

基本网络测试工具及应用工具 实验

1

冯巾松

fengjinsong@tongji.edu.cn

网络测试

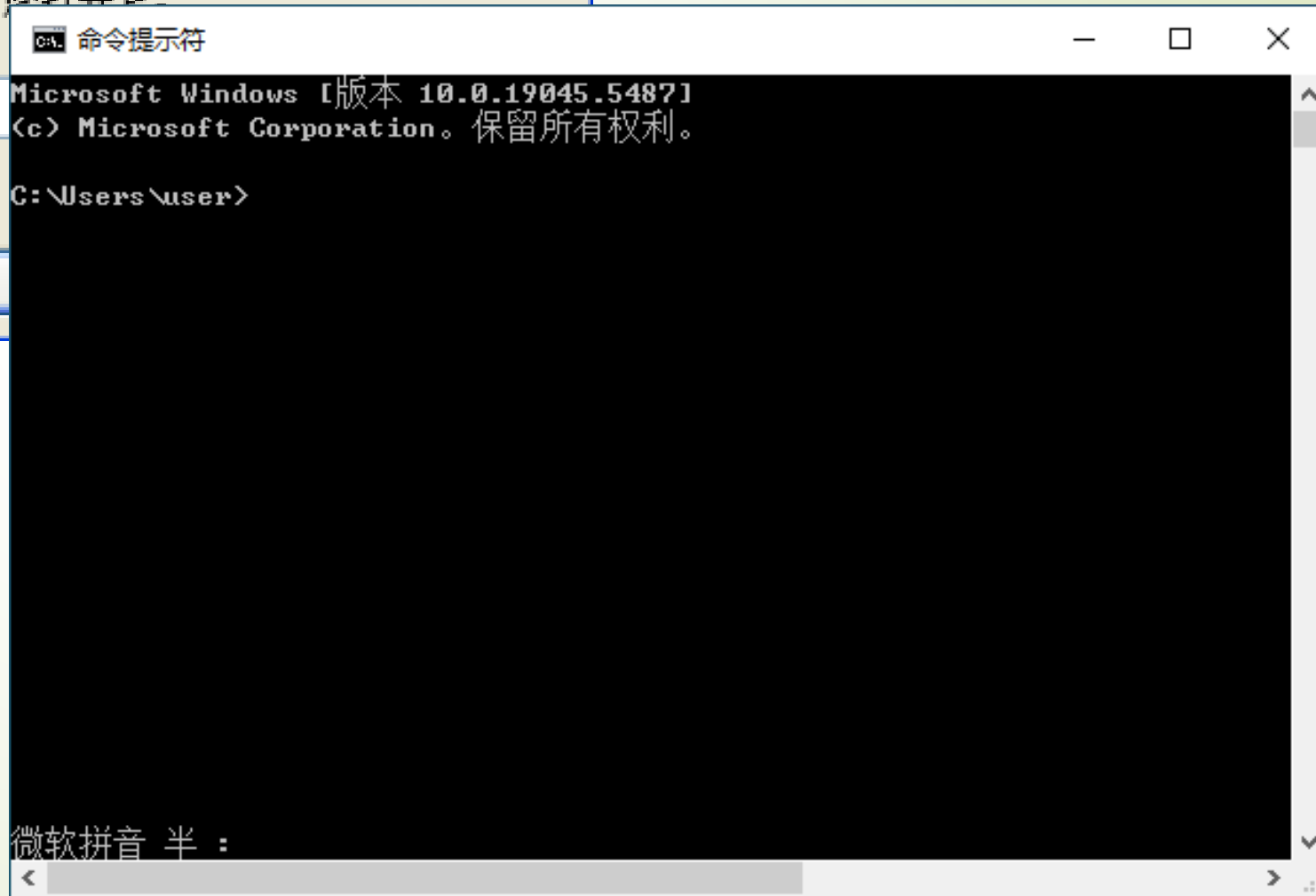
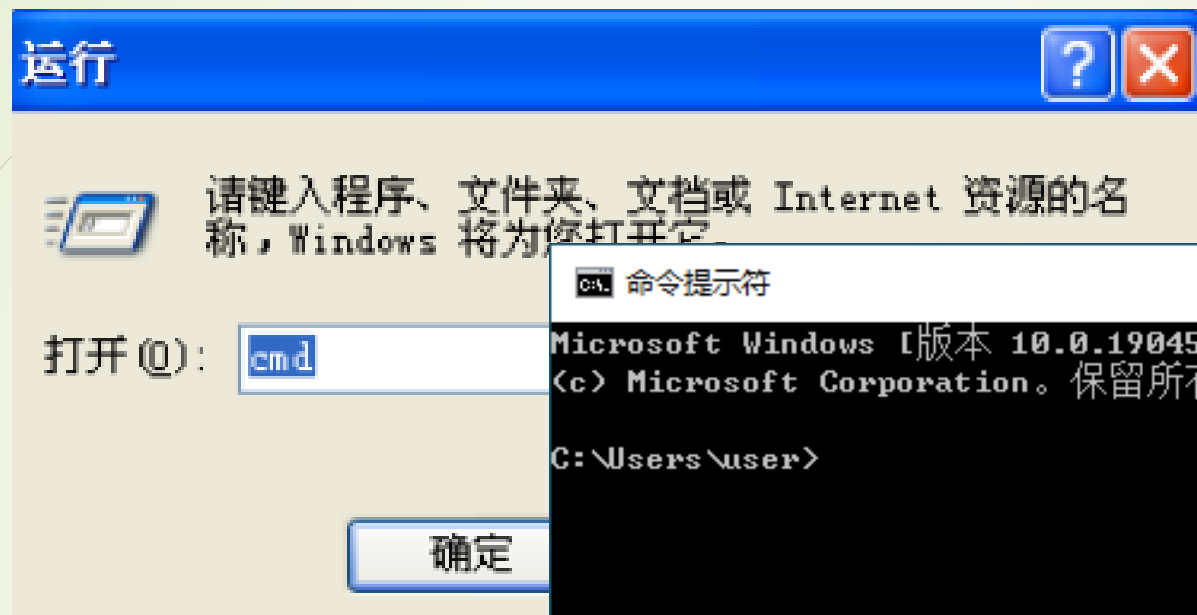
2

➡ 操作系统中也内置了一些非常有用的软件网络测试工具，如果能使用得当，并掌握一定的测试技巧是完全可以满足一般需求的，有的甚至被黑客作为黑客工具！其实有许多黑客工具软件也是基于这些内置的网络测试软件而编制、改写的。

➡ 这些工具虽然不能称之为专业测试工具，但可以简单判断网络的具体实际状况

运行方式

3



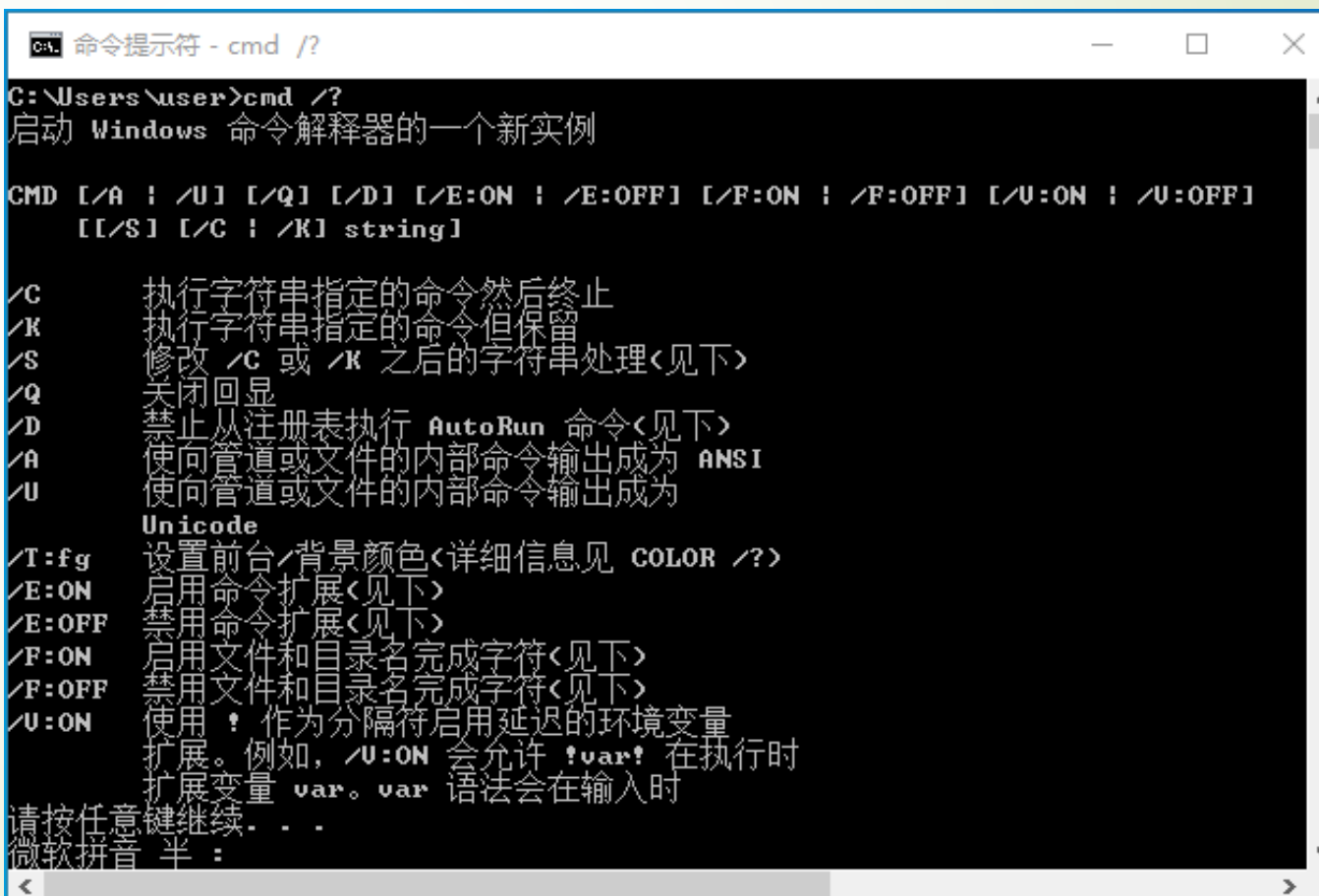
命令基本格式

➤ 命令 参数 回车

➤ Cmd [option]

例如：cmd /?

获得cmd命令的帮助信息



```
CA: 命令提示符 - cmd /?
C:\Users\user>cmd /?
启动 Windows 命令解释器的一个新实例

CMD [/A : /U] [/Q] [/D] [/E:ON : /E:OFF] [/F:ON : /F:OFF] [/U:ON : /U:OFF]
  [/S] [/C : /K] string]

/C      执行字符串指定的命令然后终止
/K      执行字符串指定的命令但保留
/S      修改 /C 或 /K 之后的字符串处理<见下>
/Q      关闭回显
/D      禁止从注册表执行 AutoRun 命令<见下>
/A      使向管道或文件的内部命令输出成为 ANSI
/U      使向管道或文件的内部命令输出成为
        Unicode
/T:fg   设置前台背景颜色<详细信息见 COLOR /?>
/E:ON   启用命令扩展<见下>
/E:OFF  禁用命令扩展<见下>
/F:ON   启用文件和目录名完成字符<见下>
/F:OFF  禁用文件和目录名完成字符<见下>
/U:ON   使用 ! 作为分隔符启用延迟的环境变量
        扩展。例如，/U:ON 会允许 !var! 在执行时
        扩展变量 var。var 语法会在输入时
        请按任意键继续...
        微软拼音 半：
```

Ping命令

- Ping是工作在TCP/IP网络体系结构中应用层的一个服务命令
- ping命令用于查看网络上的主机的连通性和通信质量
- 工作原理是向特定的目的主机发送ICMP ECHO_REQUEST包，接收方收到后回应ICMP ECHO REPLY进行测试而达到目的

Ping命令使用：测试网络通否

➡ 网络畅通的：

```
C:\Users\user>ping 10.60.41.1
```

```
正在 Ping 10.60.41.1 具有 32 字节的数据：
```

```
来自 10.60.41.1 的回复： 字节=32 时间=9ms TTL=58
```

```
来自 10.60.41.1 的回复： 字节=32 时间=9ms TTL=58
```

```
来自 10.60.41.1 的回复： 字节=32 时间=10ms TTL=58
```

```
来自 10.60.41.1 的回复： 字节=32 时间=8ms TTL=58
```

```
10.60.41.1 的 Ping 统计信息：
```

```
数据包： 已发送 = 4， 已接收 = 4， 丢失 = 0 (0% 丢失)，
```

```
往返行程的估计时间(以毫秒为单位)：
```

```
最短 = 8ms， 最长 = 10ms， 平均 = 9ms
```

```
C:\Users\user>
```

Ping命令使用：测试网络通否

➡ 网络不通

```
C:\Users\user>ping 10.60.41.1
```

```
正在 Ping 10.60.41.1 具有 32 字节的数据:
```

```
请求超时。
```

```
请求超时。
```

```
请求超时。
```

```
请求超时。
```

```
10.60.41.1 的 Ping 统计信息:
```

```
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

```
C:\Users\user>
```


Ping命令参数

- `ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j -Host list] | [-k Host-list]] [-w timeout] destination-list`
- `-t`——有这个参数时，当你ping一个主机时系统就不停的运行ping这个命令，直到按下Control-C。
- `-a`——解析主机的NETBIOS主机名，如果你想知道你所ping的计算机名则要加上这个参数，一般是在运用ping命令后的第一行就显示出来。

Ping命令参数 (2)

- `-n count`—定义用来测试所发出的测试包的个数，缺省值为4。通过该命令可自定义发送的个数，对衡量网络速度很有帮助，比如想测试发送20个数据包的返回的平均时间为多少，最快时间为多少，最慢时间为多少，就可以通过执行带有这个参数的命令获得
- `-l length`—定义所发送缓冲区的数据包的大小，在默认情况下windows的ping发送的数据包大小为32byte，也可自定义，但有个限制，即最大只能发送65500byte，超过这个数时，对方就很有可能因接收的数据包太大而死机，所以微软公司为了解决这一安全漏洞于是限制了ping的数据包大小。

Ping命令参数 (3)

- `-f`—在数据包中发送“不要分段”标志，一般你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。
- `-i ttl`—指定TTL值在对方的系统里停留的时间，此参数同样是帮助检查网络运转情况的。
- `-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。一般情况下你发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定你想探测经过的路由个数，不过限制在了9个，也就是说只能跟踪到9个路由。

Ping命令参数（4）

11

- -s count—指定“count”指定的跃点数的时间戳，此参数和-r差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录4个。
- -j host-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IP 允许的最大数量为 9。
- -k host-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 —是指要测试的主机名或IP地址

Ping命令获取计算机的IP地址

■ 利用ping这个工具可以获取对方计算机的IP地址，特别是在局域网中，经常是利用DHCP动态IP地址服务自动为各工作站分配动态IP地址，这时要知道所要测试的计算机的NETBIOS名，也即通常在“网络邻居”中看到的“计算机名”。使用ping命令时只要用ping命令加上目标计算机名即可，如果网络连接正常，则会显示所ping的这台机的动态IP地址。其实我们完全可以在互联网使用，以获取对方的动态IP地址，这一点对于黑客来说是比较有用的，当然首先的一点就是先要知道对方的计算机名

Ping -a hostname

- C:\Documents and Settings\Xiaby>ping -a SSELINUX
- Pinging SSELINUX [10.60.40.2] with 32 bytes of data:
- Reply from 10.60.40.2: bytes=32 time<1ms TTL=64
- Reply from 10.60.40.2: bytes=32 time<1ms TTL=64
- Reply from 10.60.40.2: bytes=32 time<1ms TTL=64
- Reply from 10.60.40.2: bytes=32 time<1ms TTL=64
- Ping statistics for 10.60.40.2:
- Packets: Sent = 4, Received = 4, Lost = 0 (0%)
- Approximate round trip times in milli-seconds:
- Minimum = 0ms, Maximum = 0ms, Average = 0ms

Ipconfig命令

- `ipconfig [/all] [/batch file] [/renew all] [/release all] [/renew n] [/release n]`
- `all`--显示与TCP/IP协议相关的所有细节信息，其中包括测试的主机名、IP地址、子网掩码、节点类型、是否启用IP路由、网卡的物理地址、默认网关等。
- `Batch file`—将测试的结果存入指定的“file”文件名中，以便于逐项查看，如果省略file文件名，则系统会把这测试的结果保存在系统的“winipcfg.out”文件中。
- `renew all`—更新全部适配器的通信配置情况，所有测试重新开始。
- `release all`—释放全部适配器的通信配置情况，
- `renew n`—更新第n号适配器的通信配置情况，所有测试重新开始。
- `release n`—释放第n号适配器的通信配置情况，

Ipconfig 示例

```
命令提示符
C:\Users\user>ipconfig /all

Windows IP 配置

主机名 . . . . . : DESKTOP-HUBMELT
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否

以太网适配器 以太网:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Intel(R) Ethernet Connection I219-U
物理地址. . . . . : C8-5B-76-9E-CB-DD
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是

未知适配器 本地连接:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Array Networks TAP-Windows Adapter
物理地址. . . . . : 00-FF-C6-B8-21-9D
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是

无线局域网适配器 本地连接* 2:

媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
物理地址. . . . . : F0-D5-BF-A7-24-8F
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
```


NBTSTAT

16

- NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]
- NBTSTAT命令:用于查看当前基于NETBIOS的TCP/IP连接状态, 通过该工具你可以获得远程或本地机器的组名和机器名。虽然用户使用ipconfig/winipcfg工具可以准确地得到主机的网卡地址, 但对于一个已建成的比较大型的局域网, 要去每台机器上进行这样的操作就显得过于费事了。网管人员通过在自己上网的机器上使用DOS命令nbtstat, 可以获取另一台上网主机的网卡地址

NBTSTAT参数

17

- -a Remotename—说明使用远程计算机的名称列出其名称表，此参数可以通过远程计算机的NetBios名来查看他的当前状态。
- -A IP address—说明使用远程计算机的IP地址并列出名称表，这个和-a不同的是就是这个只能使用IP，其实-a就包括了-A的功能了。
- -c—列出远程计算机的NetBIOS 名称的缓存和每个名称的IP地址 这个参数就是用来列出在你的NetBIOS里缓存的你连接过的计算机的IP。
- -n—列出本地机的 NetBIOS 名称

NBTSTAT例子

命令提示符

```
C:\Users\user>nbtstat -n
```

以太网:

节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

本地连接:

节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

WLAN:

节点 IP 地址: [192.168.1.7] 范围 ID: []

NetBIOS 本地名称表

名称	类型	状态
DESKTOP-HUBMELT<20>	唯一	已注册
DESKTOP-HUBMELT<00>	唯一	已注册
WORKGROUP <00>	组	已注册
WORKGROUP <1E>	组	已注册
WORKGROUP <1D>	唯一	已注册
.._MSBROWSE_.<01>	组	已注册

本地连接* 2:

节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

本地连接* 12:

节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

Tracert命令

- Tracert（跟踪路由）是路由跟踪实用程序，用于确定IP 数据报访问目标所采取的路径。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
- `tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name`
- `-d` 指定不将 IP 地址解析到主机名称。
- `-h maximum_hops` 指定跃点数以跟踪到称为 `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
- `target_name` 目标主机的名称或 IP 地址

Tracert例子

20

```
C:\Users\user>tracert www.baidu.com
```

通过最多 30 个跃点跟踪
到 www.a.shifen.com [180.101.51.73] 的路由:

1	2 ms	<1 毫秒	<1 毫秒	192.168.1.1
2	5 ms	4 ms	3 ms	100.64.200.1
3	*	*	*	请求超时。
4	*	*	*	请求超时。
5	*	*	*	请求超时。
6	*	10 ms	*	61.155.113.130
7	9 ms	8 ms	8 ms	58.213.95.206
8	20 ms	10 ms	10 ms	58.213.96.50
9	*	*	*	请求超时。
10	*	*	*	请求超时。
11	*	*	*	请求超时。
12	10 ms	8 ms	8 ms	180.101.51.73

节点路径隐藏

跟踪完成。

```
C:\Users\user>
```

Net命令

21

- Net命令是一个命令行工具，Net 命令有很多函数用于实用和核查计算机之间的NetBIOS连接，可以查看管理网络环境、服务、用户、登陆等信息内容；
- 要想获得Net 的HELP可以：在COMMAND下可以用字符方式：NET /?或NET HELP取得相应的方法的帮助。所有Net命令接受选项/yes和/no(可缩写为/y和/n)；

1, Net View

- ➡ 作用：显示域列表、计算机列表或指定计算机的共享资源列表。
- ➡ 命令格式：Net view [computername | /domain[:domainname]]
- ➡ 有关参数说明：
 - ✓ 不带参数的Net view显示当前域的计算机列表
 - ✓ computername 指定要查看其共享资源的计算机
 - ✓ domain[:domainname]指定要查看其可用计算机的域



```
C:\> 命令提示符

C:\Users\user>net view
服务器名称                注解

-----
\\DESKTOP-HUBMELT
\\TIAN-DELL                TIAN-DELL
命令成功完成。
```


2, Net User

- 作用：添加或更改用户帐号或显示用户帐号信息。
- 命令格式：Net user [username [password | *] [options]] [/domain]
- 有关参数说明：
 - ✓ 不带参数的Net user查看计算机上用户帐号列表
 - ✓ username添加、删除、更改或查看用户帐号名
 - ✓ password为用户帐号分配或更改密码

```
命令提示符
C:\Users\user>net user

\DESKTOP-HUBMELT 的用户帐户

-----
22465                Administrator      DefaultAccount
defaultuser0         Guest              user
WDAGUtilityAccount
命令成功完成。
```

3,Net Use

- 作用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。
- 命令格式：Net use [devicename | *] [computernamesharename[volume]] [password | *][[/user:[domainname]username][[/delete] | [/persistent:{yes | no}]]
- 有关参数说明：
 - ✓ devicename指定要连接到的资源名称或要断开的设备名称
 - ✓ computernamesharename服务器及共享资源的名称
 - ✓ password访问共享资源的密码
 - ✓ *提示键入密码
 - ✓ /user指定进行连接的另外一个用户

4,Net Time

- ➡ 作用：使计算机的时钟与另一台计算机或域的时间同步。
- ➡ 命令格式：Net time [computername | /domain[:name]] [/set]
- ➡ 有关参数说明：
 - ✓ computername 要检查或同步的服务器名
 - ✓ /domain[:name] 指定要与其时间同步的域
 - ✓ /set 使本计算机时钟与指定计算机或域的时钟同步

5, Net Start/Pause/Continue/Stop

- 命令格式: Net start service
- 作用: 启动服务, 或显示已启动服务的列表。

- 命令格式: Net pause service
- 作用: 暂停正在运行的服务。

- 命令格式: Net continue service
- 作用: 重新激活挂起的服务。

- 命令格式: Net stop service
- 作用: 停止 Windows 网络服务。

Net 其它命令 (1)

- 命令格式: `Net session [computername] [/delete]`
- 作用: 列出或断开本地计算机和与之连接的客户端的会话。
- 命令: `Net Send`
- 作用: 向网络的其他用户、计算机或通信名发送消息
- 命令格式: `Net print [computername] job# [/hold | /release | /delete]`
- 作用: 显示或控制打印作业及打印队列

Net 其它命令 (2)

- 命令格式: `Net name [name [/add | /delete]]`
- 作用: 添加或删除消息名 (有时也称别名), 或显示计算机接收消息的名称列表。
- 命令格式: `Net localgroup groupname {/add [/comment:"text "] | /delete} [/domain]`
- 作用: 添加、显示或更改本地组。
- 命令格式: `Net group groupname {/add [/comment:"text "] | /delete} [/domain]`
- 作用: 在 Windows 域中添加、显示或更改全局组。

Net 其它命令 (3)

- 命令格式: `Net file [id [/close]]`
- 作用: 显示某服务器上所有打开的共享文件名及锁定文件数。
- 命令格式: `Net config [service [options]]`
- 作用: 显示当前运行的可配置服务, 或显示并更改某项服务的设置。
- 命令格式: `Net computer computername {/add | /del}`
- 作用: 从域数据库中添加或删除计算机。

Net 其它命令 (4)

- 命令格式: Net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days | unlimited}] [/minpwage:days] [/uniquepw:number] [/domain]
- 作用: 更新用户帐号数据库、更改密码及所有帐号的登录要求。
- 当然Net命令具体在Windows 不同环境中使用, 可能会存在一些差异, 请大家参考有关的资料说明

Route命令

31

- 作用：在本地 IP 路由表中显示和修改条目。
- `route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]`
- `-f` 清除所有不是主路由（网掩码为 255.255.255.255 的路由）、环回网络路由（目标为 127.0.0.0，网掩码为 255.255.255.0 的路由）或多播路由（目标为 224.0.0.0，网掩码为 240.0.0.0 的路由）的条目的路由表。如果它与命令之一（例如 `add`、`change` 或 `delete`）结合使用，表会在运行命令之前清除。
- `-p` 与 `add` 命令共同使用时，指定路由被添加到注册表并在启动 TCP/IP 协议的时候初始化 IP 路由表。默认情况下，启动 TCP/IP 协议时不会保存添加的路由。与 `print` 命令一起使用时，则显示永久路由列表。所有其它的命令都忽略此参数

Route add命令 – 添加路由

➤ `route add 10.41.0.0 mask 255.255.0.0 10.27.0.1`

作用：添加目标IP地址为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

➤ `route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1`

作用：添加目标IP地址为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

➤ `route add 10.41.0.0 mask 255.255.0.0 10.27.0.1
metric 7`

作用：要添加目标为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

其他Route命令

- route change 更改现存路由
- route delete 删除路由
- route print 打印路由Destination

Nslookup命令

- Nslookup显示可用来诊断域名系统(DNS) 基础结构的 信息。只有在已安装TCP/IP 协议的情况下才可以使用该命令
- 命令格式：nslookup [-SubCommand ...]
[{ComputerToFind | [Server]]}
- ✓ -SubCommand ... 将一个或多个nslookup子命令指定为命令行选项。
- ✓ ComputerToFind 如果未指定其它服务器，就使用当前默认DNS 名称服务器查阅ComputerToFind 的信息。要查找不在当前 DNS 域的计算机，请在名称上附加句点。
- ✓ -Server 指定将该服务器作为DNS 名称服务器使用。如果省略了-Server，将使用默认的DNS 名称服务器。 {help | ?}

Nslookup命令示例

命令提示符 - nslookup

```
C:\Users\user>nslookup
默认服务器:  UnKnown
Address:  192.168.1.1
```

命令提示符

```
C:\Users\user>nslookup
默认服务器:  dnscache1.tongji.edu.cn
Address:  202.120.190.208
```

```
>
```

```
> bye
```

```
服务器:  dnscache1.tongji.edu.cn
Address:  202.120.190.208
```

```
非权威应答:
```

```
名称:  bye.tongji.edu.cn
Address:  202.120.164.112
```

```
> exit
```

```
C:\Users\user>
```


Netsh 命令

- 是一个windows系统本身提供的功能强大的网络配置命令行工具。
- 用法: netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName]UserName] [-p Password | *] [Command | -f ScriptFile]

Netsh interface ip show address 示例

37

```
命令提示符
C:\Users\user>netsh interface ip show address

接口 "以太网" 的配置
    DHCP 已启用: 是
    InterfaceMetric: 5

接口 "本地连接" 的配置
    DHCP 已启用: 是
    InterfaceMetric: 15

接口 "本地连接* 2" 的配置
    DHCP 已启用: 是
    InterfaceMetric: 25

接口 "本地连接* 12" 的配置
    DHCP 已启用: 否
    InterfaceMetric: 25

接口 "WLAN" 的配置
    DHCP 已启用: 是
    IP 地址: 192.168.1.7
    子网前缀: 192.168.1.0/24 <掩码 255.255.255.0>
    默认网关: 192.168.1.1
    网关跃点数: 0
    InterfaceMetric: 35

接口 "Loopback Pseudo-Interface 1" 的配置
    DHCP 已启用: 否
    IP 地址: 127.0.0.1
    子网前缀: 127.0.0.0/8 <掩码 255.0.0.0>
    InterfaceMetric: 75
```

Netsh interface dump

命令提示符

```
C:\Users\user>netsh interface dump
#=====
# 接口配置
#=====
pushd interface

popd
# 接口配置结束

# -----
# 6to4 配置
# -----
pushd interface 6to4

reset

popd
# 6to4 配置结束

# -----
# IPHTTPS 配置
# -----
pushd interface httpstunnel

reset

popd
# IPHTTPS 配置的结尾

#=====
# IPv4 配置
#=====
pushd interface ipv4
```

FTP命令

39

- 文件传输协议FTP（File Transfer Protocol）：是一个用于在计算机网络上在客户端和服务端之间进行文件传输的应用层协议。
- 命令行格式：ftp -v -d -i -n -g [主机名]，其中
 - ✓ -v 显示远程服务器的所有响应信息；
 - ✓ -n 限制ftp的自动登录
 - ✓ -d 使用调试方式；
 - ✓ -g 取消全局文件名
 - ✓ [主机名] 指定主机名称或要连到的远程主机

Telnet命令

- 远程登陆是指用户使用Telnet命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端等效于一个非智能的机器，它只负责把用户输入的每个字符传递给主机，再将主机输出的每个信息回显在屏幕上
- 命令格式：`telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]`

Telnet命令参数

- ➡ -a 企图自动登录。除了用当前已登陆的用户名以外， 与-l 选项相同。
- ➡ -e 跳过字符来进入telnet 客户提示。
- ➡ -f 客户端登录的文件名
- ➡ -l 指定远程系统上登录用的用户名称。 要求远程系统支持TELNET ENVIRON 选项。
- ➡ -t 指定终端类型。 支持的终端类型仅是：vt100, vt52, ansi 和vtnt。
- ➡ host 指定要连接的远程计算机的主机名或IP地址。
- ➡ port 指定端口号或服务名。

实验内容

- 在实验室网络（或宿舍网络）环境下验证以下命令的功能：

ping/ipconfig/nbtstat/tracert/
net/nslookup/netsh

- 熟悉部分命令中主要参数的使用