

## 实验二 简单的网络管理方法

### 1. 实验目的

- 1) 掌握使用 ipconfig 实用程序的方法, 藉此了解本地 PC 当前的网络配置状态;
- 2) 掌握使用 ping 实用程序检测网络的连通性、可到达性和处理名称解析的方法;
- 3) 掌握使用 traceroute 实用程序命令测量路由情况的技能;
- 4) 学会使用 netstat 命令了解网络当前状态的方法。
- 5) 学会使用 nslookup 命令测试 DNS 服务器的情况

### 2. 实验环境

- 1) 允许 Windows 2000/2003 Server/XP 操作系统的 PC 一台。
- 2) 每台 PC 具有一块以太网卡, 通过双绞线与局域网相连。

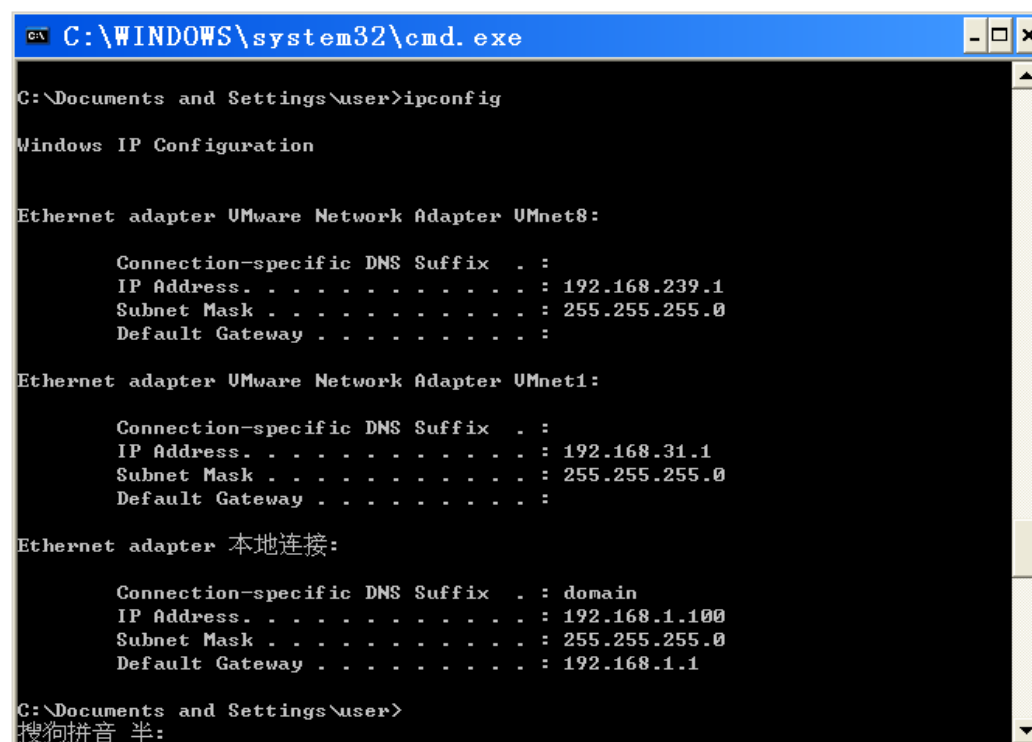
### 3. 实验步骤

#### ➤ ipconfig 实用程序

- 1) 熟悉 ipconfig 命令

在命令提示符界面执行 ipconfig, 可以显示本机所以当前的 TCP/IP 网络配置值, 刷新动态主机配置协议 (DHCP) 和域名系统 (DNS) 设置。

使用不带参数的 ipconfig 可以显示所有适配器的 IP 地址、子网掩码、默认网关, 如图 2-1 所示。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\user>ipconfig

Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.239.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.31.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

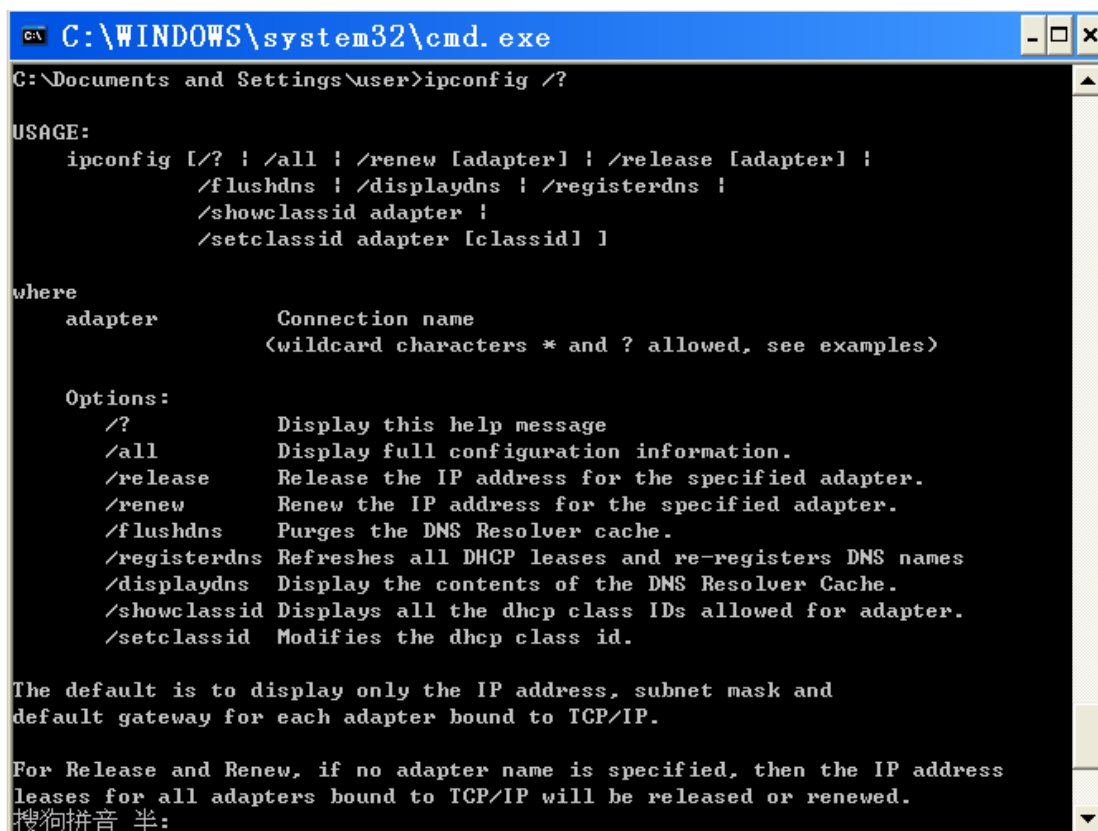
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : domain
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

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

图 2-1 显示适配器的基本 TCP/IP 配置

如果不熟悉 ipconfig 命令的参数，可以在命令提示符执行命令“ipconfig /?”查看 ipconfig 命令的所有参数信息，如图 2-2 所示。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\user>ipconfig /?

USAGE:
    ipconfig [/? ! /all ! /renew [adapter] ! /release [adapter] !
           /flushdns ! /displaydns ! /registerdns !
           /showclassid adapter !
           /setclassid adapter [classid] ]

where
    adapter      Connection name
                  (wildcard characters * and ? allowed, see examples)

Options:
    /?           Display this help message
    /all         Display full configuration information.
    /release     Release the IP address for the specified adapter.
    /renew       Renew the IP address for the specified adapter.
    /flushdns    Purges the DNS Resolver cache.
    /registerdns Refreshes all DHCP leases and re-registers DNS names
    /displaydns  Display the contents of the DNS Resolver Cache.
    /showclassid Displays all the dhcp class IDs allowed for adapter.
    /setclassid  Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.
搜狗拼音 半:
```

图 2-2 ipconfig 的参数信息

## 2) 使用 ipconfig 命令

- a) 显示所有适配器的基本 TCP/IP 配置，键入“ipconfig”命令查看。
- b) 显示所有适配器的完整 TCP/IP 配置，键入“ipconfig /all”命令查看，并与 a) 中的显示进行比较，注意增加的信息。
- c) 对 DHCP 服务器分配 IP 地址操作。如果需要释放所有适配器的当前 DHCP 配置并丢弃 IP 地址配置，同时禁用配置为自动获取 IP 地址的适配器的 TCP/IP，应键入“ipconfig /release”。如果为更新所有适配器的 DHCP 配置，在自动获取 IP 地址的网卡的计算机上，应键入“ipconfig /renew”。
- d) 在排除 DND 的名称解析故障期间清理 DNS 解析器缓存，键入“ipconfig /flushdns”。

### 注意事项：

- 1) 只有当 TCP/IP 协议安装为网络适配器属性的器件后，该命令才可用。
- 2) 如果适配器名称包含空格，要在该适配器名称两边使用引号（即 “Address Name”）。对于适配器名称，ipconfig 可以使用星号（\*）通配符指定名称为指定字符串开头的适配器，或名称包含有指定串的适配器。例如，Local \*可以匹

配所有包含字符串 Local 开头的适配器。而\*Con\*可以匹配所有包含字符串 Con 的适配器。

## ➤ ping 实用程序

### 1) 熟悉 ping 命令

ping 实用程序通过发送方向接收方发送“互联网控制报文协议(ICMP)”回显(echo)请求消息，接收方将对该回显请求进行自动回显应答，来验证两台支持 TCP/IP 协议的计算机之间的 IP 层连接，并在发送方将回显应答消息的接受情况与往返过程的次数一起显示出来。Ping 是用于检测网络连接性、可到达性和名称解析等疑难问题的主要 TCP/IP 命令。

如果不带参数，ping 将自行显示帮助，或者在命令提示符下执行“ping /?”命令，如图 2-3 所示。

```
C:\Documents and Settings\user>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.
```

图 2-3 ping 的参数信息

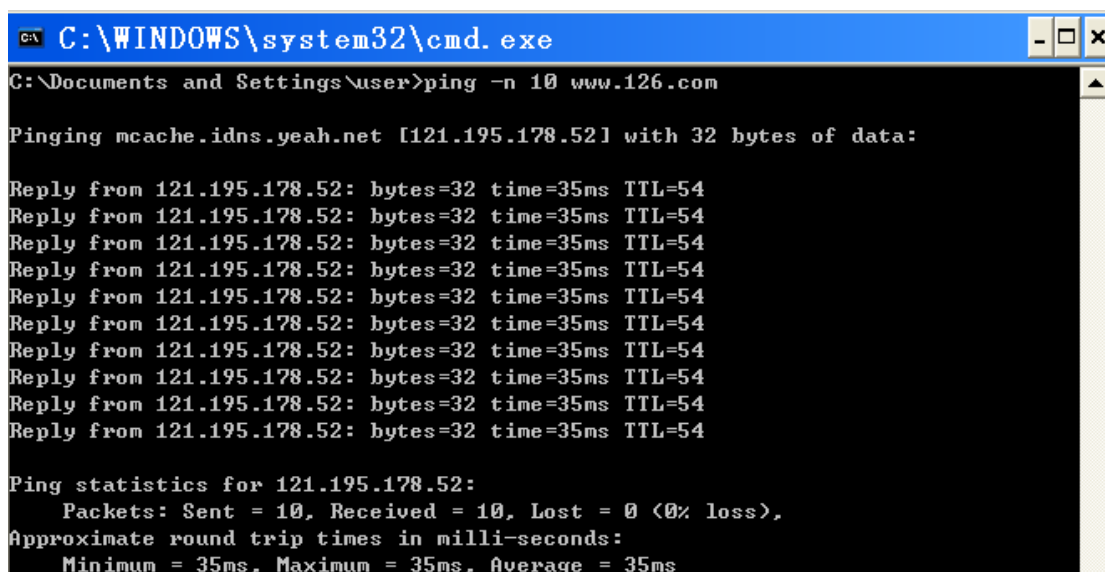
### 2) 使用 ping 命令

a) 测试目的主机的可达性。执行“ping<目的主机地址或域名>”，如果在有限的时间内能够得到目的主机的正确应答，则可认为本机可达目的主机；否则，则可能是本机不可达目的主机，也可能是因为有些主机处于安全或性能原因，将主机设置为不对远端主机的 ping 操作做出响应。

b) 计算机域名和计算机 IP 地址。如果成功验证了 IP 地址，但未成功验证计算机域名，则可能是由于名称解析问题所致。在这种情况下，要确保指定的计算机名可以通过本地主机文件进行解析，其方法是通过域名系统（DNS）查询或 NetBIOS 名称解析技术进行解析。

c) 测试目的主机的连通性能。为了粗略地检查网络的连通的性能情况，可向目的主机发送 N 个回显请求消息，看有多少消息能够到达，消息用了多少时间到达。

例如，我没向 [www.126.com](http://www.126.com) 发送 10 个回显请求消息，得到图 2-3 所示的结果。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\user>ping -n 10 www.126.com

Pinging mcache.idns.yeah.net [121.195.178.52] with 32 bytes of data:

Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54
Reply from 121.195.178.52: bytes=32 time=35ms TTL=54

Ping statistics for 121.195.178.52:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms
```

图 2-3 测试目的主机的连通性

可以看出接收到了 10 个消息，丢失率为 0；往返时延为 35 ms。

- 3) 提示：测试网络连通性能是一个非常复杂的问题，应当采用数理统计的方法才能得出较为客观的结果。

#### 注意事项：

- 1) 只有当 TCP/IP 协议在“网络连接”中安装为网络适配器属性的组件时，ping 命令才可用。
- 2) 随着防火墙功能在网络中的广泛应用当你 ping 其他主机或其他主机 ping 你的 [http://v.youku.com/v\\_show/id\\_XMTE1NjMzNTg4.html](http://v.youku.com/v_show/id_XMTE1NjMzNTg4.html) 主机时，而显示主机不可达的时候，不要草率的下结论。最好与某台“设置良好”主机的 ping 结果进行对比。

## ➤ traceroute 实用程序

traceroute 通过设置 IP 首部中的寿命（Time To Live, TTL）字段来实现路由探测的功能。IP 分组经过每个路由器的时候都会将 TTL 值减去 1，即 TTL 值可以看作经过的路由器跳数的计数器。当路由器接收到一个 TTL 为 0 或者 1 的 IP 分组时，路由器就不再转发这个分组，而是直接丢弃，并且发生一个 ICMP “超时”报文给源主机。

traceroute 程序的关键在于返回的超时错误的 ICMP 分组的 IP 首部的源地址就是这个路由器的入口 IP 地址。通过逐渐增大 TTL 的值，可以得到该路径上的所有路由器的入口 IP 地址，直到对目的主机发生一个 UDP 端口不可达报文，并收到其 ICMP 的“端口不可达”响应分组为止。

#### 1) traceroute 的基本操作

- a) traceroute 命令的基本用法是，在命令提示符后键入“tracert *host\_name*”或

“tracert *ip\_address*”，其中 tracert 是 traceroute 在 Windows 操作系统上的称呼，*host\_name* 与 *ip\_address* 分别是目的计算机的主机名或 IP 地址。图 2-4 是以新浪网（[www.sina.com.cn](http://www.sina.com.cn)）为目的地的执行结果。输出有 5 列：第一列是描述路径的第 *n* 跳的数值，即沿着该路径的路由器序号；第二列是第一次往返时间；第三列是第二次往返时间时延；第四列是第三次往返时延；第五列是路由器名字及其输入端口的 IP 地址。

```
C:\Documents and Settings\user>tracert www.sina.com.cn

Tracing route to cernetnews.sina.com.cn [121.194.0.208]
over a maximum of 30 hops:

  1    35 ms    34 ms    34 ms    121.194.0.208

Trace complete.
```

图 2-4 执行 tracert 操作

b) 如果源从任何给定的路由器接收到的报文少于 3 条(由于网络中的分组丢失)，traceroute 在该路由器号码后面放一个星号，并报告到达那台路由器的少于 3 次的往返时间。

c) 多尝试几次“ping [www.sina.com.cn](http://www.sina.com.cn)”的操作，比较得到的新浪网的 IP 地址。如果两次 ping 得到的 IP 地址不同，试考虑其中的原因（如考虑到负载均衡）。然后针对这些不同的 IP 地址，执行“tracert *ip\_address*”命令，观察分析输出的结果是否有差异。

## 2) traceroute 的参数

在 Windows 操作系统上，可在命令提示符中键入“tracert”命令即可获得 tracert 的语法说明信息，如图 2-5 所示。自行测试各种参数并记录结果。

```
C:\Documents and Settings\user>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.
```

图 2-5 tracert 参数说明

## 3) 测试大型网络的路由

a) 对于大型网络中的某站点进行 traceroute 测试，记录测试结果。观察其中是否出现第 *n* 跳的时延小于第 *n-1* 跳的时延情况。试分析其中原因（提示：可分别考虑时延的各个构成成分在总时延中所起的作用）。

b) 在一天的不同时段内，用 traceroute 程序多次测量从固定主机到远程固定 IP 地址的主机的路由。试分析比较测量数据，观察该路由是否有变化？如果有变化，该变化频繁吗？

## 注意事项:

- 1) 执行 `tracert` 命令所显示的路径是源主机与目的主机间的路径中的路由器的近侧路由器接口列表。近侧接口是距离路径中的发送主机最近的路由器的接口。

## ➤ netstat 命令的使用

`netstat` 命令能够显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议）以及 IPv6 统计信息（对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及 UDP 协议）。使用时如果不带参数，`netstat` 显示活动的 TCP 连接。

### 1) netstat 的参数及其用法

在命令提示符中键入“`netstat -?`”命令列出 `netstat` 的所有参数及其用法，如图 2-6 所示。测试各种参数显示的信息并记录结果。

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

图 2-6 netstat 参数信息

### 2) 了解本机的通信状况

用“`netstat -n`”命令观察对方的 IP 地址，可以迅速得知自己与自己通信的对方所使用的 IP 地址，如图 2-6 所示；进一步使用“`netstat -a`”命令，就可以看到对方上网时所使用

的 IP 或 ISP 域名了，甚至可以看到所有端口，如图 2-7 所示。

```
C:\Documents and Settings\user>netstat -n

Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:1403          127.0.0.1:8081         CLOSE_WAIT
TCP   127.0.0.1:1416          127.0.0.1:8081         ESTABLISHED
TCP   127.0.0.1:8081          127.0.0.1:1416         ESTABLISHED
TCP   192.168.1.100:1111      221.176.31.1:8080      ESTABLISHED
TCP   192.168.1.100:2003      221.130.45.215:80      TIME_WAIT
TCP   192.168.1.100:2534      64.233.189.99:80       CLOSE_WAIT
```

图 2-6 以点分十进制的形式列出 IP 地址

```
C:\Documents and Settings\user>netstat -a

Active Connections

Proto Local Address          Foreign Address         State
TCP   scut-b7-01:epmap       scut-b7-01:0           LISTENING
TCP   scut-b7-01:microsoft-ds scut-b7-01:0           LISTENING
TCP   scut-b7-01:912         scut-b7-01:0           LISTENING
TCP   scut-b7-01:1440        scut-b7-01:0           LISTENING
TCP   scut-b7-01:6059        scut-b7-01:0           LISTENING
TCP   scut-b7-01:843         scut-b7-01:0           LISTENING
TCP   scut-b7-01:1034        scut-b7-01:0           LISTENING
TCP   scut-b7-01:1403        localhost:8081          CLOSE_WAIT
TCP   scut-b7-01:1416        localhost:8081          ESTABLISHED
TCP   scut-b7-01:8081        scut-b7-01:0           LISTENING
TCP   scut-b7-01:8081        localhost:1416          ESTABLISHED
TCP   scut-b7-01:8082        scut-b7-01:0           LISTENING
TCP   scut-b7-01:8083        scut-b7-01:0           LISTENING
TCP   scut-b7-01:netbios-ssn scut-b7-01:0           LISTENING
TCP   scut-b7-01:1111        221.176.31.1:8080      ESTABLISHED
TCP   scut-b7-01:2003        221.130.45.215:http    TIME_WAIT
TCP   scut-b7-01:2534        hkg01s01-in-f99.google.com:http CLOSE_WAIT
TCP   scut-b7-01:netbios-ssn scut-b7-01:0           LISTENING
TCP   scut-b7-01:netbios-ssn scut-b7-01:0           LISTENING
UDP   scut-b7-01:microsoft-ds *: *
UDP   scut-b7-01:1135        *: *
UDP   scut-b7-01:1136        *: *
UDP   scut-b7-01:1155        *: *
```

图 2-7 显示含有所有有效连接信息的列表

➤ nslookup 命令

nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。nslookup 必须在安装了 TCP/IP 协议的网络环境中才能使用。

在命令提示符下输入：

```
nslookup
```

这样就可以进入 nslookup 环境。

(1) 设置 DNS Server

在 nslookup 提示符下输入：

```
ls
```



列出 DNS 域的信息，如图 2-8 所示。

```
> ls
Server:  apple
Address:  222.201.130.30
```

图 2-8 列出 DNS 信息

在 nslookup 提示符下输入：

root

将默认的服务器更改为 DNS 域名空间的根的服务器，如图 2-9 所示。

```
> root
Default Server:  A.ROOT-SERVERS.NET
Address:  198.41.0.4
> _
```

图 2-9 nslookup root 命令执行结果

在 nslookup 提示符下输入：

server IP

将默认的服务器更改为指定的 DNS 服务器，其中参数 IP 为指定的 DNS 服务器的 IP 地址，如图 2-10 所示。

```
> server 166.111.8.28
Default Server:  dns-a.tsinghua.edu.cn
Address:  166.111.8.28
>
```

图 2-10 更改 DNS 服务器

## (2) 域名解析

nslookup 提供了将域名解析为 IP 地址的功能，同时也提供了将 IP 地址反向解析为域名的功能。

在命令提示符下输入：

nslookup [www.baidu.com](http://www.baidu.com)

结果显示 [www.baidu.com](http://www.baidu.com) 域名对应的 IP 地址为：205.188.238.109，如图 2-11 所示。

```
C:\Documents and Settings\user>nslookup www.time.com
Server:  apple
Address:  222.201.130.30

Non-authoritative answer:
Name:    mags1.gtimeinc.aol.com
Address:  205.188.238.109
Aliases:  www.time.com
```

图 2-11 nslookup 域名解析



在命令提示符下输入：

```
nslookup 205.188.238.109
```

结果显示 205.188.238.109 主机的域名为 `www1.pathfinder.aol.com`，如图 2-12 所示。值得注意的是，IP 地址与域名并不是严格的一对一映射，往往由于某些需要被配置为多对一或一对多的映射。



```
C:\Documents and Settings\user>nslookup 205.188.238.109
Server:  apple
Address:  222.201.130.30

Name:     www1.pathfinder.aol.com
Address:  205.188.238.109
```

图 2-12 nslookup 反向域名解析

#### 4. 实验心得与体会