<https://blog.csdn.net/tjvictor/article/details/1328409>

Ping命令详解

对于Windows下ping命令相信大家已经再熟悉不过了，但是能把ping的功能发挥到最大的人却并不是很多，当然我也并不是说我可以让ping发挥最大的功能，我也只不过经常用ping这个工具，也总结了一些小经验，现在和大家分享一下。  
  
现在我就参照ping命令的帮助说明来给大家说说我使用ping时会用到的技巧，ping只有在安装了TCP/IP协议以后才可以使用：  
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  
Options:  
-t Ping the specified host until stopped.To see statistics and continue - type Control-Break;To stop - type Control-C.  
不停的ping地方主机，直到你按下Control-C。  
此功能没有什么特别的技巧，不过可以配合其它参数使用，将在下面提到。  
  
  
-a Resolve addresses to hostnames.  
解析计算机NetBios名。  
示例：C:＼>ping -a 192.168.1.21  
Pinging iceblood.yofor.com [192.168.1.21] with 32 bytes of data:  
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254  
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254  
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254  
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254  
Ping statistics for 192.168.1.21:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms  
从上面就可以知道IP为192.168.1.21的计算机NetBios名为iceblood.yofor.com。  
  
-n count Number of echo requests to send.  
发送count指定的Echo数据包数。  
在默认情况下，一般都只发送四个数据包，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50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以下获知：  
C:＼>ping -n 50 202.103.96.68  
Pinging 202.103.96.68 with 32 bytes of data:  
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241  
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241  
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241  
Request timed out.  
………………  
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241  
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241  
Ping statistics for 202.103.96.68:  
Packets: Sent = 50, Received = 48, Lost = 2 (4% loss),Approximate round trip times in milli-seconds:  
Minimum = 40ms, Maximum = 51ms, Average = 46ms  
从以上我就可以知道在给202.103.96.68发送50个数据包的过程当中，返回了48个，其中有两个由于未知原因丢失，这48个数据包当中返回速度最快为40ms，最慢为51ms，平均速度为46ms。  
  
  
-l size Send buffer size.  
定义echo数据包大小。  
在默认的情况下windows的ping发送的数据包大小为32byt，我们也可以自己定义它的大小，但有一个大小的限制，就是最大只能发送 65500byt，也许有人会问为什么要限制到65500byt，因为Windows系列的系统都有一个安全漏洞（也许还包括其它系统）就是当向对方一次发送的数据包大于或等于65532时，对方就很有可能挡机，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。虽然微软公司已经做了此限制，但这个参数配合其它参数以后危害依然非常强大，比如我们就可以通过配合-t参数来实现一个带有攻击性的命令：（以下介绍带有危险性，仅用于试验，请勿轻易施于别人机器上，否则后果自负）  
C:＼>ping -l 65500 -t 192.168.1.21  
Pinging 192.168.1.21 with 65500 bytes of data:  
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254  
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254  
………………  
这样它就会不停的向192.168.1.21计算机发送大小为65500byt的数据包，如果你只有一台计算机也许没有什么效果，但如果有很多计算机那么就可以使对方完全瘫痪，我曾经就做过这样的试验，当我同时使用10台以上计算机ping一台Win2000Pro系统的计算机时，不到5分钟对方的网络就已经完全瘫痪，网络严重堵塞，HTTP和FTP服务完全停止，由此可见威力非同小可。  
  
  
-f Set Don't Fragment flag in packet.  
在数据包中发送“不要分段”标志。  
在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 Time To Live.  
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 Type Of Service.  
将“服务类型”字段设置为 tos 指定的值。  
  
-r count Record route for count hops.  
在“记录路由”字段中记录传出和返回数据包的路由。  
在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，如果想探测更多，可以通过其它命令实现，我将在以后的文章中给大家讲解。以下为示例：  
C:＼>ping -n 1 -r 9 202.96.105.101 （发送一个数据包，最多记录9个路由）  
  
Pinging 202.96.105.101 with 32 bytes of data:  
  
Reply from 202.96.105.101: bytes=32 time=10ms TTL=249  
Route: 202.107.208.187 ->  
202.107.210.214 ->  
61.153.112.70 ->  
61.153.112.89 ->  
202.96.105.149 ->  
202.96.105.97 ->  
202.96.105.101 ->  
202.96.105.150 ->  
61.153.112.90  
  
Ping statistics for 202.96.105.101:  
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 10ms, Maximum = 10ms, Average = 10ms  
从上面我就可以知道从我的计算机到202.96.105.101一共通过了202.107.208.187 ，202.107.210.214 , 61.153.112.70 , 61.153.112.89 , 202.96.105.149 , 202.96.105.97这几个路由。  
  
  
-s count Timestamp for count hops.  
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 Loose source route along 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（路由稀疏源）IP 允许的最大数量为 9。  
  
  
-k host-list Strict source route along 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（路由严格源）IP 允许的最大数量为 9。  
  
  
-w timeout Timeout in milliseconds to wait for each reply.  
指定超时间隔，单位为毫秒。  
此参数没有什么其它技巧。  
  
ping命令的其它技巧：在一般情况下还可以通过ping对方让对方返回给你的TTL值大小，粗略的判断目标主机的系统类型是Windows系列还是 UNIX/Linux系列，一般情况下Windows系列的系统返回的TTL值在100-130之间，而UNIX/Linux系列的系统返回的TTL值在 240-255之间，当然TTL的值在对方的主机里是可以修改的，Windows系列的系统可以通过修改注册表以下键值实现：  
[HKEY\_LOCAL\_MACHINE＼SYSTEM＼CurrentControlSet＼Services＼Tcpip＼Parameters]  
"DefaultTTL"=dword:000000ff  
255---FF  
　 128---80  
　 64----40  
　 32----20