常用 Windows 网络命令

命令的使用：在 Windows 环境下的命令提示符窗口中直接输入各命令。

1、 Ping 命令

Ping 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，可以推断 TCP/IP 参数是否设置得正确以及运行是否正常。

按照缺省设置，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 存在时间）值，我们可以通过 TTL 值推算一下数据包已经通过了多少个路由器：源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）-返回时 TTL 值。例如，返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段（128-119）；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 9 个路由器网段。

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：

• ping 127.0.0.1

这个 Ping 命令被送到本地计算机的 IP 软件，该命令永不退出该计算机。如果没有做到这一点，就表示 TCP/IP 的安装或运行存在某些最基本的问题。

• 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 命令作出应答，如果没有，则表示本地配置或安装存在问题。出现此问题时，局域网用户请断开网络电缆，然后重新发送该命令。如果网线断开后本命令正确，则表示另一台计算机可能配置了相同的 IP 地址。

• 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，那么表示子网掩码（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。

• 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作出应答。

• ping 远程 IP

如果收到 4 个应答，表示成功的使用了缺省网关。对于拨号上网用户则表示能够成功的访问 Internet（但不排除 ISP 的 DNS 会有问题）。

• ping localhost

localhost 是一个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。如果没有做到点，则表示主机文件（/Windows/host）中存在问题。

• ping www.xxx.com（如 www.yesky.com 天极网）

对这个域名执行 Ping www.xxx.com 地址，通常是通过 DNS 服务器 ，如果这里出现故障，则表示 DNS 服务器的 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）。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，这些命令的成功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。

Ping 命令的常用参数选项

• ping IP －t

连续对 IP 地址执行 Ping 命令，直到被用户以 Ctrl+C 中断。

• ping IP -l 3000

指定 Ping 命令中的数据长度为 3000 字节，而不是缺省的 32 字

节。

• ping IP －n

执行特定次数的 Ping 命令。

2、Netstat 命令

Netstat 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。

netstat 的一些常用选项

• netstat －s

本选项能够按照各个协议分别显示其统计数据。如果我们的应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 Web 页之类的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

• netstat －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）。

• netstat －r

本选项可以显示关于路由表的信息，类似于后面所讲使用 route print 命令时看到的 信息。除了显示有效路由外，还显示当前有效的连接。

• netstat －a

本选项显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的那些连接。

• netstat －n

显示所有已建立的有效连接。

3、IPConfig 命令

IPConfig 可用于显示当前的 TCP/IP 配置的设置值。（对于 Windows 95 和 Windows 98 的客户机，请使用 winipcfg 命令而不是 ipconfig 命令）这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。但是，如果我们的计算机和所在的局域网使用了动态主机配置协议（DHCP），这个程序所显示的信息也许更加实用。这时，IPConfig 可以让我们了解自己的计算机是否成功的租用到一个 IP 地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的 IP 地址、子网掩码和缺省网关实际上是进行测试和故障分 析的必要项目。

IPConfig 最常用的选项

• ipconfig

当使用 IPConfig 时不带任何参数选项，那么它为每个已经配置了的接口显示 IP 地址、子网掩码和缺省网关值。

• ipconfig /all

当使用 all 选项时，IPConfig 能为 DNS 和 WINS 服务器显示它已配置且所要使用的附加信息（如 IP 地址等），并且显示内置于本地网

卡中的物理地址（MAC）。如果 IP 地址是从 DHCP 服务器租用的，IPConfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。

• ipconfig /release 和 ipconfig /renew

这是两个附加选项，只能在向 DHCP 服务器租用其 IP 地址的计算机上起作用。如果我们输入 ipconfig /release，那么所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。如果我们输入 ipconfig /renew，那么本地计算机便设法与 DHCP 服务器取得联系，并租用一个 IP 地址。请注意，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。

下面的范例是 ipconfig /all 命令输出，该计算机配置成使用 DHCP 服务器动态配置 TCP/IP，并使用 WINS 和 DNS 服务器解析名称。

Windows 2000 IP Configuration

Node Type.. . . . . : Hybrid

IP Routing Enabled.. . . . : No

WINS Proxy Enabled.. . . . : No

Ethernet adapter Local Area Connection:

Host Name.. . . . . : corp1.microsoft.com

DNS Servers . . . . . : 10.1.0.200

Description. . . . . : 3Com 3C90x Ethernet Adapter

Physical Address. . . . . : 00-60-08-3E-46-07

DHCP Enabled.. . . . . : Yes

Autoconfiguration Enabled.: Yes

IP Address. . . . . : 192.168.0.112

Subnet Mask. . . . . : 255.255.0.0

Default Gateway. . . . . : 192.168.0.1

DHCP Server. . . . . : 10.1.0.50

Primary WINS Server. . . . : 10.1.0.101

Secondary WINS Server. . . : 10.1.0.102

Lease Obtained.. . . . . : Wednesday, September 02, 1998 10:32:13 AM

Lease Expires.. . . . . : Friday, September 18, 1998 10:32:13 AM

4、ARP 命令

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，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缺省网关和本地服务器等常用主机进行这项工作，有助于减少网络上的信息量。

按照缺省设置，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 至 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时，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）。

ARP 常用命令选项：

• arp -a 或 arp －g

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，-g 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。

• arp -a IP

如果我们有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。

• arp -s IP 物理地址

我们可以向 ARP 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态，或者在出现错误时，人工配置的物理地址将自动更新该项目。

• arp -d IP

使用本命令能够人工删除一个静态项目。

例如我们在命令提示符下，键入 Arp －a；如果我们使用过 Ping 命令测试并验证从这台计算机到 IP 地址为 10.0.0.99 的主机的连通

性，则 ARP 缓存显示以下项：

Interface:10.0.0.1 on interface 0x1

Internet Address	Physical Address	Type
10.0.0.99	00-e0-98-00-7c-dc	dynamic

在此例中，缓存项指出位于 10.0.0.99 的远程主机解析成 00-e0-98-00-7c-dc 的媒体访问控制地址，它是在远程计算机的网卡硬件中分配的。媒体访问控制地址是计算机用于与网络上远程 TCP/IP 主机物理通讯的地址。

至此我们可以用 ipconfig 和 ping 命令来查看自己的网络配置并判断是否正确、可以用 netstat 查看别人与我们所建立的连接并找出 ICQ 使用者所隐藏的 IP 信息、可以用 arp 查看网卡的 MAC 地址。

5、Tracert 命令

如果有网络连通性问题，可以使用 tracert 命令来检查到达的目标 IP 地址的路径并记录结果。tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器，以及每个跃点所需的时间。如果数据包不能传递到目标，tracert 命令将显示成功转发数据包的最后一个路由器。当数据报从我们的计算机经过多个网关传送到目的地时，Tracert 命令可以用来跟踪数据报使用的路由（路径）。该实用程序跟踪的路径是源计算机到目的地的一条路径，不能保证或认为数据报总遵循这个路径。如果我们的配置使用 DNS，那么我们常常会从所产生的应答中得到城市、地址和常见通信公司的名字。Tracert 是一个运行得比较慢的命令（如果我们指定的目标地址比较远），每个路

由器我们大约需要给它 15 秒钟。

Tracert 的使用很简单，只需要在 tracert 后面跟一个 IP 地址或 URL，Tracert 会进行相应的域名转换的。

tracert 最常见的用法：

tracert IP address [-d] 该命令返回到达 IP 地址所经过的路由器列表。通过使用 -d 选项，将更快地显示路由器路径，因为 tracert 不会尝试解析路径中路由器的名称。

Tracert 一般用来检测故障的位置，我们可以用 tracert IP 在哪个环节上出了问题，虽然还是没有确定是什么问题，但它已经告诉了我们问题所在的地方，我们也就可以很有把握的告诉别人----某某地方出了问题。

6、Route 命令

大多数主机一般都是驻留在只连接一台路由器的网段上。由于只有一台路由器，因此不存在使用哪一台路由器将数据报发表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缺省网关来输入。

但是，当网络上拥有两个或多个路由器时，我们就不一定想只依赖缺省网关了。实际上我们可能想让我们的某些远程 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，我们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 就是用来显示、人工添加和修改路由表项目的。

一般使用选项：

• route print

本命令用于显示路由表中的当前项目，在单路由器网段上的输出；由于用 IP 地址配置了网卡，因此所有的这些项目都是自动添加的。

• route add

使用本命令，可以将信路由项目添加给路由表。例如，如果要设定一个到目的网络 209.98.32.33 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，器 IP 为 202.96.123.5，子网掩码为 255.255.255.224，那么我们应该输入以下命令：

route add 209.98.32.33 mask 255.255.255.224 202.96.123.5 metric 5

• route change

我们可以使用本命令来修改数据的传输路由，不过，我们不能使用本命令来改变数据的目的地。下面这个例子可以将数据的路由改到另一个路由器，它采用一条包含 3 个网段的更直的路径：

route add 209.98.32.33 mask 255.255.255.224 202.96.123.250 metric 3

• route delete

使用本命令可以从路由表中删除路由。例如：route delete

209.98.32.33

7、pathping 命令

pathping 命令是一个路由跟踪工具，它将 ping 和 tracert 命令的功能和这两个工具所不提供的其他信息结合起来。pathping 命令在一段时间内将数据包发送到到达最终目标的路径上的每个路由器，然后基于数据包的计算机结果从每个跃点返回。由于命令显示数据包在任何给定路由器或链接上丢失的程度，因此可以很容易地确定可能导致网络问题的路由器或链接。某些选项是可用的，如下表所示。

选项 名称 功能

-n Hostnames 不将地址解析成主机名。

-h Maximum hops 搜索目标的最大跃点数。

-g Host-list 沿着路由列表释放源路由。

-p Period 在 ping 之间等待的毫秒数。

-q Num_queries 每个跃点的查询数。

-w Time-out 为每次回复所等待的毫秒数。

-T Layer 2 tag 将第 2 层优先级标记（例如，对于 IEEE 802.1p）连接到数据包并将它发送到路径中的每个网络设备。这有助于标识没有正确配置第 2 层优先级的网络设备。-T 开关用于测试服务质量 (QoS) 连通性。

-R RSVP isbase Che 检查以确定路径中的每个路由器是否支持“资源保留协议 (RSVP)”，此协议允许主机为数据流保留一定量的带宽。 -R 开关用于测试服务质量 (QoS) 连通性。

默认的跃点数是 30，并且超时前的默认等待时间是 3 秒。默认时间是 250 毫秒，并且沿着路径对每个路由器进行查询的次数是 100。

以下是典型的 pathping 报告。跃点列表后所编辑的统计信息表明在每个独立路由器上数据包丢失的情况。

D:\>pathping -n msw

Tracing route to msw [7.54.1.196]

over a maximum of 30 hops:

0 172.16.87.35

1 172.16.87.218

2 192.68.52.1

3 192.68.80.1

4 7.54.247.14

5 7.54.1.196

Computing statistics for 125 seconds...

Source to Here This Node/Link

Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address

0 172.16.87.35

0/ 100 = 0% |

1 41ms 0/ 100 = 0% 0/ 100 = 0% 172.16.87.21813/ 100 = 13% |

2 22ms 16/ 100 = 16% 3/ 100 = 3% 192.68.52.10/ 100 = 0% |

3 24ms 13/ 100 = 13% 0/ 100 = 0% 192.68.80.1 0/ 100 = 0% |

4 21ms 14/ 100 = 14% 1/ 100 = 1% 10.54.247.14 0/ 100 = 0% |

5 24ms 13/ 100 = 13% 0/ 100 = 0% 10.54.1.196

Trace complete.

当运行 pathping 时，在测试问题时首先查看路由的结果。此路径与 tracert 命令所显示的路径相同。然后 pathping 命令对下一个 125 毫秒显示忙消息（此时间根据跃点计数变化）。在此期间，pathping 从以前列出的所有路由器和它们之间的链接之间收集信息。在此期间结束时，它显示测试结果。

最右边的两栏 This Node/Link Lost/Sent=Pct 和 Address 包含的信息最有用。172.16.87.218（跃点 1）和 192.68.52.1（跃点 2）丢失 13% 的数据包。 所有其他链接工作正常。在跃点 2 和 4 中的路由器也丢失寻址到它们的数据包（如 This Node /Link 栏中所示），但是该丢失不会影响转发的路径。

对链接显示的丢失率（在最右边的栏中标记为 |）表明沿路径转发丢失的数据包。该丢失表明链接阻塞。对路由器显示的丢失率（通过最右边栏中的 IP 地址显示）表明这些路由器的 CPU 可能超负荷运行。这些阻塞的路由器可能也是端对端问题的一个因素，尤其是在软件路由器转发数据包时。