Detailed Description and Small Skills of Ping Command in Windows

冷志宇 2007-09-26 发表

Detailed Description and Small Skills of Ping Command in Windows

We are all familiar with the **ping** command in Windows, but not all of us can maximize its function. I would like to share with you my experience in using the command.

Against the help description of the **ping** command, I will introduce my skills in using the command. It can be used only after TCP/IP is installed.

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.

Continuously ping the local host, until you press **Ctrl+C**.

This function has no special skills, but can be used in coordination with other parameters (mentioned later).

-a Resolve addresses to hostnames.

Resolve the NetBios name of PC.

Example: 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

The above shows that the NetBios name of the PC with its IP being 192.168.1.21 is **iceblood.yofor.com**.

-n count Number of echo requests to send.

Send the number of echo packets specified by **count**.

1 Four packets are sent by default. You can use this command to customize the sending count, which is helpful for measuring the network speed. For example, perform the following operation to test the average/maximum/minimum time when 50 packets are returned:

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

The above shows that 48 packets are returned among 50 packets sent to 202.103.96.68, and two packets are lost due to unknown reasons. For the return of 48 packets, the minimum time is 40ms, the maximum time is 51ms, and the average time is 46ms.

-l size Send buffer size.

Define the size of echo packet.

The size of ping packets in Windows is 32 bytes by default. You can customize the size and limit it to 65500 bytes. Such limit is set because of a security hole of Windows system (including other systems maybe). That is, when 65532 bytes or more ar

e sent to the remote end for once, the remote end probably becomes down. Therefor e, Microsoft limits the size of ping packets. However, this parameter is still harmful in coordination with other parameters. For example, the following is an attacking comm and by coordinating **-l** with **-t** (for experiment only and never execute it at will).

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

??????

In this case, your PC will continuously send packets of 65500 bytes to 192.168.1.21. Sending such packets from several PCs at the same time can make th e remote end crash. I have made such an experiment. When I use more than 10 PCs to ping a Win2000Pro PC, its network is completely down in five minutes and HTTP/FTP services are all stopped.

-f Set Don't Fragment flag in packet.

Send the **Don ¢ t Fragment** flag in packets.

The packets are generally fragmented before sending to the remote end. This p arameter disables the route fragmentation.

-i TTL Time To Live.

Specify **TTL** to the time when packets stay at the remote system.

This parameter also helps you check the network operation.

-v TOS Type Of Service.

Set **Type Of Service** to the value specified by **tos**.

-r count Record route for count hops.

Record the route of transmitted and returned packets in **Record route**.

In general cases, the packets you send reach the destination through some rout es. This parameter helps you trace up to nine routes. For more routes, you can use other commands. I will mention it in future articles. See the following example:

C:\>ping -n 1 -r 9 202.96.105.101(Send one packet, and up to nine routes are re corded)

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:

1 Minimum = 10ms, Maximum = 10ms, Average = 10ms

The above shows that the routes from my PC to 202.96.105.101 include: 202.10 7.208.187, 202.107.210.214, 61.153.112.70, 61.153.112.89, 202.96.105.149 and 20 2.96.105.97.

-s count Timestamp for count hops.

Set the time stamp of hop count specified by **count**.

This parameter is similar to **–r**, but does not record the returning routes of packet s or records four routes at most.

-j host-list Loose source route along host-list.

Specify the computer list route packet by **computer-list**. Up to nine consecutive PCs can be allowed by the intermediate gateway isolation (loose source route) IP.

-k host-list Strict source route along host-list.

Specify the computer list route packet by **computer-list**. Up to nine consecutive

PCs cannot be allowed by the intermediate gateway isolation (strict source route) IP.

-w timeout Timeout in milliseconds to wait for each reply.

Specify the timeout, in milliseconds.

This parameter has no skills.

Other skills for the **ping** command: You can judge the destination host system to Windows or UNIX/Linux through the returned TTL value in the ping operation. Generally, the returned TTL value of Windows system is 100-130 and that of UNIX/Linux system is 240-255. Of course, the TTL value can be modified on the remote host. For example, you can achieve it in Windows system by modifying the following values in the registry table:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]

"DefaultTTL"=dword:000000ff

255---FF

128---80

64----40

32----20

The **ping** command is basically explained. For some reasons including my little collection, the parameters of **–j** and **–k** are not described in detail. I hope you can add more using skills after reading this article. Thank you.