第3章

常用网络命令

【实验内容】

常用网络命令及使用

【实验目的与要求】

- 掌握常用网络命令的用途及使用方法
- 学会使用常用网络命令对网络进行检测与配置

实验 3　常用网络命令及使用

在人们平常的网络使用过程中，经常会有一些特定的需求，比如需要查看 IP 地址、测试网络是不是连通的、查询某个域名对应的 IP 地址是多少、查询物理地址、对发出去的数据包进行跟踪，等等。虽然也有人编写了专门的工具用于完成这些任务，但实际上，可以有更简单的办法——网络命令。虽然目前的操作系统都是图形界面，但一些在命令行下面使用的常用网络命令依旧十分有用。对这些命令有常识性的了解，将有益于更好地使用和维护计算机网络。

在 Windows 操作系统中，单击“开始”→“运行”→输入“cmd”，即可进入命令提示符运行模式。或者，也可以使用快捷键 Win＋R 快速打开运行窗口，再输入“cmd”即可。当然，如果还是觉得麻烦，也可以自己定义一个直接打开命令提示符界面的快捷键。单击“开始”→“附件”→“命令提示符”→“属性”→“快捷方式”，其中有一项是“快捷键”，默认为“无”，该输入框中的内容是无法编辑的。这时候可以直接按下键盘上的某个键，比如 C 键，就可以看到它自动设置了快捷键为 Ctrl＋Alt＋C，如图 3-1 所示，单击“确定”按钮。现在回到桌面上按 Ctrl＋Alt＋C 键试一试，命令提示符窗口就出来了。

图 3-1　设置“命令提示符”的快捷键

打开命令提示符窗口之后，就可以在其中执行网络命令了。只要输入相应的命令代码，即会返回对应的结果。

下面介绍比较常用的 10 个网络命令。

3.1 ping

ping 是一个使用频率极高的实用命令，主要用于确定网络的连通性。这对确定网络是否正确连接以及网络连接的状况十分有用。简单地说，ping 就是一个测试程序，如果 ping 运行正常，大体上就可以排除网络访问、网卡、输入输出线路、电缆和路由器等存在的故障，从而缩小排除网络故障问题的范围。

ping 能够以毫秒为单位显示发送请求到返回应答之间的时间量。如果应答时间短，通常表示数据报不必通过太多的路由器或网络，连接速度比较快。ping 还能显示 TTL（Time To Live，生存时间）值，通过 TTL 值可以大致推算数据包通过了多少个路由器，路由器个数＝源地点 TTL 起始值（比返回 TTL 大的最小 2 的乘方数）－返回时 TTL 值。如返回 TTL 值为 119，那么比返回 TTL 大的最小 2 的乘方数应为 128，则经过的路由器个数为 9（128－119）。

3.1.1 格式和选项

```
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] [ - 4] [ - 6] target_name
```

格式中的“[ ]”内容为选项，其意义如下。

-t：ping 指定的主机，直到停止。

若要查看统计信息并继续操作，请输入 Control-Break；若要停止，请输入 Control-C。

-a：将地址解析成主机名。

-n count：要发送的回显请求数。

-l size：发送缓冲区大小。

-f：在数据包中设置“不分段”标志（仅适用于 IPv4）。

-i TTL：生存时间。

-v TOS：服务类型（仅适用于 IPv4。该设置已不赞成使用，且对 IP 标头中的服务字段类型没有任何影响）。

-r count：记录计数跃点的路由（仅适用于 IPv4）。

-s count：计数跃点的时间戳（仅适用于 IPv4）。

-j host-list：与主机列表一起的松散源路由（仅适用于 IPv4）。

-k host-list：与主机列表一起的严格源路由（仅适用于 IPv4）。

-w timeout：等待每次回复的超时时间（ms）。

-R：同样使用路由标头测试反向路由（仅适用于 IPv6）。

-S srcaddr：要使用的源地址。

-4：强制使用 IPv4。

-6：强制使用 IPv6。

3.1.2 说明

按照默认设置，Windows 上运行的 ping 命令发送 4 个 ICMP（Internet Control Message Protocol，网间控制报文协议）回送请求，每个 32 字节数据，如果正常，应能得到 4 个回送应答。

3.1.3 实例

1. 测试本机是否连通

输入“ping 本机 IP 地址或 ping 127.0.0.1”，该命令将回送数据报送给本地计算机所配置的 IP 地址，本地计算机应该对 ping 命令做出应答。如果没有，则表示本地配置或安装存在问题。若出现此问题，请先断开网络电缆，然后重新发送该命令，如果网线断开后该命令运行正常，则表明有另外计算机配置的 IP 地址与本机 IP 地址相同，如图 3-2 所示。

图 3-2 对本机进行测试

另外，ping localhost 在某些场合也是必要的。

local host 是系统的网络保留名，它是 127.0.0.1 的别名，每台计算机都应该能够将该名字转换成该地址。否则，表示主机文件（/Windows/host）中存在问题。

2. 测试与局域网内其他计算机是否连通

输入“ping 局域网内其他计算机 IP 地址”，该命令将回送数据报送给指定的 IP 地址的计算机，数据报经过本地计算机网卡及连接的网络电缆到达其他计算机，再返回回送应答。若收到回送应答，则表明本地计算机中的网卡和网络电缆正常。如果收到 0 个回送应答，则表明子网掩码不正确或网卡配置错误或电缆系统有问题。

3. 测试网关连通情况

输入“ping 网关 IP 地址”，若该命令应答正确，表明与本机连接的网关路由器正在运行

并能够连通。

4. 远程连通测试

输入“ping 远程计算机 IP 地址”，如果收到 4 个应答，表示成功地使用了默认网关。对于拨号上网用户则表示能够成功地访问 Internet(但不排除 ISP 的 DNS 会有问题)。

5. 测试 DNS 是否正常

输入“ping 域名地址(如 www.yahoo.com.cn)”，采用域名地址访问，通常需要 DNS 服务转换，所以该命令一方面可以测试网络是否连通，另一方面可以测试 DNS 服务器是否运行正常。如果出现错误提示，则表明 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障。

3.2 ipconfig

ipconfig 实用程序可用于显示当前的 TCP/IP 配置的设置值。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。

如果计算机和所在的局域网使用了动态主机配置协议 DHCP，使用 ipconfig 命令可以了解到计算机是否成功地租用到了一个 IP 地址，如果已经租用到，则可以了解它目前得到的是什么地址，包括 IP 地址、子网掩码和默认网关等网络配置信息。

3.2.1 格式和选项

```
ipconfig [/all|/renew [adapter]|/release[adapter]]
```

格式中选项的意义如下。

当使用不带任何参数选项 ipconfig 命令时，显示每个已经配置了的接口的 IP 地址、子网掩码和默认网关值。

/all：产生完整显示。在没有该参数的情况下 ipconfig 只显示 IP 地址、子网掩码和每个网卡的默认网关值。

/release 或/renew [adapter]：这两个参数只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果使用 ipconfig /release，那么所有接口的租用 IP 地址将重新交付给 DHCP 服务器(归还 IP 地址)。如果使用 ipconfig /renew，那么本地计算机将设法与 DHCP 服务器取得联系，并租用一个 IP 地址。但在大多数情况下网卡将被重新赋予和以前所赋予的相同的 IP 地址。要查看适配器名称，可输入不带参数的 ipconfig 命令便可显示适配器名称。

3.2.2 实例

显示本地计算机所有已经配置了的接口配置情况，如图 3-3 所示。

图 3-3 查看本机 IP 地址

3.3 arp

arp 是 TCP/IP 协议族中的一个重要协议，用于确定对应 IP 地址的网卡物理地址。

使用 arp 命令，能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。此外，使用 arp 命令可以人工方式设置静态的网卡物理地址/IP 地址对，使用这种方式可以为默认网关和本地服务器等常用主机进行本地静态配置，这有助于减少网络上的信息量。

按照默认设置，ARP 高速缓存中的项目是动态的，每当向指定地点发送数据并且此时高速缓存中不存在当前项目时，ARP 便会自动添加该项目。

3.3.1 格式和选项

```
arp [ - a [InetAddr] [ - N IfaceAddr]] [ - g [InetAddr] [ - N IfaceAddr]] [ - d InetAddr
[IfaceAddr]] [ - s InetAddr EtherAddr [IfaceAddr]]
```

格式中选项的意义如下。

-a [InetAddr] [-N IfaceAddr]：通过询问当前协议数据，显示当前 ARP 项。要显示指定 IP 地址的 ARP 缓存项，则应该使用带有 InetAddr 参数的 arp -a，此处的 InetAddr 代表指定的 IP 地址。要显示指定接口的 ARP 缓存表，则使用-N IfaceAddr 参数，此处的 IfaceAddr 代表分配给指定接口的 IP 地址。-N 参数区分大小写。此外，如果不止一个网络接口使用 ARP，则显示每个 ARP 表的项。

-g：与-a 相同。

-d InetAddr [IfaceAddr]：删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表分配给该

接口的 IP 地址。inet_addr 可以是通配符 *，以删除所有主机。

-s InetAddr EtherAddr [IfaceAddr]：向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 ARP 缓存项，则使用 IfaceAddr 参数，此处的 IfaceAddr 代表分配给该接口的 IP 地址。

3.3.2 说明

(1) InetAddr 和 IfaceAddr 的 IP 地址用带圆点的十进制记数法表示。物理地址 EtherAddr 由 6 个字节组成，这些字节用十六进制记数法表示并且用连字符隔开(如 00-AA-00-4F-2A-9C)。

(2) 通过-s 参数添加的项属于静态项，它们不会在 ARP 缓存中超时。如果终止 TCP/IP 协议后再启动，这些项会被删除。要创建永久的静态 ARP 缓存项，请在批处理文件中使用适当的 ARP 命令，并通过“计划任务程序”在启动时运行该批处理文件。

(3) 只有当网际协议(TCP/IP)在网络连接中安装为网络适配器属性的组件时，该命令才可用。

3.3.3 实例

(1) 查看 ARP 高速缓存中所有物理/IP 地址对内容，输入“arp -a”，如图 3-4 所示。

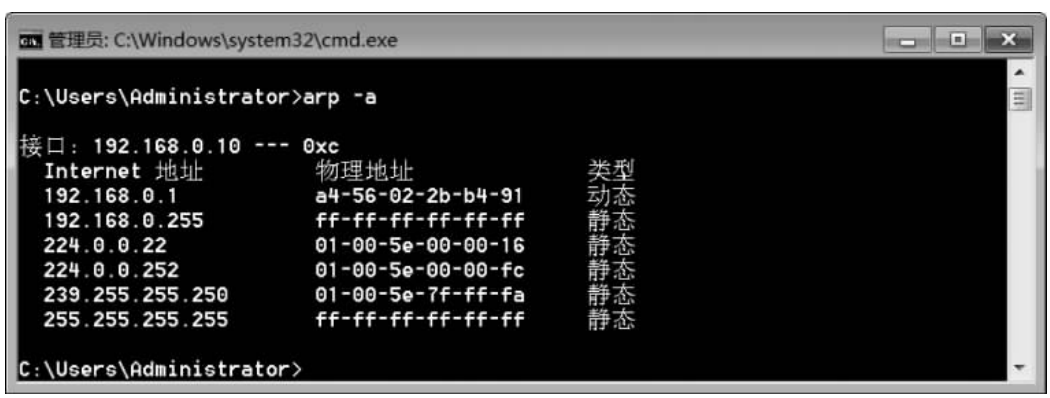

图 3-4 查看 ARP 高速缓存

(2) 如果某台计算机有多块网卡，那么使用 arp-a 加上接口的 IP 地址，即输入“arp -a IP”，就可以只显示与该接口相关的 ARP 缓存内容。

(3) 向 ARP 高速缓存中人工输入一个静态地址对，输入“arp -s IP 物理地址”，如：arp -s 157.55.85.212 00-aa-00-62-c6-09。

(4) 人工删除一个静态地址对，输入“arp -d IP”。

3.4 tracert

该命令主要用来显示数据包到达目标主机的一组路由器，以及到达每个跃点(hop)的时间。即用来显示数据包到达目的主机所经过的路径。

3.4.1 格式和选项

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

格式中选项的意义如下。

-d：不将地址解析成主机名。

-h maximum_hops：搜索目标的最大跃点数。

-j host-list：与主机列表一起的松散源路由(仅适用于 IPv4)。

-w timeout：等待每个回复的超时时间(以 ms 为单位)。

-R：跟踪往返行程路径(仅适用于 IPv6)。

-S srcaddr：要使用的源地址(仅适用于 IPv6)。

-4：强制使用 IPv4。

-6：强制使用 IPv6。

3.4.2 说明

(1) 该命令用 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。

(2) 如果数据包不能到达目标，将显示成功转发数据包的最后一个路由器。

(3) Tracert 命令功能同 Ping 类似，但它所获得的信息要比 Ping 命令更详细，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来，该命令比较适用于大型网络。

(4) 如果源从任何给定的路由器接收到的报文少于三条(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三次的往返时间。

(5) 此外，tracert 命令还可以用来查看网络在连接站点时经过的步骤或采取哪种路线，如果是网络出现故障，就可以通过这条命令查看出现问题的位置。

3.4.3 实例

返回到达 IP 地址所经过的路由器列表，输入“tracert [-d] IP address”。使用-d 选项，将快速显示所经过的路由器的路径，因为 tracert 不尝试解析路径中路由器的名称，如图 3-5 所示。

3.4.4 拓展

(1) 多尝试几次“ping www.baidu.com”操作，比较得到的百度的 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) 对于大型网络中的某站点进行 tracert 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)。

图 3-5 本地主机到 Baidu 服务器的路由追踪

(3) 在一天的不同时段内,用 tracert 程序多次测试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?

3.5 nslookup

nslookup 的功能是查询任何一台机器的 IP 地址和其对应的域名。它通常需要一台域名服务器来提供域名。如果用户已经设置好域名服务器,就可以用这个命令查看不同主机的 IP 地址对应的域名。

3.5.1 格式和选项

```
nslookup [ - option ...] [computer - to - find | - [server]]
```

格式中选项的意义如下。

-option...: 将一个或多个 nslookup 命令指定为命令行选项。每个选项均由连字符"-"后紧跟命令名组成,有时是等号"="后跟一个数值,命令行长度不能超过 254 个字符。

computer-to-find: 使用当前默认的服务器或使用指定的 server 来查找 computer-to-find 的信息。如果 computer-to-find 是 IP 地址,则返回计算机的名称。如果 computer-to-find 是名称,并且没有后缀句点,则默认的 DNS 域名附加到该名称上。要查找不在当前 DNS 域的计算机,请在名称上附加句点。如果输入连字符"-"代替 computer-to-find,则进入 nslookup 交互状态; 要从交互状态返回 DOS 状态,则输入 exit 命令。

Server: 指定服务器作为 DNS 名称服务器,若省略 server,将使用默认的 DNS 名称服务器。

3.5.2 说明

nslookup 有交互式和非交互式两种模式。

如果仅需要查找一块数据，则只要使用非交互模式即可。若采用非交互模式，则命令后的第一个参数为要查找的计算机的名称或 IP 地址，第二个参数为指定的 DNS 名称服务器的名称或 IP 地址。如果省略第二个参数，则使用默认的 DNS 名称服务器。

如果需要查找多块数据，则通常使用交互模式。若采用交互模式，则命令后的第一个参数为连字符“-”，第二个参数为指定的 DNS 名称服务器的名称或 IP 地址，或者省略第二个参数，使用默认的 DNS 名称服务器。

3.5.3 实例

(1) 在本地机上使用 nslookup 命令，可在命令行输入 nslookup，屏幕显示图 3-6。

图 3-6 本机 nslookup

在符号“>”后面输入要查询的 IP 地址或域名并回车即可。如果要退出该命令，输入 exit 并回车即可。

(2) 查找指定的域名(www. tzc. edu. cn)的计算机名和 IP 地址，则在命令行输入 nslookup www. tzc. edu. cn，屏幕显示结果如图 3-7 所示。

图 3-7 nslookup 查找指定域名

3.6 hostname

显示当前计算机(主机)的名称。

3.6.1 格式和选项

hostname

3.6.2 实例

在命令行下直接输入 hostname,得到图 3-8 所示的结果,即为当前计算机(主机)名称。

图 3-8 利用 hostname 查询当前主机名称

3.7 netstat

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(包括 IP、ICMP、TCP 和 UDP)以及 IPv6 统计信息(包括 IPv6、ICMPv6、TCP v6 和 UDPv6)。如果不带参数,netstat 显示活动的 TCP 连接。

3.7.1 格式和选项

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

格式中选项的意义如下。

-a:显示所有活动的 TCP 连接的端口号,以及计算机侦听到的 TCP 和 UDP 端口号。

-e:显示以太网统计信息,如发送和接收的字节数、数据包数。该参数可以与-s 结合使用。

-n:以数字表格形式显示地址和端口。

-o:显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。

-p Protocol:显示 Protocol 所指定的协议的连接。Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。如果该参数与-s 一起使用,则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6。

-s：显示每个协议的使用状态。默认情况显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 IPv6 协议，还会显示 TCPv6、UDPv6、ICMPv6 和 IPv6 协议的统计信息。

-r：显示本机的 IP 路由表内容，该参数与 route print 命令等价。

Interval：每隔 Interval 秒重新显示一次选定的信息，按 Ctrl＋C 键停止重新显示统计信息。

3.7.2 说明

(1) Netstat 提供下列统计信息。

Proto——协议的名称(TCP 或 UDP)。

Local Address——本地计算机的 IP 地址和正在使用的端口号。如果不指定-n 参数，就显示与 IP 地址和端口的名称对应的本地计算机名称。如果端口尚未建立，端口以星号“*”显示。

Foreign Address——连接该插槽的远程计算机的 IP 地址和端口号码。如果不指定-n 参数，就显示与 IP 地址和端口对应的名称。如果端口尚未建立，端口以星号“*”显示。

State——表明 TCP 连接的状态。可能的状态有 CLOSE_WAIT、CLOSED、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2、LAST_ACK、LISTEN、SYN_RECEIVED、SYN_SEND、TIMED_WAIT。

(2) 只有当网际协议(TCP/IP)在网络连接中安装为网络适配器属性的组件时，该命令才可用。

3.7.3 实例

(1) 显示活动的 TCP 连接，显示结果如图 3-9 所示。

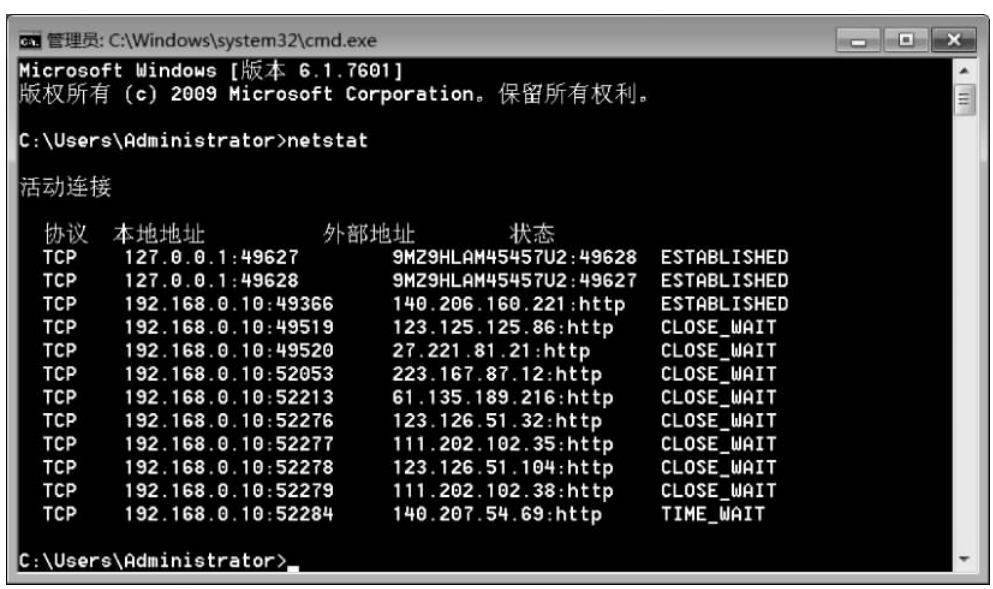

图 3-9 利用 netstat 查询显示活动的 TCP 连接

(2) 显示以太网统计信息,输入命令 netstat -e,显示结果如图 3-10 所示。

图 3-10 利用 netstat 查询显示以太网统计信息

(3) 显示以太网统计信息和所有协议的统计信息,输入命令 netstat -e -s。

(4) 仅显示 TCP 和 UDP 的统计信息,输入命令 netstat -s -p tcp udp。

(5) 每 5 秒钟显示一次活动的 TCP 连接和进程 ID,输入命令 netstat -o 5。

(6) 以数字形式显示活动的 TCP 连接和进程 ID,输入命令 netstat -n -o。

3.8 nbtstat

用于显示协议统计和当前 TCP/IP 连接,只有在安装了 TCP/IP 协议之后才可用。TCP/IP 上的 NetBIOS 将 NetBIOS 名称解析为 IP 地址。TCP/IP 为 NetBIOS 名称解析提供了许多选项,其中包括本地缓存查找、WINS 服务器查询、广播、DNS 服务器查询以及 LMHOSTS 和 HOSTS 查找。命令是一种用于排除 NetBIOS 名称解析问题的工具,可以使用 NBTSTAT 命令删除或更正预加载的项目。

3.8.1 格式和选项

```
nbtstat [ - a remotename] [ - A IP address] [ - c] [ - n] [ - R] [ - r] [ - S] [ - s] [interval]
```

格式中选项的意义如下。

-a remotename: 显示远程计算机的 NetBIOS 名称表,其中,remotename 是远程计算机的 NetBIOS 计算机名称。

-A IPAddress: 显示远程计算机的 NetBIOS 名称表,其名称由远程计算机的 IP 地址指定(以小数点分隔)。其实参数-a 也可以用远程计算机的 IP 地址,也就是参数-a 已包含参数-A 的功能。

-c: 给定每个名称的 IP 地址并列出 NetBIOS 名称缓存的内容。

-n: 列出本地 NetBIOS 名称。此参数和 netstat -a 类似,参数-a 是检查远程的,而它是检查本地的,如果把 netstat -a 后面的 IP 采用本地的 IP 地址,就和 netstat -n 的效果一样

了。其中的状态是用于标识该名称是通过广播或 WINS 服务器注册的。

-r：显示 NetBIOS 名称解析统计资料。在配置使用 WINS 的 Windows 2000 计算机上，此选项返回要通过广播或 WINS 来解析和注册的名称数。

-R：清除 NetBIOS 名称缓存的内容，并从 Lmhosts 文件中重新加载带有 #PRE 标记的项目。

-RR：重新释放并刷新通过 WINS 注册的本地计算机的 NetBIOS 名称。

-s：显示 NetBIOS 客户和服务器会话，并试图将目标 IP 地址转化为名称。

-S：显示 NetBIOS 客户和服务器会话，只通过 IP 地址列出远程计算机。

Interval：每隔 Interval 秒重新显示选择的统计资料，按 Ctrl+C 键停止重新显示统计信息。

3.8.2 说明

(1) nbtstat 命令行参数区分大小写。

(2) 由 nbtstat 产生的列标题的含义如表 3-1 所示。

表 3-1 nbtstat 产生的列标题含义

标 题	说 明
Input	接收的字节数
Output	发送的字节数
In/Out	该连接是传出还是传入
Lift	名称表缓存项在被清除之前所保存的时间
Local Name	本地 NetBIOS 名称
Remote Host	远程计算机 NetBIOS 名称

(3) Type(名称类型)有两类，分别为 Unique (单个名称)和 Group(组名称)。

(4) State NetBIOS 可能的连接的状态如表 3-2 所示。

表 3-2 NetBIOS 可能的连接状态

状 态	说 明
已连接	会话已建立
关联	连接的终结点已经被创建并与 IP 地址关联
正接听	该终结点对内向连接可用
空闲	该结束点已被打开但不能接收连接
正在连接	会话处于连接阶段
接收	入站会话当前正在被接收，将在短期内连接
重新连接	会话将试图重新连接
出站	会话正处于连接阶段，此阶段正在创建 TCP 连接
入站	入站会话正在连接期
正在断开	会话正在断开连接
已中断连接	本地计算机已断开连接，并正等待远程系统的确认

(5) 只有当网际协议(TCP/IP)在网络连接中安装为网络适配器属性的组件时，该命令才可用。

3.8.3 实例

(1) 显示 NetBIOS 计算机名为 TZC_JSJ 的远程计算机的 NetBIOS 名称表,输入:nbtstat -a TZC_JSJ。

(2) 显示所分配 IP 地址为 10.0.0.99 的远程计算机的 NetBIOS 名称表,输入:nbtstat -A 10.0.0.99。

(3) 显示本地计算机的 NetBIOS 名称表,输入 nbtstat -n,显示结果如图 3-11 所示。

图 3-11 显示计算机的 NetBIOS 本地名称表

(4) 显示本地计算机 NetBIOS 名称缓存的内容,输入 nbtstat -c。

(5) 清除 NetBIOS 名称缓存并重新装载本地 Lmhosts 文件中带标记#PRE 的项目,输入 nbtstat -R。

(6) 释放通过 WINS 服务器注册的 NetBIOS 名称并对其重新注册,输入 nbtstat -RR。

(7) 每隔 5s 以 IP 地址显示 NetBIOS 会话统计资料,输入 nbtstat -S 5。

3.9 route

大多数主机一般都驻留在只连接一台路由器的网段上。由于只有一台路由器,因此不存在选择使用哪一台路由器将数据包发送到远程计算机上去的问题,该路由器的 IP 地址可作为该网段上所有计算机的默认网关。

但是,当网络上拥有两个或多个路由器时,用户就不一定想只依赖默认网关了。实际上可能想让某些远程 IP 地址通过某个特定的路由器来传递,而其他的远程 IP 则通过另一个路由器来传递。在这种情况下,用户需要相应的路由信息,这些信息储存在路由表中,每个主机和每个路由器都配有自己独一无二的路由表。大多数路由器使用专门的路由协议来交换和动态更新路由器之间的路由表。但在有些情况下,必须人工将项目添加到路由器和主

机上的路由表中。route 命令就是管理本机路由表，可以查看、添加、修改或删除路由表条目。

3.9.1 格式和选项

```
route [ - f] [ - p] [command [destination] [mask subnetmask] [gateway] [metric costmetric]]
```

格式中选项的意义如下。

command：为子命令，作用如表 3-3 所示。

表 3-3 command 可用的命令

命 令	用 途
Print	输出路由列表
Add	添加路由
Delete	删除路由
Change	更改现存路由

-f：清除所有不是主机路由(子网掩码为 255.255.255.255 的路由)、环回网络路由(目标为 127.0.0.0，子网掩码为 255.255.255.0 的路由)或多播路由(目标为 224.0.0.0，子网掩码为 240.0.0.0 的路由)的所有路由条目。如果该参数与 add、change、delete 之一命令结合使用，则先清除后执行命令。

-p：若与 add 命令一起使用，则将指定的路由添加到注册表中，即成为永久的静态路由，在启动 TCP/IP 协议时表态路由会自动初始化 IP 路由表；若与 print 命令一起使用，则显示永久表态路由列表；若与其他子命令一起使用，将忽略此参数。

Destination：指定目标地址。目标地址可以是网络 IP 地址(主机号为 0 的 IP 地址)、主机 IP 地址或默认路由的 IP 地址(默认路由 IP 地址为 0.0.0.0)。

mask subnetmask：指定与目标地址相关联的子网掩码，其中主机路由子网掩码为 255.255.255.255、默认路由子网掩码为 0.0.0.0。如果忽略该参数，则子网掩码默认为 255.255.255.255。

Gateway：指定网关 IP 地址。用于告诉路由器应从哪个 IP 地址转发数据包才能达到目的网络。若目标地址为本地子网的 IP 地址，则网关地址为分配给连接子网接口的 IP 地址；若目标地址为经过一个或多个路由器才可到达的远程路由，则网关地址为一个分配给相邻路由器的、可直接到达的 IP 地址。

metric Metric：指定度量值，范围为 1～9999。Windows 一般不查看度量值，当有多条路径通向目标地址时，Windows 将查看度量值以确定最短或最可靠的路径，所以该参数是用来选择与目标地址最为匹配的路由。

if Interface：该参数用于告诉 Windows 使用哪一块网卡(接口索引)。接口索引可以使用十进制或十六进制表示，若为十六进制，则需在十六进制数前加 0x。若忽略 if 参数，则接口由网关地址确定。

3.9.2 说明

(1) route print 用于显示路由表中的当前项目，在单个路由器网段上的输出结果。

(2) route add 可以将路由项目添加给路由表。例如,如果要设定一个到目的网络209.99.32.33的路由,其间要经过5个路由器网段,首先要经过本地网络上的一个路由器IP为202.96.123.5,子网掩码为255.255.255.224,那么用户应该输入以下命令。

```
route add 209.99.32.33 mask 255.255.255.224 202.96.123.5 metric 5
```

(3) route change 可以用来修改数据的传输路由,不过,用户不能使用本命令来改变数据的目的地。下面这个例子将上例路由改变采用一条包含三个网段的路径。

```
route add 209.99.32.33 mask 255.255.255.224 202.96.123.250 metric 3
```

(4) route delete 可以从路由表中删除路由。例如 route delete 209.99.32.33。

(5) 如果是 print 或 delete 命令,可以忽略 Gateway 参数,也可以使用通配符来表示目标和网关。通配符是指星号“*”或问号“?”,星号代表任意一串字符,问号代表任一个字符。如10.*.1,192.168.*、127.*和*224*都是星号通配符的有效使用。

(6) 使用了无效的目标和子网掩码值的组合,会显示“Route:bad gateway address netmask”错误消息。目标中有一位或多位设置为1,而其在子网掩码中的对应位设置为0时就会发生此类错误。

3.9.3 实例

(1) 显示IP路由表的完整内容,输入 route print,如图3-12所示。

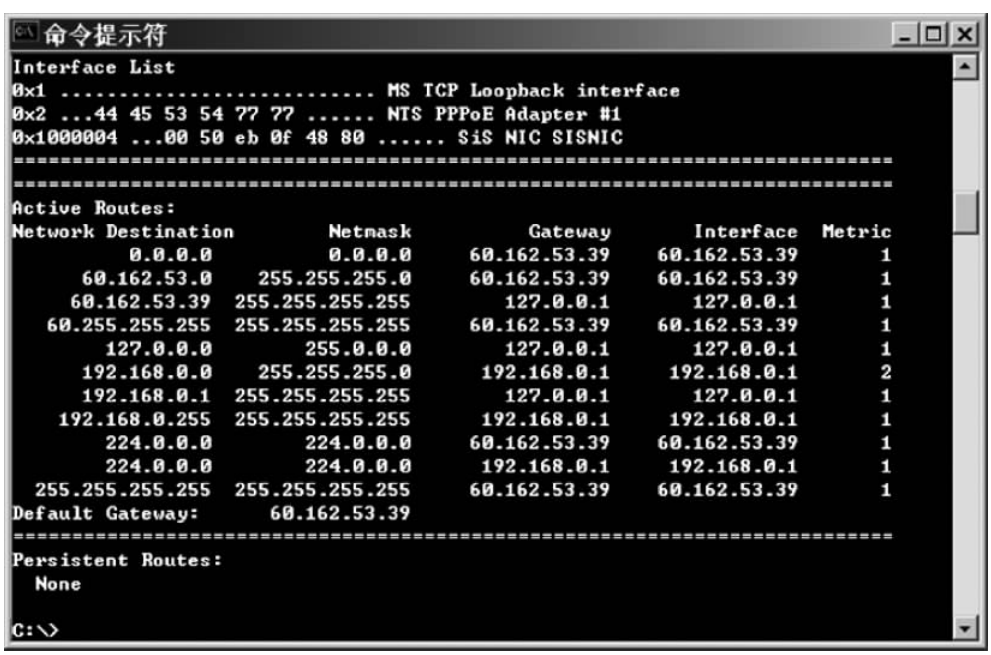

图3-12 本机上的完整路由表

图3-12中的第一列是网络目的地址,列出了路由器连接的所有的网段;第二列为子网掩码,提供了该网段的子网掩码;第三列为网关IP地址;第四列为接口列,仅指定路由器中

的网卡 IP 地址，然后路由器从该地址绑定的物理网卡转发数据包；最后一列为度量。

(2) 显示 IP 路由表中以 10.开始的路由，输入 route print 10. * 。

(3) 添加默认网关地址为 192.168.12.1 的默认路由，输入 route add 0.0.0.0 mask 0.0.0.0 192.168.12.1。

(4) 添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1 的路由，输入 route add 10.41.0.0 mask 255.255.0.0 10.27.0.1。

(5) 添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1 的永久路由，输入 route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1。

(6) 添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1，跃点数为 7 的路由，输入 route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metric 7。

(7) 添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1，接口索引为 0x3 的路由，输入 route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 if 0x3。

(8) 删除目标为 10.41.0.0，子网掩码为 255.255.0.0 的路由，输入 route delete 10.41.0.0 mask 255.255.0.0。

(9) 删除 IP 路由表中以 10.开始的所有路由，输入 route delete 10. * 。

(10) 要将目标为 10.41.0.0，子网掩码为 255.255.0.0 的路由的下一个跃点地址由 10.27.0.1 更改为 10.27.0.25，输入 route change 10.41.0.0 mask 255.255.0.0 10.27.0.25。

3.10 net

在命令行输入 net help command，可以在命令行获得 net 命令的语法帮助。例如，要得到关于 net accounts 命令的帮助信息，可输入“net help accounts”。

所有 net 命令都可以使用/y 和/n 命令行选项。例如，net stop server 命令用于提示用户确认停止所有依赖的服务器服务，net stop server/y 表示确认停止并关闭服务器服务。

3.10.1 格式和选项

```
net [accounts |computer| config | continue |file| group | help | helpmsg | localgroup | pause |
session | share | start |statistics | stop | time | use | user | view ]
```

格式中选项的意义如表 3-4 所示。

表 3-4 选项意义

选　项	例　子	意　义
accounts	net accounts	查阅当前账号设置
config	net config server	查阅本网络配置信息统计
group	net group	查阅域组(在域控制器上)
print	net print\\printserver\printer1	查阅或修改打印机映射
send	net send server1 “test message”	向别的计算机发送消息或广播消息
share	net share	查阅本地计算机上共享文件

续表

选　项	例　子	意　义
start	net start messenger	启动服务
statistics	net statistics server	查阅网络流量统计值
stop	net stop messenger	停止服务
use	net use x:\\server1\admin	将网络共享文件映射到一个驱动器字母
user	net user	查阅本地用户账号
view	net view	查阅网络上可用计算机

3.10.2 说明

net 命令的执行结果有许多与其他 Windows 管理工具所得到的结果相似。但是，net 命令可以在一个地方提供所有信息，并可以把结果重定向到打印机或一个标准的文本文件中。

许多服务所使用的网络命令都以 net 开头，这些 net 命令有一些公用属性。

3.10.3 实例

显示网络流量统计值，输入：net config server，如图 3-13 所示。

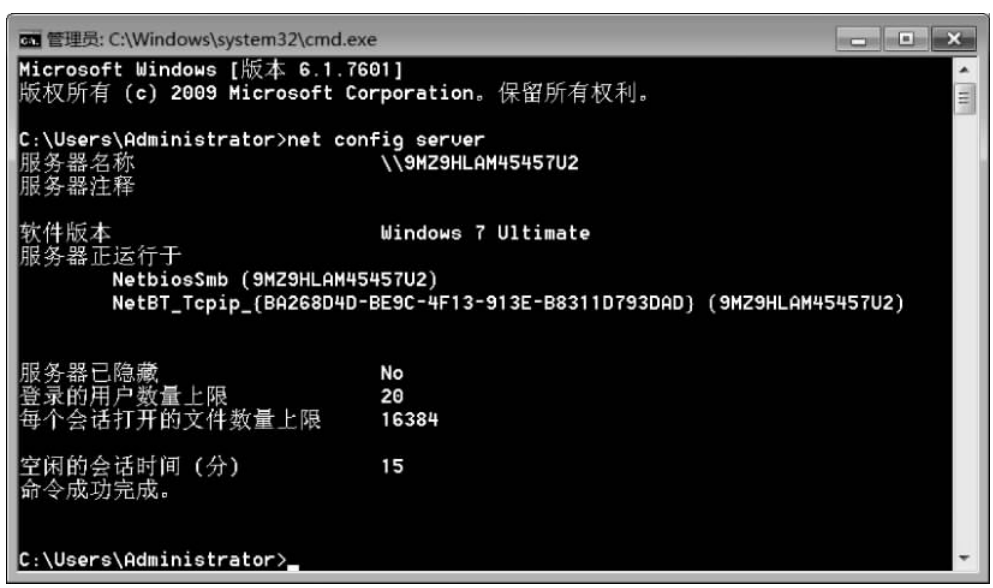

图 3-13 查阅本网络配置信息统计

思考题

(1) 如何绑定本机物理地址和 IP 地址？

(2) 在测试两台主机之间的网络连通性时，能不能规定测试的数据包数量？

（3）ping 命令的显示结果如图 3-14 所示，请问当前主机发送到 163 服务器的数据包累计通过了多少个路由器？

图 3-14　ping 命令结果