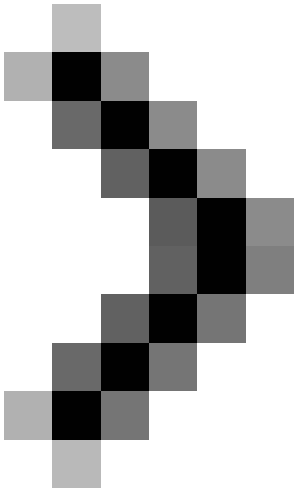
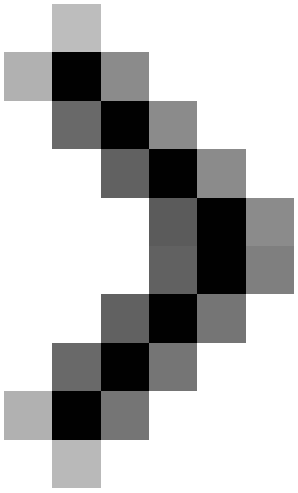
Troubleshoot connectivity problems in the network - Part 4

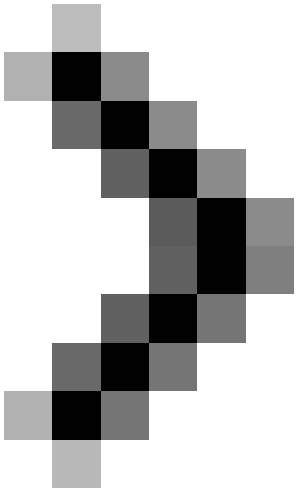
This section will continue the series on troubleshooting network connectivity issues in Windows by introducing packet loss issues and how to track packet data routes in the network.



Troubleshoot network connectivity problems (Part 1)



Troubleshoot network connectivity problems (Part 2)



Troubleshoot network connectivity problems (Part 3)
Brien M. Posey

Network Administration - *So far in this series, we have introduced the types of operations you can perform on the ping command to diagnose network connectivity problems. In this section, we will continue with some other variations of this technique.*

Packet loss

When we used the ping command, even if the command was successful or failed, it really was still insignificant. You can recall that the ping command is designed to return four different responses. Sometimes one or more of those responses may fail, while others may succeed. This happens to mean that the system is experiencing packet loss.

In such a case, the local host and the remote host or both work well, but there may be some other conditions that cause packet loss during transmission. Although the TCP / IP protocol is designed to enable it to retry a packet that has been lost during this transmission, the loss of the packet will reduce the performance of the system. A slow connection will now be more efficient for a high-speed connection that appears to have lost packet data.

One difficult thing about packet loss is finding its trace again. You may know that packet loss occurs if some responses to the ping command fail, but the ICMP packets used by this ping command are too small to return an existing network condition causing loss phenomenon in real situations.

If you suspect that packet loss may occur but when ping does not return any errors, then you can increase the size of the ICMP packets. Larger packages often lead to failure if a problem network exists. You can set a larger

package size in the ping command using the –L switch.

Using this switch is quite simple. All we need to do is enter the ping command and follow the address you want to ping, followed by the –L switch and the number of bytes you want to send. For example, suppose that your network is performing extremely poorly when connecting to a particular host. You may suspect at this time that packet loss may occur, but when ping results in great success. Please execute the ping command with the packet size of 1024 bytes as follows:

Ping 192.168.1.1 –L 1024

You can see the real example of how this command works in Figure A.

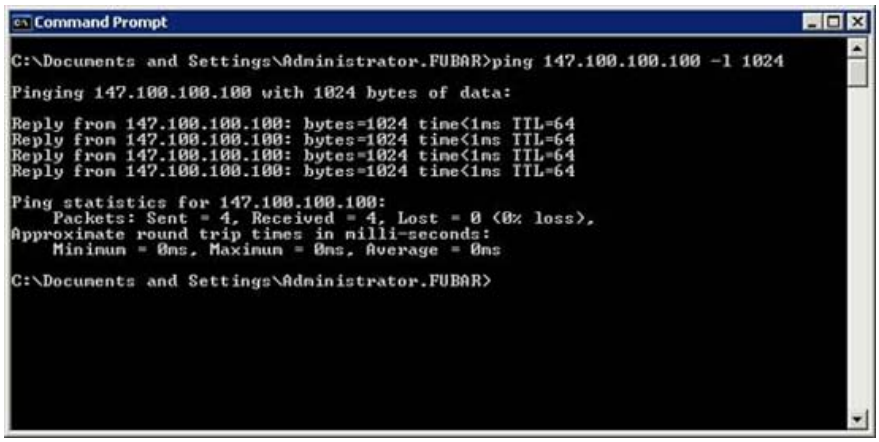


Figure A: Attaching the –L command to the ping command allows you to increase the size of the ICMP packet

Life time

The next concept that I want to show you is related to the ping command, which is a lifetime (Time To Live, abbreviated to TTL). If you look at Figure A, you will see at the end of each picture a reply that has TTL = 64.

As you may know, the Internet consists of a large number of connected routes. Each route is connected to at least two other routes. The idea behind the architecture is that if the link fails, there will still be at least one other path leading to the destination. The problem with this type of architecture is that when any link fails, the phenomenon of packets transmitted in endless loops will appear, and these loops will remain in the network without reaching the destination. Its finally.

This is the problem that design experts have included in the TTL value. You can assume the TTL value as a mechanism to destroy packets. This value is set to you first quite high, although this number may vary depending on the operating system you are using. Each time the packet travels through a router, the packet will be prompted to perform a jump. Every time a jump occurs, the TTL value is reduced by one. If the TTL value is zero, then the packet will be completely canceled. This avoids the fact that data packets do not go to the destination but are always on the Internet.

Check the route

Another reason why the TTL value is so useful is because the troubleshooting tool named tracert works on it. Using the ping command is good for troubleshooting small networks that have remote hosts near the hosts sending data, but when it comes to Internet or to a wide area network, the remote host might be the way. to thousands of miles. In addition, ICMP packets generated by the ping command can be transmitted through many routers to reach the remote host. So sometimes you will have a situation in which the local host and the remote host or both are good but one of the routers somewhere else has a problem. To fix that problem you can use the tracert command to diagnose what your problem is.

The tracert command works based on the ping command. The basic idea behind this command is to send an ICMP packet to the remote host, but with the TTL value set to a certain number. This makes the first router it encounters send back an expired TTL in the transmission message. This message includes information such as router identification that generates the message. Verify the router is demonstrated, then the ICMP packet is sent again but now with a different TTL value. At this point, the ICMP packet reaches the second router before the TTL value expires. This process is repeated, increasing the TTL value is done so until the destination host is reached. This allows you to get information about routers between the local host and the remote host. Sometimes you can use this information to track router problems that affect traffic flow.

Using the tracert command is the same as using the ping command. To do so, simply enter the tracert command, followed by the IP address or the complete domain name of the remote host. Figure B shows a case of using the tracert command.

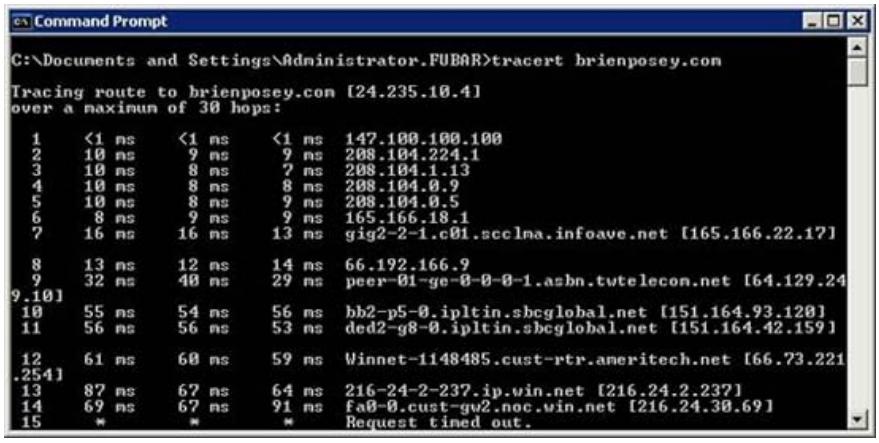


Figure B: Tracert command can be used to solve traffic flow problems

There are two issues to keep in mind while using this tracert command: first, some hosts can use firewalls to block ICMP packets. In this case, you will see a series of asterisks indicating that routing is not possible with the host because information cannot be obtained from that host.

Another problem lies in the hosts themselves, each router is assigned an IP address. Regardless of whether they are used for hosts or for routers, IP addresses are structured in a way that allows them to reflect geographic locations. In fact, sometimes this geographic information or even the route instructions are provided inside the tracert. If you want more information, try third-party software tools, which can graphically track tracert commands based on geographic information. You can see an example of such a tool in Figure C.

Figure C: You can perform a virtual tracert to determine the geographic location of the host

Conclude

In this article, I have shown you how to increase the number of bytes while using the ping command to trace a packet loss. Next, introduce the tracert command. In the next part of this series, we will continue the discussion by introducing how to interpret the results given by the tracert command.

You finished reading the article "**Troubleshoot connectivity problems in the network - Part 4**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.