(Solved) DNS_PROBE_FINISHED error, degraded internet performance

Friday, May 15th, 2015

Recently at the office we started having major network issues:

- On my own computer, the problem surfaced as a `DNS_PROBE_FINISHED` error when I tried to load any websites in Chrome (sometimes instead the error would be `DNS_PROBE_STARTED` or `DNS_PROBE_NXDOMAIN`).
- I would then open up my command prompt and attempt to `ping google.com`—sometimes this would result in `unable to find google.com` and sometimes it would find a specific IP address to try but none of the pings would go through.
- I also tried `ping 8.8.8.8` (Google's DNS servers) or `ping 75.75.75.75` (Comcast DNS)—interestingly, the first 4-6 pings would fail, and then the rest would go through reliably at about 10ms every time thereafter.
- Ping traffic between any two points within the LAN (including the firewall) was completely unaffected.

Troubleshooting

Google searches for the `DNS_PROBE_FINISHED` error invariably lead you to advice suggesting that you perform a `netsh winsock reset` and restart your computer. However this didn't work in our case, unsurprisingly. The problem began affecting everyone at once, so unless there had been a bad Windows update or something (our IT support agency hadn't heard of any) this would be unlikely to help.

We also ruled out the ISP as the cause. We have two WAN connections–one fiber and one cable–and switching to one or the other exclusively did not resolve the issue. Support tickets with ISPs confirmed there were no upstream connection or network problems.

Examining Switches

We had just that day moved a bunch of desks around one part of the office. Our IT support agency suggested we had some kind of switch-level spanning tree problem[1]–a switch plugged into itself, perhaps, in some roundabout way. I tried rebooting the main switch used for non-VoIP traffic, and the problem immediately cleared up–for about ten minutes, and then it returned. We also tried disconnecting all the jacks for each person who had been affected by the move to rule out any subtle looping issues created (even though only one or two jacks had been affected); no dice.

I opened a support ticket with the switch company (Extreme Networks). They had me telnet into the switch and capture the output of a bunch of commands and send it to them, which allowed them to rule out any configuration or looping issues on the switch.

We upgraded the firmware, which dated from 2011, and restarted the switch. Again the problem cleared up and did not recur for the rest of the day. But by this point most people had gone home or to find somewhere else to work. I was curious if the problem would recur on Monday when everyone came back; sure enough, with 10 people in the office at 8:00 am Monday everything was fine, but by 8:30 we were having the same problem again.

At this point we were ready to try unplugging every person, port by port, waiting 5 seconds, and pinging google, to see if we could narrow the problem down to a particular network jack/user. Thankfully it didn't come to that.

The culprit

This time on our firewall I noticed that the "connection count" was hovering close to or even above the stated maximum of 10,000. Occasionally the connection utilization would drop to 5–6% and then the problem would go away. I used the firewall's "packet capture" interface to look at a few seconds' worth of network traffic and noticed a high number of UDP packets coming from a particular LAN IP address, with sequential foreign destination IPs.

I was able to track down the computer with this IP address, it happened to be one of our sales people. The laptop was a Lenovo running Windows 8. In Task Manager I saw that it was sending 1.5 MBps over the wired Ethernet interface and 800–900 Kbps over the wireless interface, even with no apps running. (Task Manager did not show which process

1. http://www.networkworld.com/article/2223757/cisco-subnet/9-common-spanning-tree-mistakes.html

was casuing this.) Upon disconnecting the CAT5e cable the connection utilization on the firewall dropped to 40%. Disconnecting the wifi dropped it further to 7%.

By looking at the CPU usage it appears that the process `discovery.exe` was abnormally high. A Google search finally turned up this article: Excessive network traffic and wifi drops linked to LenovoEMC Storage connector[2], which stated:

> Corporate networks or ISPs may detect an excessive amount of unusual network traffic coming from ThinkPad systems preloaded with Microsoft Windows 8.1. The network traffic may be interpreted as a network flood or denial-of-service attack. As a result, the system may become restricted on the network or the network may stop functioning normally.
>
> "LenovoEMC Storage Connector" is preloaded on some ThinkPad models to help customers discover and connect to LenovoEMC storage devices on their network. The process causing the network flood is `discovery.exe`, which is a component of "LenovoEMC Storage Connector".

Uninstalling the Lenovo EMC Storage Connector from the offending laptop finally fixed the issue.

2. https://forums.lenovo.com/t5/LenovoEMC-Network-Desktop/Excessive-network-traffic-and-wifi-drops-linked-to-LenovoEMC/ta-p/1513962