r/pihole Search Reddit Advertise

r/pihole

Posts Github Community Documentation Donate

Posted by u/elias4444 2 years ago

Chicken and Egg problem with Asus Router WAN connection

I'm trying to figure out how to solve this particular problem. When I set my Asus router to use an internal IP address for DNS (pi-hole on RPi) under the WAN connection, it often doesn't connect to my ISP at all (Xfinity). I'm guessing it's trying to lookup a domain name to establish a connection, which Pi-hole can't get because, well, it's not connected to the Internet yet.

If I setup clients to use Pi-hole for DNS directly in DHCP settings, I get ads, because then the router always feeds itself as a backup DNS (and, ergo, the ISP assigned DNS), even when not specified.

How have others gotten around this?

ANSWERED: For those who find this, I discovered a solution. Make sure to first set the pi-hole address as the DNS server under LAN->DHCP Server->DNS Server.

Then, you'll need to SSH into your router (enable SSH under Administration->System) and do the following commands (where yyy.yyy.yyy.yyy is the IP address for your pi-hole):

```
nvram set dhcp_dns2_x=yyy.yyy.yyy.yyy | nvram commit
service restart_dnsmasq
```

This will set the pi-hole as both the primary and secondary DNS server for clients via DHCP.

By default, Asus routers set the router as the secondary. If Merlin firmware is available for your model, you can run that instead, and it will give you an option to turn off this behavior rather than using the work around above.

36 Comments Award Share ...

Comment as netmind604

What are your thoughts?

Markdown Mode Comment

TheMadMan007 · 2 yr. ago

Set the Pi-Hole as the LAN DNS not the WAN.

8 Reply Give Award Share Report Save Follow

elias4444 OP · 2 yr. ago

Right, but if I do that, the router adds itself as a backup DNS even though I don't specify it. How can I stop that?

1 Reply Share ···

Scurro · 2 yr. ago

Disable DHCP on your router and use the pihole for DHCP.

12 Reply Share ···

backyardprospector · 1 yr. ago

It breaks NTP though and remote administration of the router.

1 Reply Share ···

Scurro · 1 yr. ago

It does not. Your router should be set up with a static IP for the LAN interface.

1 Reply Share ···

MaT4w8b2UmFX · 2 yr. ago · *edited 2 yr. ago*

> If Merlin firmware is available for your model, you can run that instead, and it will give you an option to turn off this behavior rather than using the work around above.

I will second this solution. Just did this a couple days ago to enable the toggle option. I'm rocking a single DNS server on my clients now, my Pi-Hole!

6 Reply Give Award Share Report Save Follow

tallmansix · 2 yr. ago · *edited 2 yr. ago*

TLDR: Use the PiHole as the DHCP server

I've just spent the last week faffing around with this and learned quite a lot about getting PiHole running with an Asus router.

PiHole in the WAN DNS - so as per other posts, leave that setting as a normal external DNS provider. Even if this worked, it isn't the best setup because you can't see which client is sending the DNS traffic in the PiHole query log.

2. When you set DNS in the LAN DHCP for a stock Asus router you can only provide the primary DNS for your PiHole and the secondary DNS will always be set as the router itself so some (half maybe) of your DNS traffic will end up being resolved by the router / external DNS rather than PiHole.
3. Apparently with ASUSWRT Merlin firmware you can set a secondary DNS and stop the router advertising itself as a DNS server. I can only use stock firmware on my GT-AC5300 so I can't take this option.
4. So I've decided to use the PiHole as the DHCP server because this stops the router being advertised as the secondary DNS server to the clients. It does however again only provide a primary DNS server option so some clients take it upon themselves to appoint their own secondary DNS server.
5. To force a secondary DNS server in the DHCP settings create a config file with additional settings for primary and secondary DNS:

Create a new config file:

```
sudo nano /etc/dnsmasq.d/03-pihole-dhcp.conf
```

Add the following and save

```
#PI hole IP addresses - replace with your actual PiHole IP address(es)
dhcp-option=6,192.168.74.3,192.168.74.3
```

Restart PiHole or reboot to grab the new settings.

Even after the above I'm still getting some DNS leaks direct to the router, it might be DHCP leases that haven't renewed yet so will have to wait another 24 hours or reboot the clients to know for sure but I did the following on the router to detect the leaks: (replace IP addresses with your PiHole IP address)

```
iptables -t nat -A PREROUTING ! -s 192.168.74.3 ! -d 192.168.74.3 -i br0 -p tcp
iptables -t nat -A PREROUTING ! -s 192.168.74.3 ! -d 192.168.74.3 -i br0 -p udp
```

This reroutes any DNS traffic that is not already routed to/from PiHole and sends it to the PiHole.

I can see on my PiHole logs a number of DNS requests that are from the router after doing the above so some clients still aren't adhering to the DHCP settings right now - I'll know more in another day or so as to whether these are hardcoded DNS server in some of the clients.

14 Reply Give Award Share Report Save Follow

6 Reply Share ···

tallmansix · 2 yr. ago

Me too, that's why I've spent a week on this trying to keep the router as DHCP server and the only option so far means I can't see the per client activity in PiHole.

I've also started to realise that the PI is now a potential single point of failure on an otherwise robust network setup and I'm not totally happy with it, more so for the DNS than the DHCP.

I'm now thinking of getting a second one for redundancy.

2 Reply Share ···

sur_surly · 2 yr. ago

I had a pihole on my network for adblocking, but setup a backup public DNS so if the pihole failed I'd still have internet. At some point later, I was like "why am I seeing so many ads?" come to find out the pihole crashed weeks ago.

Could have redundant piholes for dns blocking but unless you can setup redundant dhcp servers via pihole I'd be wary (I haven't tried, maybe it's possible and then it'd be fine)

Though I don't have an Asus router. So OP's problem isn't one I needed to solve.

1 Reply Share ···

tallmansix · 2 yr. ago

How did you set up a backup public DNS?

I ask because my understanding is that when you set primary and secondary DNS, clients will use either and not necessarily the primary one all the time.

I believe dual DHCP servers are possible as long as the scope of each doesn't overlap ie - DHCP server 1 gives out 192.168.1.1 - 120 and DHCP 2 gives out 192.168.1.121 - 254 for example.

4 Reply Share ···

tallmansix · 2 yr. ago · *edited 2 yr. ago*

Just seen your answer in the question after posting my reply, I will give that a try as an alternative although I'm not convinced it will stop the router advertising itself as a DNS forwarder as the ASUSWRT-Merlin firmware has this is a separate setting to the two DNS servers.

4 Reply ···

saint-lascivious · 2 yr. ago

> I'm not convinced it will stop the router advertising itself as a DNS forwarder

Good. Because it won't.

4 Reply Share ···

tallmansix · 2 yr. ago

Thanks for confirming, will stick with PiHole DHCP and try to figure out what is still leaking DNS requests direct to the router. I noticed for example my Netflix app on a Samsung TV automatically assigned 8.8.8.8 as secondary DNS server even though the TV itself only had my PiHole listed as DNS in the network settings.

1 Reply Share ···

saint-lascivious · 2 yr. ago

An Android based TV?

This is usual behavior. Everything should have a secondary upstream per specification. So it's doing it for you. Push two upstreams, make them both your Pi-hole.

If it won't let you enter the same address twice, either give the Pi-hole a second static address, or push a null or unassigned address as the secondary.

3 Reply Share ···

tallmansix · 2 yr. ago

Not Android, Tizen based Samsung TV.

And yes, 100% is now pushing two DNS servers via DHCP after making the change in my original comment, shows as PiHole IP for 1st and 2nd DNS on my laptop and iPhone for example however the Samsung TV only shows one DNS on the network settings, even if I try to manually change it, only one allowed.

Then when I open the Netflix App on the TV and go to network status it is showing PiHole as DNS 1 and 8.8.8.8 as DNS 2 with no way of editing it.

Learning a lot this week - especially how chatty my Samsung TV's are with telemetry / advert domains.

2 Reply Share ···

mag914 · 2 yr. ago

3 Reply Give Award Share Report Save Follow

tallmansix · 2 yr. ago

See my comment above, I’m also using a ROG GT-AC5300 and yes it does behave in the same way but there are ways round it.

1 Reply Share ···

mini4x · 2 yr. ago
#131

Just add two!

1 Reply Share ···

billiarddaddy · 2 yr. ago

The DNS the router uses and the one it assigns via dhcp might be two different things.

2 Reply Give Award Share Report Save Follow

renna99 · 2 yr. ago

Had the same problem - either use the solution provided in OPs post or just set your pinhole as dhcp server, that fixes it aswell.

If both are not an option Merlin firmware allows to turn off the router advertising itself as dns2.

2 Reply Give Award Share Report Save Follow

hoiduck · 2 yr. ago

This is an excellent post, mate. Your solution was remarkably lucid and quick to follow. Thanks!

2 Reply Give Award Share Report Save Follow

slinkyrichie · 2 yr. ago

Set the PiHole IP in the DHCP settings.

1 Reply Give Award Share Report Save Follow

elias4444 OP · 2 yr. ago

Right, but if I do that, the router adds itself as a backup DNS even though I don't specify it. How can I stop that?

slinkyrichie · 2 yr. ago

The DNS settings under DHCP? So that the DNS is handed out to clients with an IP.

1 Reply Share ···

elias4444 OP · 2 yr. ago

I put the address for the pi-hole server there, and it hands it out correctly. However, it also automatically tacks on the address of the router as a secondary DNS server. The router then uses the DNS it was assigned through it's WAN connection to the ISP, effectively circumventing the pi-hole DNS.

When I used the MERLIN firmware, there was an option to turn this off. However, after upgrading my router (model that doesn't have MERLIN available), I can no longer turn that off as far as I can find.

1 Reply Share ···

slinkyrichie · 2 yr. ago

What router do you have? I used to run the AC68U, AC87U, AC88U, and the final one was the AX88U. All ran Merlin and I run PiHole.

On a device that's connected to the network, check the network settings. Usually there will be 2 DNS records, or one if using PiHole. What are the 2 DNS IPs that show?

1 Reply Share ···

garciaargos · 2 yr. ago

I have an RT-AX88U running the default Asus firmware (latest version, working since a couple of versions ago), handling both the DHCP and it correctly tells every client to use my pi-hole (and only the pi-hole) as the DNS server, as configured in the LAN DHCP Server page. The WAN DNS is set to OpenDNS. All clients correctly get the pi-hole as the sole DNS server. At no time have I ever had to do any SSH sorcery for things to work in my setup. I'm confused why you would need to do such things.

Just to be clear: the WAN settings should have no reference to the pi-hole IP address. This goes only into the LAN DHCP server settings.

I don't think I've ever seen any setting that would cause the router to send its own IP address as DNS when one is already set, but it might be different for different models and firmware versions.

1 Reply Give Award Share Report Save Follow

MaT4w8b2UmFX · 2 yr. ago

I wonder if they changed this in the newer firmwares then. All the old ones automatically add the router's LAN IP address as a secondary DNS server, giving any clients a total of two DNS servers.

Can you confirm this with some sort of client screenshot?

To enable a toggle, to get the same setup you have (a single DNS server), I had to do the custom firmware Merlin upgrade, or as you can see another user details out the SSH commands that will accomplish the same thing.

1 Reply Share ···

garciaargos · 2 yr. ago

Well, aren't I an doofus. I was looking at my desktop config which is set manually. Of course that one shows a single DNS server, duh. The phone shows the router as well, in second place. I stand very much corrected.

However, this would only be an issue in case the pi-hole is actually down, wouldn't it?

I did a quick check on the phone and a couple of other machines set to automatically get the DNS server, and it definitely resolves using the pi-hole first, so blocked sites in the lists do get blocked. I also correctly see blocks for every client in the network.

2 Reply Share ···

elias4444 **OP** · 2 yr. ago

I'm using the Asus XT8 mesh routers. I can confirm that the latest firmware automatically adds the router as a secondary DNS to whatever you put into the DNS setting under DHCP.

1 Reply Share ···

user__already__taken · 2 yr. ago

I suspect you will have to add that command to a script that gets executed at startup, otherwise you'd have to run it each time you reboot. I used to own an ASUS router and it was being rebooted on a weekly basis!

1 Reply Give Award Share Report Save Follow

elias4444 **OP** · 2 yr. ago

I did test for that with a router reboot, and at least in that case, the new setting remained in effect.

1 Reply Share ···

rougebarman · 1 yr. ago

WAN DNS triggers this error. I'm experimenting with changing DHCP server from router to pihole, but too early to deem a success.

Static IP allows me to specify DNS, blocks ads but my DNS records leak which is a major concern in the UK. Might be a temporary work around for those less concerned by leaks and just wanting ad blocks.

1 Reply Give Award Share Report Save Follow

backyardprospector · 1 yr. ago

Thank you I was looking for a solution to this other than turning off wan dns which is what I had been doing. No Merlin for the rog router.

1 Reply Give Award Share Report Save Follow

demigoth2010 · 3 mo. ago

I am coming late to the party, I just set the advertise to NO in my ASUS router with merlin firmware and now I am getting 3 DNS servers, 2 are my pihole and my third is the router... am I doing something wrong?

1 Reply Give Award Share Report Save Follow