

实验一 常用网络命令

1. 实验目的

- 掌握常用网络命令的使用方法；
- 熟悉和掌握网络管理、网络维护的基本内容和方法

2. 实验前的准备

- 阅读本实验的内容及操作步骤；弄清楚每个命令的作用及主要应用场景。

3. 实验内容

(1) ARP: 该命令可用于显示和修改 IP 地址与物理地址之间的转换表

ARP -s inet_addr eth_addr [if_addr]

ARP -d inet_addr [if_addr]

ARP -a [inet_addr] [-N if_addr]

-a 显示当前的 ARP 信息，可以指定网络地址

-d 删除由 inet_addr 指定的主机.可以使用* 来删除所有主机.

-s 添加主机，并将网络地址跟物理地址相对应，这一项是永久生效的。

eth_addr 物理地址.

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.

例子:

C:\>arp -a (显示当前所有的表项)

Interface: 10.111.142.71 on Interface 0x10000003

Internet Address	Physical Address	Type
10.111.142.1	00-01-f4-0c-8e-3b	dynamic //物理地址一般为 48 位
10.111.142.112	52-54-ab-21-6a-0e	dynamic

C:\>arp -a 10.111.142.1 (只显示其中一项)

Interface: 10.111.142.71 on Interface 0x10000003

Internet Address	Physical Address	Type
10.111.142.1	00-01-f4-0c-8e-3b	dynamic

C:\>arp -s 157.55.85.212 00-aa-00-62-c6-09 添加，可以再打入 arp -a 验证是否已经加入.

(2) Ipconfig: 该诊断命令显示所有当前的 TCP/IP 网络配置值。该命令在运行 DHCP 系统上的特殊用途, 允许用户决定 DHCP 配置的 TCP/IP 配置值。

```
ipconfig [/? | /all | /release [adapter] | /renew [adapter]
        | /flushdns | /registerdns
        | /showclassid adapter
        | /setclassid adapter [classidtoreset] ]
```

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

例如:

```
C:\>ipconfig
```

Windows 2000 IP Configuration

Ethernet adapter 本地连接:

```
Connection-specific DNS Suffix . :
IP Address. . . . . : 10.111.142.71      //IP 地址
Subnet Mask . . . . . : 255.255.255.0   //子网掩码
Default Gateway . . . . . : 10.111.142.1 //缺省网关
```

```
C:\>ipconfig /displaydns      //显示本机上的 DNS 域名解析列表
```

```
C:\>ipconfig /flushdns       //删除本机上的 DNS 域名解析列表
```

(3) Nbtstat: 该诊断命令使用 NBT (TCP/IP 上的 NetBIOS) 显示协议统计和当前 TCP/IP 连接。该命令只有在安装了 TCP/IP 协议之后才可用。

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

参数

-a remotename 使用远程计算机的名称列出其名称表。

-A IP address 使用远程计算机的 IP 地址并列出名称表。

-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。“已注册”表明该名称已被广播 (Bnode) 或者 WINS (其他节点类型) 注册。

-R 清除 NetBIOS 名称缓存中的所有名称后, 重新装入 Lmhosts 文件。

-r 列出 Windows 网络名称解析的名称解析统计。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。

-S 显示客户端和服务会话，只通过 IP 地址列出远程计算机。

-s 显示客户端和服务会话。尝试将远程计算机 IP 地址转换成使用主机文件的名称。

interval 重新显示选中的统计，在每个显示之间暂停 interval 秒。按 CTRL+C 停止重新显示统计信息。如果省略该参数，nbtstat 打印一次当前的配置信息。

例子：

C:\>nbtstat -A 周围主机的 ip 地址

C:\>nbtstat -c

C:\>nbtstat -n

C:\>nbtstat -S

本地连接：

Node IpAddress: [10.111.142.71] Scope Id: []

NetBIOS Connection Table

Local Name	State	In/Out	Remote Host	Input	Output
JJY	<03>	Listening			

另外可以加上间隔时间，以秒为单位

(4)nslookup: 允许主机向指定的 DNS 服务器查询某个 DNS 记录。如果没有指明 DNS 服务器，nslookup 将把查询请求发向默认的 DNS 服务器。nslookup 的一般格式是：

nslookup -option1 -option2 host-to-find dns-server

ipconfig 命令用来显示你当前的 TCP/IP 信息，包括：你的地址、DNS 服务器的地址、适配器的类型等信息。如果，要显示与主机相关的信息用命令：

ipconfig/all

如果查看 DNS 缓存中的记录用命令：

ipconfig/displaydns

要清空 DNS 缓存，用命令：

ipconfig /flushdns

例如：使用 nslookup 命令来查询 www.baidu.com 的 ip 地址，都返回了哪些信息，各部分的意义是什么？

nslookup www.baidu.com

(5) Netstat: 显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装了 TCP/IP 协议后才可以使⤵用。

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

参数

-a 显示所有连接和侦听端口。服务器连接通常不显示。

-e 显示以太网统计。该参数可以与 -s 选项结合使用。

-n 以数字格式显示地址和端口号（而不是尝试查找名称）。

-s 显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-p protocol 显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp。如果与 -s 选项一同使用显示每个协议的统计，protocol 可以是 tcp、udp、icmp 或 ip。

-r 显示路由表的内容。

Interval 重新显示所选的统计，在每次显示之间暂停 interval 秒。按 CTRL+B 停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

例如：

C:\>netstat -as

IP Statistics

Packets Received = 256325

...

ICMP Statistics

	Received	Sent
Messages	16	68

...

TCP Statistics

...

Segments Received = 41828

UDP Statistics

Datagrams Received = 82401

...

(6) **Ping**: 验证与远程计算机的连接。该命令只有在安装了 TCP/IP 协议后才可以使⤵用。

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list]
| [-k computer-list]] [-w timeout] destination-list

参数

-t Ping 指定的计算机直到中断。

-a 将地址解析为计算机名。

-n count 发送 count 指定的 ECHO 数据包数。默认值为 4。

-l length 发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节；最大值是 65,527。

-f 在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。

-i ttl 将“生存时间”字段设置为 ttl 指定的值。

-v tos 将“服务类型”字段设置为 tos 指定的值。

-r count 在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。

-s count 指定 count 指定的跃点数的时间戳。

-j computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

-k computer-list 利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

-w timeout 指定超时间隔，单位为毫秒。

destination-list 指定要 ping 的远程计算机。

较一般的用法是 ping -t www.zju.edu.cn

例如：

C:\>ping www.zju.edu.cn

Pinging zjuwww.zju.edu.cn [10.10.2.21] with 32 bytes of data:

Reply from 10.10.2.21: bytes=32 time=10ms TTL=253

Ping statistics for 10.10.2.21:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 10ms, Average = 2ms

(7) Route: 控制网络路由表。该命令只有在安装了 TCP/IP 协议后才可以使⤵用。

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

参数

-f 清除所有网关入口的路由表。如果该参数与某个命令组合使用，路由表将在运行命令前清除。

-p 该参数与 add 命令一起使用时，将使路由在系统引导程序之间持久存在。默认情况下，系统重新启动时不保留路由。与 print 命令一起使用时，显示已注册的持久路由列表。忽略其他所有总是影响相应持久路由的命令。

Command 指定下列的一个命令。

命令 目的

print 打印路由

add 添加路由

delete 删除路由

change 更改现存路由

destination 指定发送 command 的计算机。

mask subnetmask 指定与该路由条目关联的子网掩码。如果没有指定，将使用 255.255.255.255。

gateway 指定网关。

metric costmetric 指派整数跃点数（从 1 到 9999）在计算最快速、最可靠和（或）最便宜的路由时使用。

例如：本机 ip 为 10.111.142.71，缺省网关是 10.111.142.1，假设此网段上另有一网关 10.111.142.254，现在想添加一项路由，使得当访问 10.13.0.0 子网络时通过这一个网关，那么可以加入如下命令：

```
C:\>route add 10.13.0.0 mask 255.255.0.0 10.111.142.1
```

```
C:\>route print （键入此命令查看路由表，看是否已经添加了）
```

```
C:\>route delete 10.13.0.0
```

```
C:\>route print (此时可以看见已经没了添加的项)
```

(8) Tracert: 该诊断实用程序将包含不同生存时间 (TTL) 值的 Internet 控制消息协议 (ICMP) 回显数据包发送到目标, 以决定到达目标采用的路由。要在转发数据包上的 TTL 之前至少递减 1, 必需路径上的每个路由器, 所以 TTL 是有效的跃点计数。数据包上的 TTL 到达 0 时, 路由器应该将 “ICMP 已超时” 的消息发送回源系统。Tracert 先发送 TTL 为 1 的回显数据包, 并在随后的每次发送过程将 TTL 递增 1, 直到目标响应或 TTL 达到最大值, 从而确定路由。路由通过检查中级路由器发送回的 “ICMP 已超时” 的消息来确定路由。不过, 有些路由器悄悄地下传包含过期 TTL 值的数据包, 而 tracert 看不到。

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

参数

/d 指定不将地址解析为计算机名。

-h maximum_hops 指定搜索目标的最大跃点数。

-j computer-list 指定沿 computer-list 的稀疏源路由。

-w timeout 每次应答等待 timeout 指定的微秒数。

target_name 目标计算机的名称。

最简单的一种用法如下:

```
C:\>tracert www.cumt.edu.cn
```

```
Tracing route to www.cumt.edu.cn [202.119.200.12]
```

```
over a maximum of 30 hops:
```

```
 1  <10 ms  <10 ms  <10 ms  10.111.136.1
 2  <10 ms  <10 ms  <10 ms  10.0.0.10
 3  <10 ms  <10 ms  <10 ms  10.10.2.21
```

```
Trace complete.
```

4. 实验要求

- 查阅资料掌握常用网络命令的功能及应用
- 在联网的计算机中正确使用网络命令, 观察执行结果。
- 在实验报告 (有模板) 中记录实验中所要做的测试内容、使用的命令和执行结果, 截图并分析、回答问题。

5. 实验时间: 2 机时