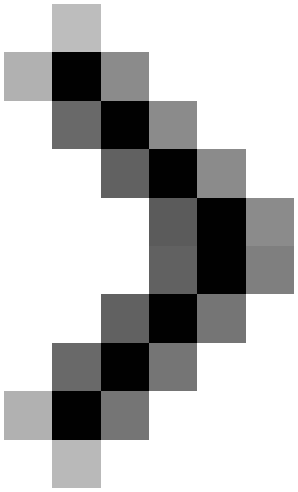
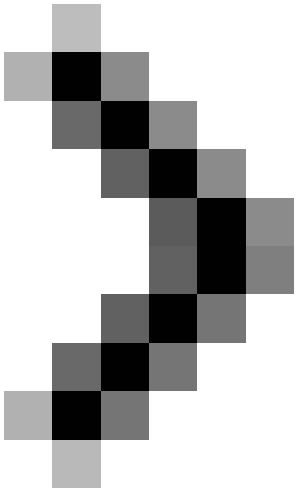
Troubleshoot network connectivity problems (Part 3)

The first test that you need to perform is to ping a local host address. There are a number of different ways to accomplish this task.



Troubleshoot network connectivity problems (Part 1)



Troubleshoot network connectivity problems (Part 2)

Brien M. Posey

Network Administration - *In the previous article of this series, I showed you how to distinguish which IP address your system is using as the primary address. The next step in the process is to verify if the IP address configuration works correctly and does not appear to have any problems with the TCP / IP protocol stack.*

The first test that you need to perform is to ping a local host address. There are a number of different ways to accomplish this task. The first way is to enter the command below:

PING LOCALHOST

When you enter this command, Windows will ping the address 127.0.0.1. Regardless of the IP address of your device, Windows always uses the 127.0.0.1 address as a local host address. Therefore, another alternative to the above command is to enter the following command:

Ping 127.0.0.1

After entering this command, you will see a successful ping process similar to other ping commands. See the example shown in Figure A.

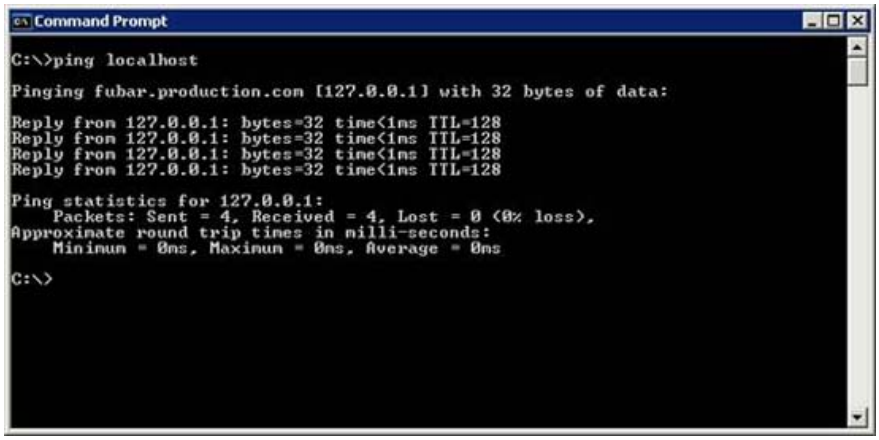


Figure A: You will receive a successful ping when you ping the local host address

Pinging the local host address has no effect in diagnosing communication issues with remote hosts. However, it does allow you to confirm that your local TCP / IP stack is functioning properly. If you ping the local host address and receive an error message stating that the destination has not been confirmed, then TCP / IP has been misconfigured or partially broken by a local TCP / IP stack.

Default Ping Gateway

In the previous article of this series, we mentioned that there are a number of different aspects of TCP / IP configuration and a bit of troubleshooting. Besides, there is some information or IP address of the default Gateway and the main DNS server.

Assuming that the hosts you want to communicate with are on a remote network, or on another network segment of your company, the next thing you need to do is ping the default Gateway. You can do this by appending the default gateway IP address to the ping command. For example, see in Figure B that you will see that the TCP / IP configuration lists the default Gateway address of 147,100,100,100. We have pinged this address. This operation has verified that the local machine can communicate with the default Gateway. It also tells you that communication on the local network is currently working as intended, at least at the IP address level.

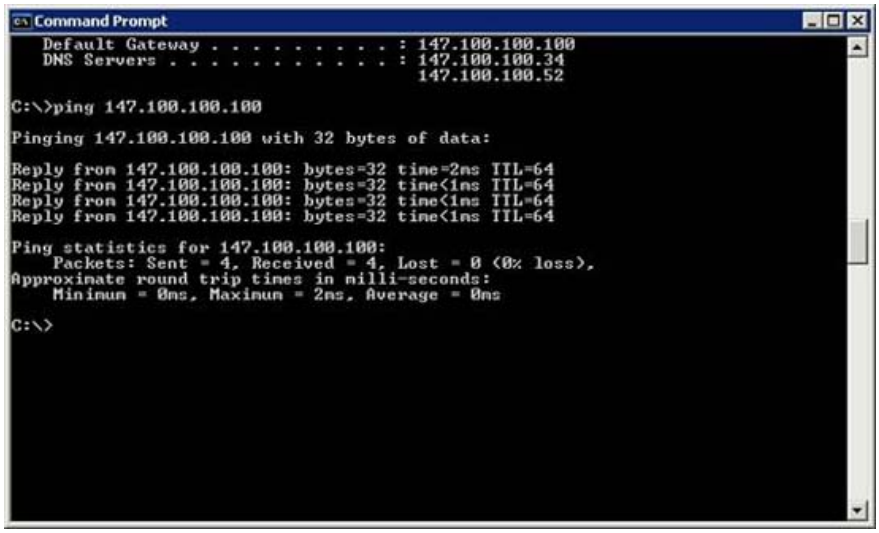


Figure B: Pinging the default gateway verified that IP packets can be reached default port of the network.

Ping DNS Server

So far, we have verified that IP-level communication is currently working between the local computer and the default Gateway. However, this does not guarantee that hostnames currently represent IP addresses. In the first part of this series, I showed you how to use the destination host's full domain name in conjunction with the ping command to verify that the DNS server is currently performing its job. However, there are other ways to easily test DNS.

One thing you can do here is to ping the DNS server's IP address, as shown in Figure C. While this operation does not guarantee whether the current DNS works properly, it also verifies that Internal computers can communicate with DNS servers.

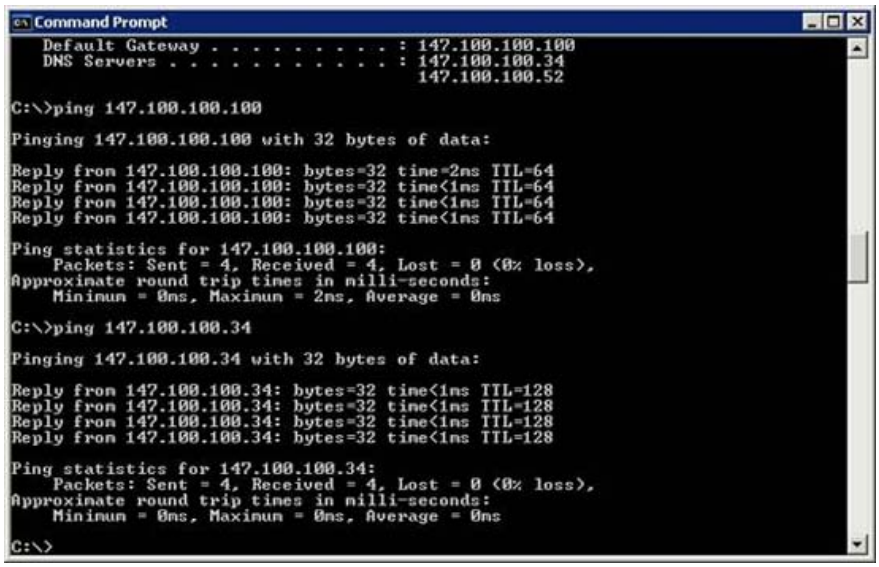


Figure C: You need to verify that the host can communicate with the DNS server

Another problem you can do is to use the Nslookup command to verify that DNS is working properly. To do this, simply enter the Nslookup command, followed by the full domain name of the remote host. The Nslookup command can analyze the complete domain name into an IP address, as shown in Figure D.

Figure D: The Nslookup command notifies you of the DNS server can resolve hostname or not.

The image above can be a bit confusing at first if you are not used to working with Nslookup. Initially, this screen will show an error report. If you look closely, you will see that the first pass is returned to the internal DNS server. This is because the referenced IP address matches the DNS server's IP address. However, the section below the returned information gives you the IP address of the host you requested. As long as this IP address is listed, your DNS query was successful.

If the domain resolution process fails, then there is a DNS problem. The real problem may be one of the problems with DNS servers. For example, DNS servers that are forwarding addresses may be wrong, or DNS servers may not be able to access the Internet (access levels need to contact higher-level DNS servers). It is also possible that the DNS server's DNS service may be stopped. These types of problems can also affect other clients because many clients often depend on a certain DNS server.

If DNS domain resolution is successful, you need to verify the IP address returned during the analysis process. You can do this by comparing the returned IP address with the real IP address that the remote host is using. These IP addresses need to be commensurate with each other, but there are some conditions that may cause the command to fail, and the communication result will fail.

If you encounter an IP address error, it could be the result of a malware intrusion into the client, or it could be the result of DNS infection. DNS infection is a process in which DNS cache will be propagated by wrong or invalid IP addresses.

If you encounter such a problem, we recommend that you scan the client for malware. You can also scan for spyware and viruses because they can cause problems like that. When the client is completely clean, clean the DNS cache. You can clean up DNS cache by entering the following command:

IPCONFIG / FLUSHDNS

You can see an example of this command in Figure E.

It is important to note that the DNS cache may contain incorrect IP addresses but it does not mean that DNS is poisoned. Sometimes hosts are assigned new IP addresses, which makes DNS cache sometimes unaware of those changes.

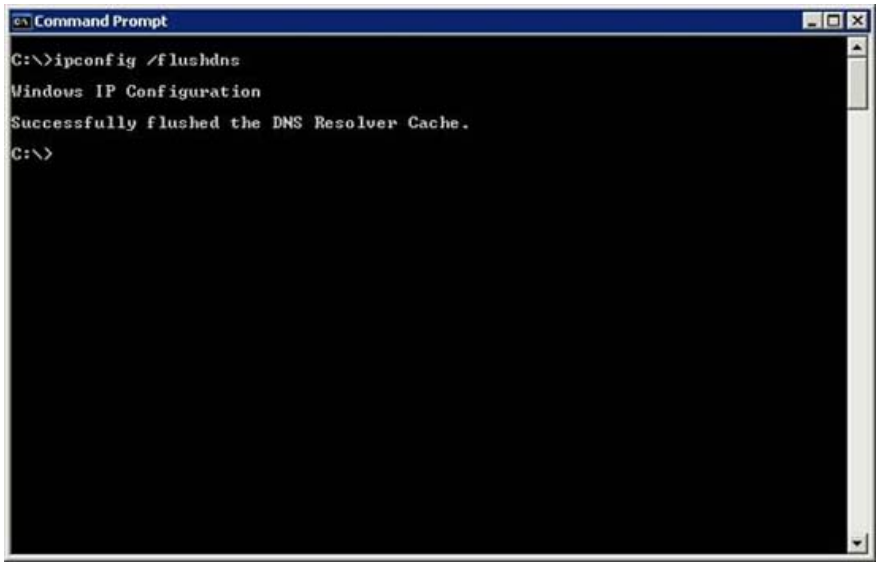


Figure E: If you suspect the DNS cache contains incorrect information, take measures to scan and clean the Internet

Conclude

In this article, I have shown you how to verify if the internal TCP / IP protocol stack is working properly. Next, explain how to test the internal host's ability to communicate with the DNS server and the default gateway server and how to test Hostname. In the next part of this series, I will show you some common problems in using the Ping command, namely discussing routing issues.

You finished reading the article "**Troubleshoot network connectivity problems (Part 3)**" 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.