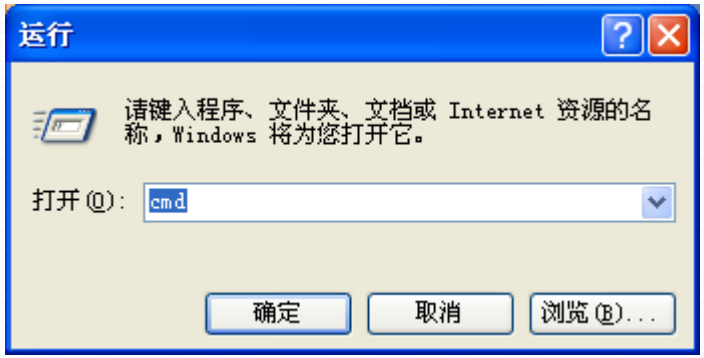
基本网络测试工具及应用工具实验

同济大学软件学院

网络测试

- 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一般来说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


运行
请键入程序、文件夹、文档或 Internet 资源的名称，Windows 将为您打开它。
打开(O):
cmd
确定
取消
浏览(B)...

命令基本方式

- 命令 参数 回车
- Cmd 【option】

一般 cmd /? 是该命令的帮助信息。如ipconfig /?

Ping 命令

- Ping命令是Windows9X/NT中集成的一个专用于TCP/IP协议的测试工具，ping命令是用于查看网络上的主机是否在工作，它是通过向该主机发送ICMP ECHO_REQUEST包进行测试而达到目的的。一般凡是应用TCP/IP协议的局域或广域网络，不管你是内部只有几台电脑的家庭、办公室局域网，还是校园网、企业网甚至Internet国际互联网络，当客户端与客户端之间无法正常进行访问或者网络工作出现各种不稳定的情况时，建议大家一定要先试试用Ping这个命令来测试一下网络的通信是否正常，多数时候是可以一次奏效的。

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，直到你按下Control-C。
- -a—解析主机的NETBIOS主机名，如果你想知道你所ping的要机计算机名则要加上这个参数了，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。通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，比如我想测试发送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知。
- -l length—定义所发送缓冲区的数据包的大小，在默认的情况下windows的ping发送的数据包大小为32byt，也可以自己定义，但有一个限制，就是最大只能发送65500byt，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，此参数同样是帮助你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的个数，不过限制在了9个，也就是说你只能跟踪到9个路由。

Ping命令参数（4）

- -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命令使用：测试网络通否

- C:\Documents and Settings\xiaby>ping 10.60.38.2
  Pinging 10.60.38.2 with 32 bytes of data:
- Reply from 10.60.38.2: bytes=32 time<1ms TTL=61
- Reply from 10.60.38.2: bytes=32 time<1ms TTL=61
- Reply from 10.60.38.2: bytes=32 time<1ms TTL=61
- Reply from 10.60.38.2: bytes=32 time<1ms TTL=61
- Ping statistics for 10.60.38.2:
- Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
- Approximate round trip times in milli-seconds:
- Minimum = 0ms, Maximum = 0ms, Average = 0ms
- 表示 网络是通畅的。

网络不通畅

- C:\Documents and Settings\xiaby>ping 40.60.38.2

- Pinging 40.60.38.2 with 32 bytes of data:

- Request timed out.
- Request timed out.
- Request timed out.
- Request timed out.

- Ping statistics for 40.60.38.2:
- Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Ping命令获取计算机的IP地址

- 利用ping这个工具我们可以获取对方计算机的IP地址，特别是在局域网中，我们经常是利用DHCP动态IP地址服务自动为各工作站分配动态IP地址，这时当然我们要知道所要测试的计算机的NETBIOS名，也即我们通常在“网络邻居”中看到的“计算机名”。使用ping命令时我们只要用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你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% l
- Approximate round trip times in milli-seconds:
- Minimum = oms, Maximum = oms, Average = oms

Ipconfig 的使用

- 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 例子（1）

- C:\Documents and Settings\xiaby>ipconfig /all
- Windows IP Configuration
- Host Name . . . . . : PC201010281 5grv
- Primary Dns Suffix . . . . . :
- Node Type . . . . . : Unknown
- IP Routing Enabled. . . . . : Yes
- WINS Proxy Enabled. . . . . : No
- Ethernet adapter 本地连接:

Ipconfig 例子（2）

- Connection-specific DNS Suffix . :
- Description . . . . . : Marvell Yukon 88E8039 PCI-E Fast Ethernet Controller
- Physical Address. . . . . : 00-16-D3-FA-59-25
- Dhcp Enabled. . . . . : Yes
- Autoconfiguration Enabled . . . . : Yes
- Autoconfiguration IP Address. . . : 10.60.40.208
- Subnet Mask . . . . . : 255.255.255.0
- Default Gateway . . . . . : 10.60.40.254
- DNS Servers . . . . . : 202.120.190.108
- 10.10.173.100

Nbtstat

- 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

- -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

- C:\Documents and Settings\xiaby>nbtstat –n
- 无线网络连接:
- Node IpAddress: [0.0.0.0] Scope Id: []
- No names in cache
- 本地连接:
- Node IpAddress: [10.60.40.208] Scope Id: []
- NetBIOS Local Name Table
- Name Type Status
- ---
- PC20101028l5GRV<00> UNIQUE Registered
- PC20101028l5GRV<20> UNIQUE Registered
- WORKGROUP <00> GROUP Registered
- WORKGROUP <1E> GROUP Registered

Tracert

- tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
  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
- **-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

- C:\Documents and Settings\xiaby>Tracert 10.60.38.2
- Tracing route to 10.60.38.2 over a maximum of 30 hops
- 1 * * * Request timed out.
- 2 1 ms 1 ms 1 ms 172.20.61.94
- 3 * * * Request timed out.
- 4 <1 ms <1 ms <1 ms 10.60.38.2
- Trace complete.

Net命令

- Net命令是一个命令行命令，Net 命令有很多函数用于实用和核查计算机之间的NetBIOS连接，可以查看我们的管理网络环境、服务、用户、登陆等信息内容；要想获得Net 的HELP可以：
- (1)在Windows下可以用图形的方式，开始->帮助->索引->输入NET；
- (2)在COMMAND下可以用字符方式：NET /?或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：
- ·键入不带参数的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

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：
- ·键入不带参数的Net user查看计算机上的用户帐号列表
- ·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
- ·提示输入密码

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}]]
- Net use列出网络连接
- ·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

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

- 作 用：暂停正在运行的服务。
- 命令格式：Net pause service
-
- 作 用：重新激活挂起的服务。
- 命令格式：Net continue service
-
- 作 用：停止 Windows 网络服务。
- 命令格式：Net stop service
-

Net其它（1）

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

Net其它（2）

- **Net Name**
- 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 name [name [/add | /delete]]
- **Net Localgroup**
- 作 用：添加、显示或更改本地组。
- 命令格式：Net localgroup groupname {/add [/comment:"text "] | /delete} [/domain]
- **Net Group**
- 作 用：在 Windows域中添加、显示或更改全局组。
- 命令格式：Net group groupname {/add [/comment:"text "] | /delete} [/domain]

Net 其它（3）

- **Net File**
- 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 file [id [/close]]
- **Net Config**
- 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 config [service [options]]
- **Net Computer**
- 作 用：从域数据库中添加或删除计算机。
- 命令格式：Net computer computername {/add | /del}

其它（4）

- 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。
- 命令格式：Net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days | unlimited}] [/minpwage:days] [/uniquepw:number] [/domain]
-
- **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

- 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 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命令

- Command
- 指定要运行的命令。下表列出了有效的命令。
- 命令 目的
- add 添加路由
- change 更改现存路由
- delete 删除路由
- print 打印路由Destination
- 指定路由的网络目标地址。目标地址可以是一个 IP 网络地址（其中网络地址的主机地址位设置为 0），对于主机路由是 IP 地址，对于默认路由是 0.0.0.0

实例

- 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 的路由，请键入：
  route add 10.41.0.0 mask 255.255.0.0 10.27.0.1
- 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 的永久路由，请键入：
  route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1
- 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，请键入： route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metric 7
- Route print？

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 Nslookup 命令行工具。
  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|?}

实例

- C:\Documents and Settings\xiaby>nslookup
- Default Server: dns183.tongji.edu.cn
- Address: 202.120.190.108

- > ?

Netsh 命令行

- netsh [-a AliasFile] [-c Context] [-r RemoteMachine] [Command | -f ScriptFile]

  ? - 显示命令列表。
  aaaa - 更改到 `aaaa' 上下文。
  add - 将一个配置项添加到项目列表中。
  delete - 在项目列表上删除一个配置项目。
  dhcp - 更改到 `dhcp' 上下文。
  dump o - 显示一个配置脚本。
  exec - 运行一个脚本文件。
  help - 显示命令列表。
  interface - 更改到 `interface' 上下文。
  ras - 更改到 `ras' 上下文。
  routing - 更改到 `routing' 上下文。
  set - 更新配置设置。
  show - 显示信息
  wins - 更改到 `wins' 上下文。

Ftp命令

- FTP命令是Internet用户使用最频繁的命令之一，不论是在DOS还是UNIX操作系统下使用FTP，都会遇到大量的FTP内部命令。熟悉并灵活应用FTP的内部命令，可以大大方便使用者，并收到事半功倍之效。
  FTP的命令行格式为：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，即不使用；
  .n etrc文件；
  -d使用调试方式；
  -g取消全局文件名。

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。
- 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。

Telnet BBS.tsinghua.edu.cn

- 欢迎使用 Microsoft Telnet Client
- Escape 字符是 'CTRL+]'
- Microsoft Telnet> ?
- 命令可以缩写。支持的命令为:
- c - close 关闭当前连接
- d - display 显示操作参数
- o - open hostname [port] 连接到主机名称(默认端口 23).
- q - quit 退出 telnet
- set - set 设置选项 (要列表，请键入 'set ?')
- sen - send 将字符串发送到服务器

Telnet BBS.tsinghua.edu.cn

- st - status 打印状态信息
- u - unset 解除设置选项 (要列表，请键入 'unset ?')
- ?/h - help 打印帮助信息
- Microsoft Telnet> open
- (到) bbs.tsinghua.edu.cn
- 正在连接到bbs.tsinghua.edu.cn...
- .....