报文数量
Segments Sent	已经发送的报文数量
Segments Retransmitted	被重传的报文数量

在 UDP 的统计信息中，可以看到的项目如表 4 所示。

表 4 UDP 的统计信息中的项目

项 目 名 称	描 述 信 息
Datagrams Received	接收到数据包数量
No Ports	没有端口的数据包数量
Receive Errors	接收错误的数据包数量
Datagrams Sent	发送的数据包数量

3.4 tracert命令

注释：Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标路径。

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。

- d: 指定不将 IP 地址解析到主机名称。
- hmaximum_hops: 指定跃点数以跟踪到称 target_name 的主机的路由。
- j host-list: 指定 tracert 实用程序数据包所采用路径中的路由器接口列表。
- w timeout: 等待 timeout 为每次回复所指定的毫秒数。

```
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

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] 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.
    -w timeout         Wait timeout milliseconds for each reply.

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

图 13tracert 命令

3.5 nslookup命令的使用

NSLOOKUP 是 NT、2000 中连接 DNS 服务器，查询域名信息的一个非常有用的命令是由 local DNS 的 cache 中直接读出来的，而不是 local DNS 向真正负责这个 domain 的 name server 问来的。Nslookup 必须要安装了 TCP/IP 协议的网络环境之后才能使用。

```
C:\Documents and Settings\Administrator>nslookup www.baidu.com
Server: ns.sdjnptt.net.cn
Address: 202.102.128.68

Non-authoritative answer:
Name: www.a.shifen.com
Addresses: 123.235.44.30, 123.235.44.31
```

图 14 nslookup 运行结果解释

以上结果显示，正在工作的 DNS 服务器的主机名为 ns.sdjnptt.net.cn, 它的 IP 地址是 202.102.128.68

(1) 把 123.235.44.38 地址反向解析成 www.Baidu.com 如图所示：

```
C:\Documents and Settings\Administrator>nslookup 123.235.44.38
Server: ns.sdjnptt.net.cn
Address: 202.102.128.68

*** ns.sdjnptt.net.cn can't find 123.235.44.38: Non-existent domain
```

图 15 nslookup 运行结果解释

(2) 如果出现下面这些，说明测试主机在目前的网络中，根本没有找到可以使用的 DNS 服务器

*** Can't find server name for domain: No response from server

*** Can't repairpc.nease.net : Non-existent domain

(3) 如果出现下面这些，这种情况说明网络中 DNS 服务器 ns-px.online.sh.cn 在工作，却

不能实现域名 www.Baidu.com 的正确解析。

Server: ns-px.online.sh.cn

Address: 202.96.209.5

*** ns-px.online.sh.cn can't find www.baidu.com Non-existent domain

3.6 ARP命令的使用

注释：ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写。

在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。

-a: 通过询问 TCP/IP 显示当前 ARP 项。如果指定了 inet_addr, 则只显指定计算机的 IP 和物理地址。

-g: 与 -a 相同。

inet_addr: 以加点的十进制标记指定 IP 地址。

-N: 显示由 if_addr 指定的网络界面 ARP 项。

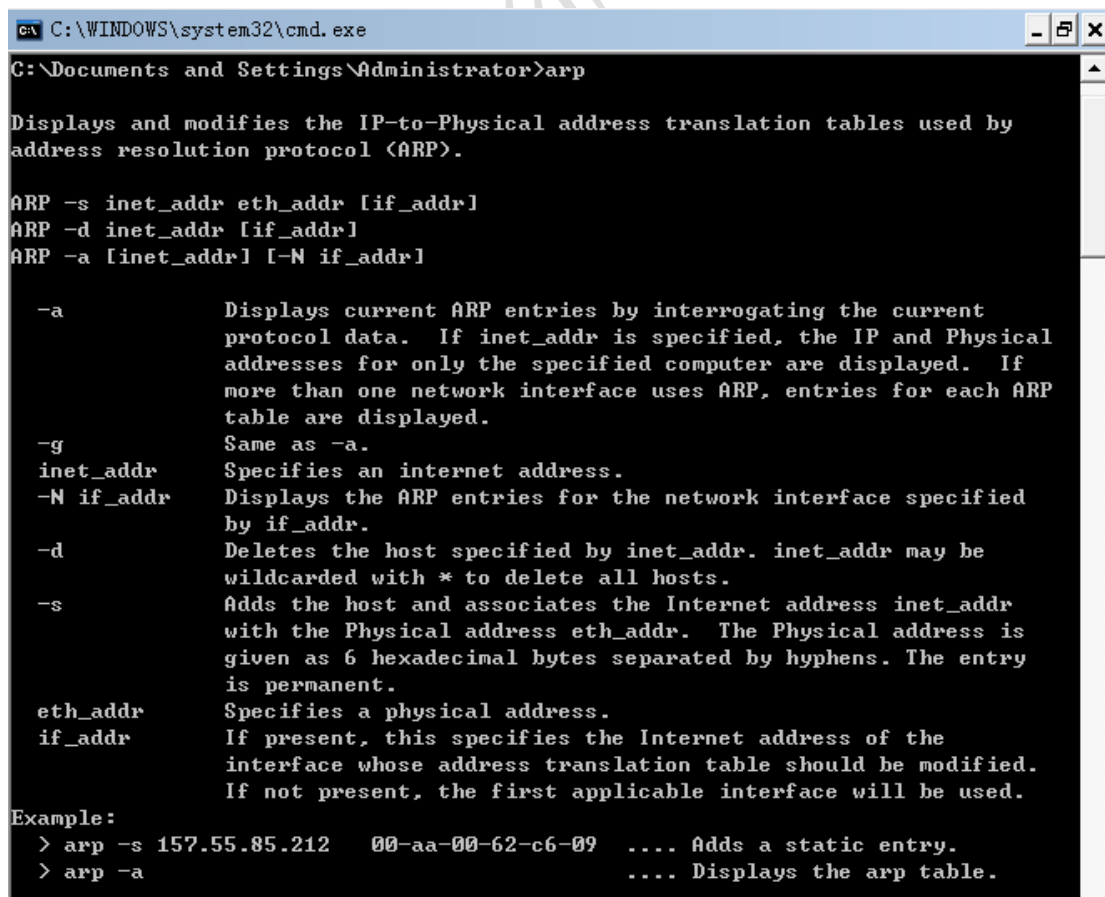
if_addr: 指定需要修改其地址转换表接口的 IP 地址（如果有的话）。如果不存在，将使用第一个可适用的接口。

-d: 删除由 inet_addr 指定的项。

-s: 在 ARP 缓存中添加项，将 IP 地址 inet_addr 和物理地址 ether_addr 关联。

物理地址由以连字符分隔的 6 个十六进制字节给定。使用带点的十进制标记指定 IP 地址项是永久性的，即在超时到期后项自动从缓存删除。

ether_addr: 指定物理地址。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>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]

-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.

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.

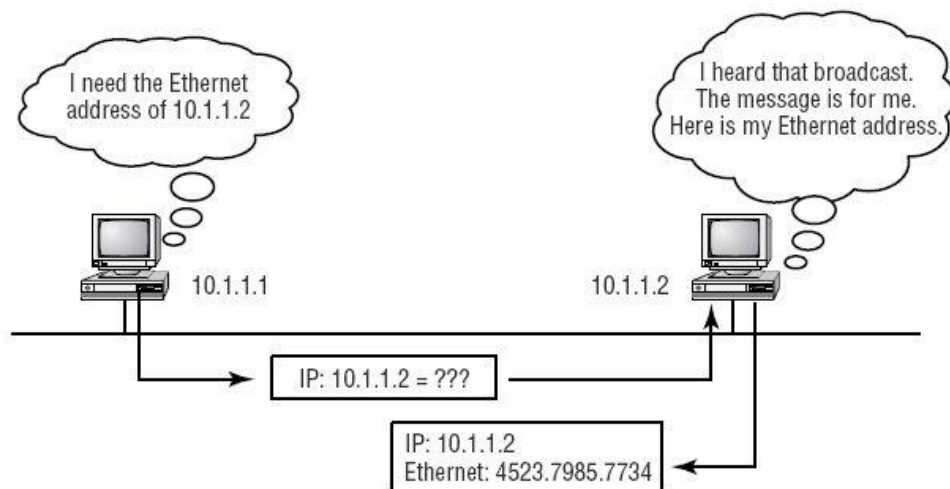
eth_addr    Specifies a physical address.

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.
```

图 16 arp 运行结果解释

FIGURE 2.8 Local ARP broadcast



Arp 工作原理：

主机 10.1.1.1 要同 10.1.1.2 通信，首先查找自己的 ARP 缓存，若没有 10.1.1.2 的缓存记录则发出如下的广播包：

“我是主机我是主机 10.1.1.1,我的 MAC 是 00-58-4C-00-03-B0,IP 为 10.1.1.2 的主机请告之你的 MAC 来”

IP 为 10.1.1.2 的主机响应这个广播，应答 ARP 广播为：

“我是 10.1.1.2，我的 MAC 是 0E-59-4C-00-33-B0”

于是，主机 10.1.1.1 刷新自己的 ARP 缓存，然后发出该 IP 包。

(1) 查看arp表

打开命令窗口，输入并执行下面的命令。

```
arp -a
```

可以查看到本地计算机的 ARP 表。Internet Address 列中显示 IP 地址，Physical Address 列中显示 MAC 地址，Type 列中显示 ARP 表项的类型，dynamic 表示从网络中动态获取的 ARP 表项，static 表示静态绑定的 ARP 表项。

(2) 删除ARP表条目

假定在第 1 步中看到 ARP 表中存在一个 IP 地址 192.168.5.205，练习执行下面的命令，从本地 ARP 表中删除 IP 地址为 192.168.5.205 的条目。

```
arp -d 192.168.5.205
```

(3) 确认条目删除

再次执行 arp -a 命令，确认该条目已经被删除。

4. 实验报告要求

实验结束后，完成《实验报告 1》。

实验报告要求：

0.文件名：实验 1 网络服务与配置-2015b110xx-名字

1.字体：宋体；字号：五号；首行缩进两格；行间距为 1.5 倍。

2.表格位置和内容居中，字体字号同要求 1，表格必须有表题，居于表的顶部居中；

3.图片居中显示，单张图片长宽不超过均不超过 5 厘米，图必须有图名，居于图下居中位置。

4.请将实验内容、步骤截图保存，记录好实验中的各种数据，体现在报告里。

5.请删除报告书内括号及括号内的内容。请勿修改报告书其余格式和文字。

6.完成实验报告后，请先交给班级学委，由学委打包好发给任课老师。