10 tips for troubleshooting DNS problems

Takeaway: Figuring out what's wrong with DNS will go faster if you have a set of troubleshooting steps to follow. Brien Posey shares his approach to isolating the cause of DNS problems.

DNS is one of the most essential services on any Windows network. Active Directory can't function without DNS, and it's is also used by any number of other network functions. So it's critical to troubleshoot DNS problems as fast as possible. Thankfully, the process is usually fairly easy. Here are10 of my favorite DNS troubleshooting techniques.

1: Verify network connectivity

When DNS problems occur, one of the first things you should do is verify that the DNS server still has network connectivity. After all, if the problem ends up being something as simple as a NIC failure, you can save yourself a lot of time by checking for the problem up front.

The easiest way to verify connectivity is to log on to the DNS server and try to ping a few machines. You should also try to ping the DNS server from a few random machines. Remember that ping will work only if you allow ICMP packets through the firewall on the machine you are pinging.

2: Determine the scope of the problem

After you have determined that basic connectivity still exists, the next step is to determine the scope of the problem. Are Internet name resolutions failing or are local name resolutions failing too? The answer is going to make a difference in how you will have to troubleshoot the problem. For example, if local name resolution works but Internet name resolution does not, the problem may lie with one of your ISP's DNS servers.

3: Find out whether all users are affected

Another thing to look at is whether the problem affects all of the users on the network or it's limited to a subset of users. If you determine that only some users are affected, check to see whether all those users are located on a common network segment. If so, the problem could be related to a router failure or a DHCP configuration error.

4: See whether the DNS server is performing load balancing

Organizations hosting high demand Web servers sometimes try to distribute the workload across multiple identical Web servers by using a load balancing technique called DNS Round Robin. The problem with this technique is that the DNS server has no way of knowing when one of the servers has failed. As a result, inbound traffic is still directed to all the servers in round robin

fashion, even if one of those servers is offline. The result is intermittent connectivity problems to the load-balanced resource.

5: Check the DNS server's forwarders

If you determine that local name resolution requests are working but Internet requests are failing, check to see whether your DNS server uses forwarders. Even though many DNS servers use root hints for Internet name resolution, some use forwarders to link to an ISP's DNS server. And if the ISP's DNS server goes down, Internet name resolution will cease to function as the entries in the resolver cache expire. If your DNS server does use forwarders, you can try pinging the server to see whether it's online. You might also have to call the ISP to see whether it's having any DNS issues and to make sure that the IP address you are using in your forwarder is still valid.

6: Try pinging a host

If name resolutions are failing on your local network, try pinging some of the servers on your network. Start out by pinging the server's IP address. This will confirm that connectivity to the server is working. Next, try pinging by computer name and by the server's fully qualified domain name.

If you can ping the host by IP address but not by name, check your DNS server to make sure that a Host (A) record exists for the host. Without a Host (A) record, the DNS server will be unable to resolve the host's name.

7: Use NSLookup

One of the handiest tools for troubleshooting DNS failures is the NSLOOKUP command, which you can access from a Windows Command Prompt window. Simply type *NSLOOKUP* followed by the name of the host for which you want to test the name resolution. Windows will return the name and IP address of the DNS server that resolved the name (although the DNS server's name is often listed as Unknown). It will also provide you with the fully qualified domain name and the IP address of the host you specified.

NSLOOKUP is useful for two things. First, it allows you to verify that name resolution is working. Second, if name resolution isn't working, it allows you to confirm which DNS server is being used. Keep in mind that NSLOOKUP will list only the DNS server it initially connects to. If the name resolution request is forwarded to other DNS servers, those servers are not listed.

8: Try an alternate DNS server

Most organizations have at least two DNS servers. If your primary DNS server is having problems, try using an alternate. If name resolution begins working after you switch DNS servers, you have confirmed that the problem is indeed related to the DNS server and not to some external factor.

9: Scan for viruses

About a week ago, someone called me because every time they would try to visit certain Web sites they were redirected to a malicious Web site instead. I initially suspected a DNS poisoning attack, but ruled out such an attack because only one computer was affected.

The problem was that a virus had integrated itself into the TCP/IP stack and was intercepting all name resolution requests. Even though this initially appeared to be a DNS problem, the virus was ultimately to blame.

10: Reboot the DNS server

I know that it sounds like a cliché, but when all else fails, reboot the DNS server. I have seen several situations over the years in which name resolution stopped for an unknown reason but rebooting the DNS server fixed the problem.

Likewise, I have seen at least two examples of consumer-grade routers that have stopped forwarding DNS requests even though other types of traffic continue to flow. In one of these situations, resetting the router fixed the problem. In the other situation, the router had to be replaced. It was thought that the router might have been damaged by a power surge that had occurred a day before the problems started.