实验 1　网络命令的使用

1.1　实验目的

（1）了解常用网络命令的工作原理。
（2）掌握常用网络命令的使用。

1.2　实验条件

（1）能够接入 Internet 的局域网。
（2）服务器端 Windows 2012 操作系统，客户机端 Windows 7 操作系统。

1.3　实验步骤

1.3.1　Ping 命令的使用技巧

Ping 是个使用频率极高的 ICMP 协议的程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。根据返回的信息，我们就可以推断 TCP/IP 参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示 TCP/IP 配置就是正确的，我们必须执行大量的本地主机与远程主机的数据报交换，才能确信 TCP/IP 的正确性。

简单地说，Ping 就是一个连通性测试程序，如果能 Ping 通目标，我们就可以排除网络访问层、网卡、Modem 的输入输出线路、电缆和路由器等存在的故障；如果 Ping 目标 A 通，而 Ping 目标 B 不通，则网络故障发生在 A 与 B 之间的链路上或 B 上，从而缩小故障的范围。

按照默认（缺省）设置，Windows 上运行的 Ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求，每个 32 字节数据，如果一切正常，我们应能得到 4 个回送应答。Ping 能够以毫秒为单位显示发送回送请求到返回

回送应答之间的时间量。如果应答时间短，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，我们可以通过 TTL 值推算数据包已经通过了多少个路由器。TTL 的初值通常是系统默认值，是包头中的 8 位的域。TTL 的最初设想是确定一个时间范围，超过此时间就把包丢弃。由于每个路由器都至少要把 TTL 域减 1，TTL 通常表示包在被丢弃前最多能经过的路由器个数。当记数到 0 时，路由器决定丢弃该包，并发送一个 ICMP 报文给最初的发送者。

另外，TTL 字段值可以帮助我们识别操作系统类型：

UNIX 及类 UNIX 操作系统，ICMP 回送应答的 TTL 字段值为 255。

Linux 系统和 Windows 10 系统，ICMP 回送应答的 TTL 字段值为 62。

微软 Windows 7/8 操作系统，ICMP 回送应答的 TTL 字段值为 128。

当然，返回的 TTL 值是相同的。但有些情况下特殊，如表 1-1 所示。

表 1-1　使用不同操作系统时，回送应答的 TTL 字段值

ICMP 回送应答的 TTL 字段值	操作系统类别
62	Linux Kernel 4.9.x
	Windows 10
128	Windows XP
	Windows 7
	Windows 8
255	FreeBSD 11.0
	Sun Solaris 10
	OpenBSD 6.0
	NetBSD 7.1
	HP UX 11.31

1.通过 Ping 检测网络故障的典型次序

正常情况下，当我们使用 Ping 命令来查找问题所在或检验网络运行情况时，我们需要使用许多 Ping 命令，如果所有 Ping 命令都运行正确，我们就可以相信基本的连通性和配置参数没有问题；如果某些 Ping 命令出现运行故障，它们也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障。

（1）Ping 127.0.0.1

Ping 环回地址，验证在本地计算机上是否正确地安装了 TCP/IP 协议，以及配置是否正确。

（2）Ping 本机 IP

这个命令被送到我们计算机所配置的 IP 地址，我们的计算机始终都应该对该 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。

（3）Ping 局域网内其他 IP

这个命令应该离开我们的计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明：本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那就表示子网掩码（进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码）不正确，或网卡配置错误，或电缆系统有问题。

（4）Ping 网关 IP

这个命令如果应答正确，表示局域网中的网关路由器正在运行，并能够做出应答。

（5）Ping 远程 IP

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（但不排除因特网服务提供商（ISP）的域名系统 DNS 会有问题）。

（6）Ping localhost

localhost（本地主机）是操作系统的网络保留名，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。如果没有做到这一点，则表示主机文件（/Windows/host）中存在问题。

（7）Ping www.×××.com

执行 Ping www.×××.com（如 www.163.com（网易）），通常是通过 DNS 服务器解析域名，如果这里出现故障，则表示本机 DNS 的 IP 地址配置不正确，或 DNS 服务器有故障（对于拨号上网用户，某些 ISP 已经不需要设置 DNS 服务器了）。顺便说一句：我们也可以利用该命令实现域名对 IP 地址的转换功能。

如果上面所列出的所有 Ping 命令都能正常运行，那么我们对自己的计算机进行本地和远程通信的功能基本上就可以放心了。但是，这并不表示我们所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

2. Ping 命令的常用参数选项

- -t：对指定的计算机一直进行 ping 操作，直到从键盘按 Ctrl+C 组合键中断为止。
- -a：将 IP 地址解析为计算机 NetBIOS（网络基本输入输出系统）名。
- -n：发送指定数量的 Echo（回应）数据包。这个命令可以自定义发送数据包的个数，对测试网络速度有帮助，默认值为 4。

1.3.2 Netstat 命令

Netstat（网络状态）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。

如果我们的计算机有时候接收到的数据报会导致出错（数据删除或故障），我们不必感到奇怪，TCP/IP 容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 IP 数据报相当大的百分比，或者它的数目正迅速增加，那么我们就应该使用 Netstat 查一查为什么会出现这些情况了。

1. Netstat 命令格式

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

Netstat 命令常用参数的含义说明如下。

- -a：本选项显示一个全部有效连接信息列表（-a 可被视为 all，即全部的意思），包括已建立的连接（Established），也包括监听连接请求（Listening）的那些连接。
- -b：本选项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的时间，如果没有足够权限可能失败。

- -e：本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量。
- -n：显示所有已建立的有效连接。
- -o：本选项显示与每个连接相关的所属进程 ID。
- -p proto：本选项显示 proto 指定的协议的连接；proto 可以是下列之一：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，ICMPv6，TCP，TCPv6，UDP 或 UDPv6。
- -r：本选项可以显示关于路由表的信息，除了显示有效路由外，还显示当前有效的连接。
- -s：本选项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。
- -v：与 –b 选项一起使用时，将显示包含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 组合键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）。

2. Netstat 命令的典型应用

（1）显示关于以太网的统计数据，显示结果如图 1-1 所示。

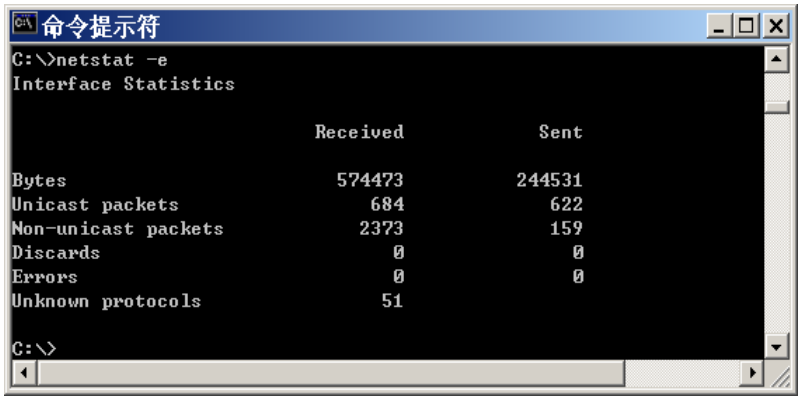

图 1-1　Netstat –e 命令的显示结果

（2）显示所有协议（如 TCP，UDP，IP 等）的使用状态，结果如图 1-2 所示。

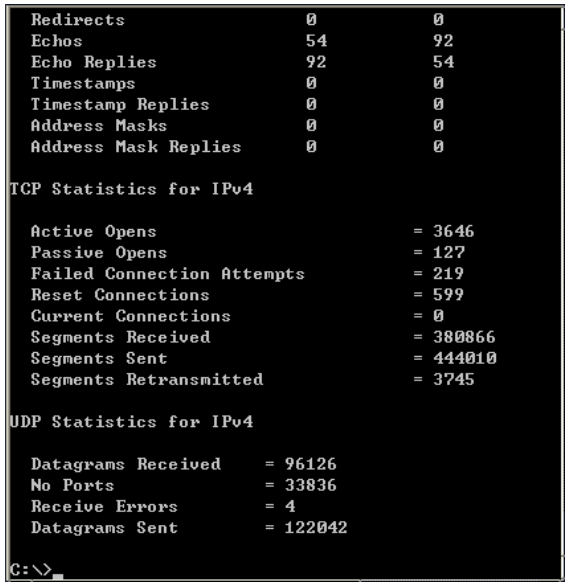

图 1-2　Netstat –s 命令的显示结果

1.3.3　IPconfig 命令

IPconfig 命令显示当前所有的 TCP/IP 配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。

1. IPconfig 命令格式

IPconfig [/all] [/renew [adapter]] [/release [adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassid adapter] [/setclassid adapter [classid]]

IPconfig 命令常用的参数含义说明如下。

- /all：显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下 IPconfig 只显示 IP 地址、子网掩码和各个适配器的默认网关值。
- /renew [adapter]：更新所有适配器（不带 adapter 参数）或特定适配器（带有 adapter 参数）的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上使用。要指定适配器名称，需输入使用不带参数的 IPconfig 命令显示的适配器名称。
- /release[adapter]：发送 DHCPRelease 消息到 DHCP 服务器，以释放所有适配器（不带 adapter 参数）或特定适配器（带有 adapter 参数）的当前 DHCP 配置，并丢弃 IP 地址配置。该参数可

以禁用配置为自动获取 IP 地址的适配器的 TCP/IP。要指定适配器名称，需输入使用不带参数的 IPconfig 命令显示的适配器名称。

2. IPconfig 命令的应用

（1)使用带/all 选项的 IPconfig 命令，给出所有接口的详细配置信息，如本机 IP 地址、子网掩码、网关、DNS、硬件地址（MAC 地址）等。结果如图 1-3 所示。

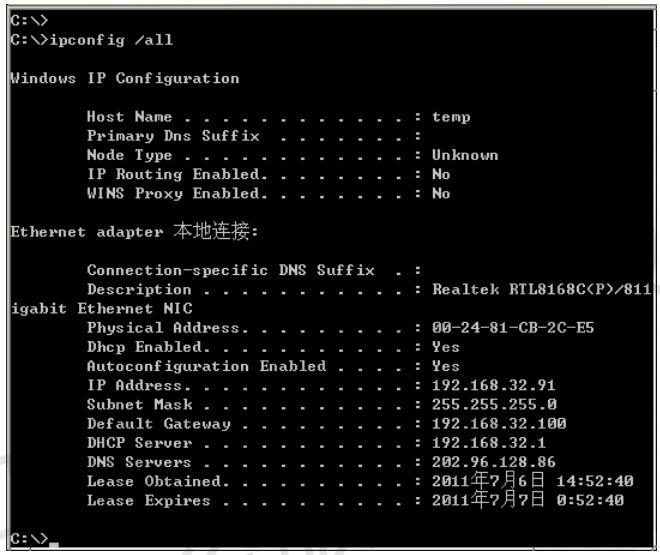

图 1-3　使用带/all 选项的 IPconfig 命令的显示结果

（2）对于启动 DHCP 的客户端，使用 IPconfig /renew 命令可以刷新配置，向 DHCP 服务器重新租用一个 IP 地址，大多数情况下网卡将重新赋予和以前所赋予的相同的 IP 地址，如图 1-4 所示。

图 1-4　使用 IPconfig /renew 命令的显示结果

1.3.4 ARP 命令

地址解析协议 ARP 是一个重要的 TCP/IP 协议，并且用于确定对应 IP 地址的网卡物理地址。使用 ARP 命令，我们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，也可以用人工方式输入静态的网卡物理/IP 地址对，我们可能会使用这种方式为默认网关和本地服务器等常用主机进行这项工作，以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，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。例如，在 Windows NT/2000 网络中，如果输入项目后不进一步使用，物理/IP 地址对就会在 2～10 分钟内失效。因此，如果 ARP 高速缓存中项目很少或根本没有，请不要奇怪，通过另一台计算机或路由器的 Ping 命令即可添加。所以，需要通过 ARP 命令查看高速缓存中的内容时，请最好先 Ping 此台计算机（不能是本机发送 Ping 命令）。

1. ARP 命令常用参数的含义

- -a：用于查看高速缓存中的所有项目。-a 和-g 参数的结果是一样的，多年来-g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项，而 Windows 用的是 arp -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的-g 选项。
- -d：删除指定的 IP 地址项。
- -s：向 ARP 高速缓存中人工输入一个静态项目。目的是让 IP 地址对应的 MAC 地址静态化，这样，病毒或攻击者就无法用伪造 MAC 地址的方法破坏局域网了。
- /?：在命令提示符下显示帮助。

2. ARP 命令的应用

查看高速缓存中的所有项目，如图 1-5 所示。

```
C:\>arp -a

Interface: 192.168.32.91 --- 0x4
  Internet Address      Physical Address      Type
  192.168.32.1          00-11-09-46-d8-f4     dynamic
  192.168.32.11         00-11-09-46-d7-b0     dynamic
  192.168.32.24         00-0d-87-04-e5-51     dynamic
  192.168.32.100        00-1a-a9-0b-9a-99     dynamic

C:\>_
```

图 1-5　查看高速缓存中的所有项目

1.3.5　Tracert 命令

Tracert 命令是跟踪路由路径的一个实用程序，用于确定数据报访问目标所经过的路径。

1. Tracert 命令格式

Tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name

Tracert 命令的各参数含义说明如下。

- -d：防止 Tracert 试图将中间路由器的 IP 地址解析为它们的名称，这样可加速显示 Tracert 的结果。
- –h maximum_hops：指定在搜索目标的路径中跃点的最大数，默认值为 30。
- –j computer-list：指定回送请求信息对于在 HostList 中指明的中间目标集实用 IP 报头中的“松散源路由”选项。主机列表中的地址或名称的最大数为 9，主机列表是一系列由空格分开的 IP 地址。
- –w timeout：每次应答等待 timeout（超时）指定的微秒数。
- target-name：目标主机名称或者 IP 地址。

2. Tracert 命令的应用

（1）在进行计算机网络日常维护时，经常使用不带任何参数选项的 Tracert 命令，如图 1-6 所示。

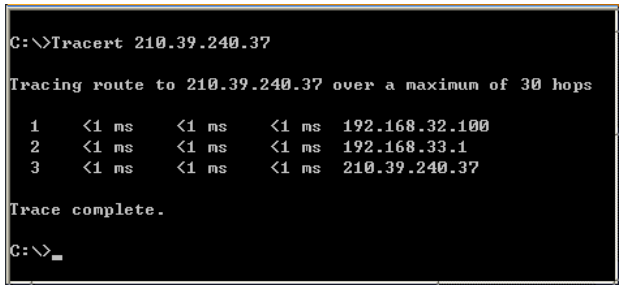

图 1-6　Tracert 命令的显示结果

（2）带 -d 参数的 Tracert 命令使用。例如，在本机查看网易服务器的路径信息，如图 1-7 所示。

利用 Tracert 命令，可以让人清楚地了解到 IP 数据包从“源”开始到“目标”访问的路径图，即这个过程所经过的路由、等待时间、数据包在网络上的停止位置等，从而帮助人们跟踪连接、测定网络连接断链处的位

置（一般表现为“*”号的点），这将为计算机网络故障的诊断与排除带来便利。

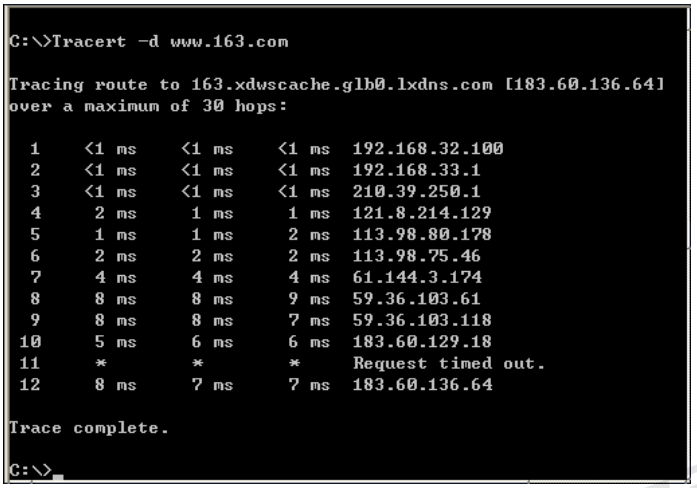

图 1-7　查看网易服务器的路径信息

1.3.6　NBtstat 命令

使用 NBtstat 命令释放和刷新 NetBIOS 名称。NBtstat（TCP/IP 上的 NetBIOS 统计数据）实用程序用于提供关于 NetBIOS 的统计数据。运用 NetBIOS，我们可以查看本地计算机或远程计算机上的 NetBIOS 名称表。

1. NBtstat 命令格式

NBtstat [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]

NBtstat 命令的各参数含义说明如下。

- –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 名称。NetBIOS 名称表是运行在该计算机上的应用程序使用的 NetBIOS 名称列表。
- –A IP address：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）。
- -c：显示 NetBIOS 名称缓存内容、NetBIOS 名称表及其解析的各个地址。
- -n：显示本地计算机的 NetBIOS 名称表。Registered 中的状态表明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。在配置为使用 WINS 的 Windows 计算机上，该参数将返回已通过广播和 WINS 解析

和注册的名称号码。

- –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：显示使用其 IP 地址的另一台计算机的 NetBIOS 连接表。
- -S：显示客户端和服务器会话，只通过 IP 地址列出远程计算机。
- interval：重新显示选择的统计资料，可以中断每个显示之间的 interval 中指定的秒数。按 Ctrl+C 组合键停止重新显示统计信息。如果省略该参数，NBtstat 将只显示一次当前的配置信息。

2. NBtstat 命令应用

知道对方 IP 地址，查对方主机的 MAC 地址，如图 1-8 所示。

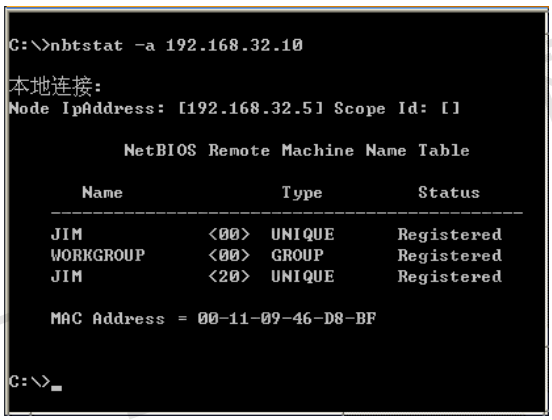

图 1-8　查对方主机的 MAC 地址显示结果

1.4　思考题

（1）你的计算机平时能正常上网，某天突然不能上网了，你能否查出是什么原因造成的？

（2）如何查出计算机的 MAC 地址？有多少种方法？

（3）在同一个局域网内，知道对方的 IP 地址，如何查出它的主机名？

1.5　实验报告

按照实验报告的格式要求书写实验报告。