

## Re: router causing strange DNS behaviour?

**Source:** <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2005-05/0757.html>

---

**From:** Moe Trin ([ibuprofin\\_at\\_painkiller.example.tld](mailto:ibuprofin_at_painkiller.example.tld))

**Date:** 05/20/05

Date: Fri, 20 May 2005 15:09:35 -0500

In article <1116564501.929117.113030@g47g2000cwa.googlegroups.com>, prg wrote:

>

>Moe Trin wrote:

>> Suspicion: 'dns.<mumble>.rogers.com' is for customers, while the unwashed

>> masses out here are supposed to use ns?.<mumble>.rogers.com.

>

>Could very well be the case. These cobbled together ISP networks can

>be Byzantine. That's why I like poking at them with traceroute just to

>see where they let me go before dropping packets. It's not very

>efficient but turns up surprising results sometimes ;)

I think this was a 'anti-denial-of-service' thing started when bandwidth was more precious.

>>> As near as I can tell from the manual, your d-link is DNS dumb and just

>>> forwards the IP/UDP/DNS packets.

>>

>> WHOOPS! Is that an intentional red flag you are waving?

>Nope, no flags, just quick-n-dirty putzing while killing an hour.

OK - just checking

>All my queries (then and below) used default UDP and UDP was all that

>was used. OP seemed concerned about the "Warnings" so ...

It was just one more thing that "could" go wrong. I suspect those warnings are due to the slow response of the authoritative name server chain.

>Tonights timed queries were quite good (once my ISP got out of the way

>looking up names for ethereal). Initial query took about 4.5 secs

>start to finish with the query time (from trace):

At least on the "default" compile of 'dig' the timeout is set to 4 seconds. That might be a problem. At least on this system, 'resolv.h' sets the RES\_TIMEOUT to 5 seconds, and the system will retry up to 3 times if there is a timeout.

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

>Standard query A www.farmimplement.com: (small town in central Arkansas)

yabbut that's 65.216.49.59 which is uu.net

>; <<>> DiG 9.2.1 <<>> @205.166.226.38 www.cityofsearcy.org

66.136.239.195 which is SBC (swbell)

>; <<>> DiG 9.2.1 <<>> @205.166.226.38 weiser.govoffice.com [in SW Idaho]

63.228.251.51 which is qworst

>; <<>> DiG 9.2.1 <<>> @205.166.226.38 www.buhlidaho.us [in S Central Idaho]

216.55.145.2 which is Abacus America (abac.com) which is a /18 with at least a decent sized feed from Level3

"Boondocksville" doesn't specifically mean that it's at the end of the earth as regards networking. Actually, only the swbell address is more than 9 hops from my border router. (SWBell looks to have their routing much more fragmented, as I make 11 hops \_within\_ their domain [SJC twice, SFO, SLC, DEN, MKC twice, and 3 in LIT] alone.)

>Can't see why OP could not use this for a name server if it \_is\_ a

>Rogers DNS issue instead of his router.

I dunno. Rogers is a Canadian ISP, and their name servers should have the IPs of the TLD servers authoritative for .ca cached (there are apparently six servers authoritative for .ca., with 2 day TTLs on their names and IP addresses). I don't know how many \_domains\_ there are in .ca (ARIN has assigned 4911 IPv4 networks totalling 64,933,888 individual IP addresses though there are only 763 autonomous system numbers). This means the worst case query scenario should be a query to the .ca name servers, which should return name and IP of the SLD server (here, nserc.ca), which should then result in a third query which should provide the desired answer. 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.

>Actually the OP's symptoms seemed a mixture of possible problems:

>-- ISP's internal workings

>-- ISP's name servers

>-- dslreports FAQ on Rogers saying that his d-link was flakey with

>certain Terayon modems used by Rogers

I'm still wondering if increasing the timeout might also help.

>Had to leave \_something\_ for OP to investigate ;)

True.

Re: router causing strange DNS behaviour?

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

Old guy