

Re: router causing strange DNS behaviour?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2005-05/0794.html>

From: Moe Trin (ibuprofin_at_painkiller.example.tld)

Date: 05/22/05

Date: Sat, 21 May 2005 21:16:48 -0500

In article <Pine.GSO.4.58.0505201730090.16395@cpu105.math.uwaterloo.ca>, James Muir wrote:

>On Fri, 20 May 2005, Moe Trin wrote:

>> "Boondocksville" doesn't specifically mean that it's at the end of the
>> earth as regards networking.

>Is there some implication here that Ottawa (the capital of Canada) is
>in the boonies? ;-

Well, it is a small provincial town, isn't it? :-) Actually, that remark was directed to prg with respect to rural towns in Arkansas and Idaho. The world really is a smaller place than it once was. Looking at the packets, nserc.ca seems to be 8 hops from my border router, but there is something two hops earlier that is dropping packets for me. The last identifiable hop is 216.191.228.70, which appears to be allstream.net in CYOW. For perspective, those internal only rogers name servers are 10 hops, the last five of which are rogers.com routers from their border (for me) host in Chicago.

>> When I tried the query of the nserc.ca name server at 198.96.3.152
>> (powerweb4.nserc.ca) asking for the IP of www.nserc.ca, dig reported
>> 305 msec.

>

>I just tried and I got 20 msec:

I just tried again so I could get the hop count (traceroute and tcptraceroute both lose it at 216.191.228.70, so I had to read the headers to get TTL), and it was 236, 240 and 238 msec.

>I have given up on Roger's DNS servers and am now using the public access
>DNS server ns1.granitecanyon.com [205.166.226.38] (courtesy of
><http://soa.granitecanyon.com/>). There are some other public access DNS
>servers listed at <http://www.open-rsc.org>. This solves the problem but it
>doesn't tell me why the problem occurred in the first place.

comp.os.linux.networking: Re: router causing strange DNS behaviour?

I can't see a good explanation either. If you want to make one more experiment, try using dig again, but this time, set the timeout to some long value (10 or 15 seconds) and see if you ever get a reply. The only explanation I have is that something in the authoritative chain of name servers is taking it's own sweet time to answer a query. Based on using dig and querying their name server by IP (which eliminates all the rest of the chain), I don't think it's nserc.ca that's holding up the show. Rogers, on the other hand...

*>Well, the OP (me) sent off a few emails to D-link tech support. They echoed
>Moe's suggestion that I statically configure each client behind the router
>to use Roger's DNS servers. This way the router would no longer be relaying
>DNS requests. Even though I tried this before without success, I decided to
>give it another go. At first this seemed to help.*

Again, using 'dig' with the +trace option might provide clues. I suddenly thought about a really unusual possibility. Could the router be also asking for IPv6 addresses (AAAA record, rather than an 'A' record_?

*>I was able to resolve www.nserc.ca a couple of times on both clients
>using Roger's DNS servers.*

Unless they've turned off caching (look at the reported TTLs), only the first query in any 60 minute period should be from "outside". There after, they should be caching the answer, and the delay in a response should only be the time to query the Rogers servers directly.

*>But, after 10mins and a few reboots, the problem came back. So it seems
>that it is not just a problem with the way the router relays DNS packets.*

That says there is something fscked with the Rogers servers, as they should be caching the answer for 3600 seconds, and your rebooting should have no effect on the results.

*>I think my service agreement with my ISP says that I am not supposed to
>have more than one client connected to the cable modem (a Webstar). I
>wonder if they have found a way to detect that there is more than one
>client behind the router*

Detecting is fairly easy, especially if the systems are running different operating systems, or if there is "unusual" use of port numbers (masquerading is often detectable because of the use of "high" port numbers (for Linux, 60,000 and above) compared to a more normal 1025 to 32000 range. At home, I run a passive O/S fingerprinting tool just to see who's sniffing at the firewall. About 3 percent of the hosts show up as masqueraded. And the TOC does prohibit more than one system per residential setup (as opposed to a business grade connection).

*>and have implemented some kind of countermeasure. But then why would I
>only be experiencing a problem with one url?*

Re: router causing strange DNS behaviour?

comp.os.linux.networking: Re: router causing strange DNS behaviour?

Highly unlikely. Without sniffing the packets on both sides of the router, it's kinda hard to isolate the problem.

*>In any case, now that I have a fix, I think I will have to stop
>investigating and get back to other things.*

Ah, you're no fun. ;-)

Old guy