DNS in Routers Considered Harmful

Priyank Mahour [2022201047]
Ujjwal Prakash [2022202009]
Prashant Kumar [2022201058]

International Institute of Information Technology, Hyderabad, India

31st March 2023

Introduction

- DNS forwarders are commonly incorporated in residential routers to facilitate the transmission of packets between LAN client devices and the upstream resolver provided by an ISP for domain name system resolution purposes.

- DNS forwarders often implement a cache to store records from DNS responses of the upstream resolver locally.

- DNS forwarders can reduce latency and enhance performance.

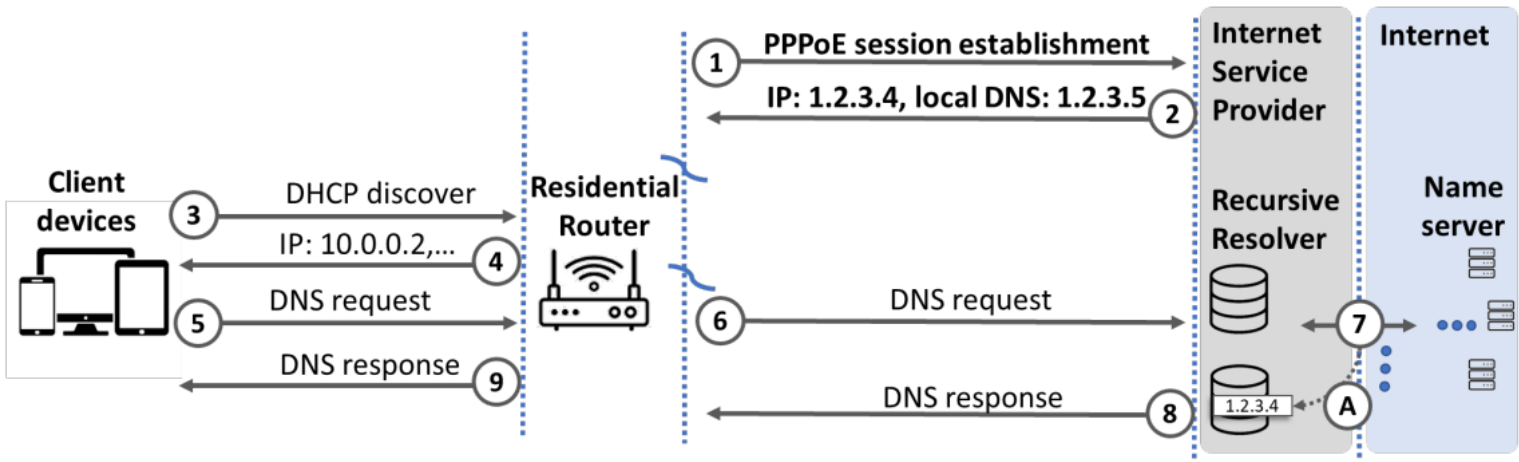

Figure 1: DNS forwarding in routers

What Makes DNS forwarders vulnerable

- Source from third-party software developers, leading to cheap and vulnerable implementations.
- Difficult to patch, leading to a high risk of attacks.
- Vulnerable to attacks, such as DNS cache poisoning, which can affect all client devices on the LAN and redirect them to incorrect malicious hosts.

Cache Poisoning Attack

- Enter false information into a DNS cache so that DNS queries return an incorrect response and users are directed to the wrong websites.

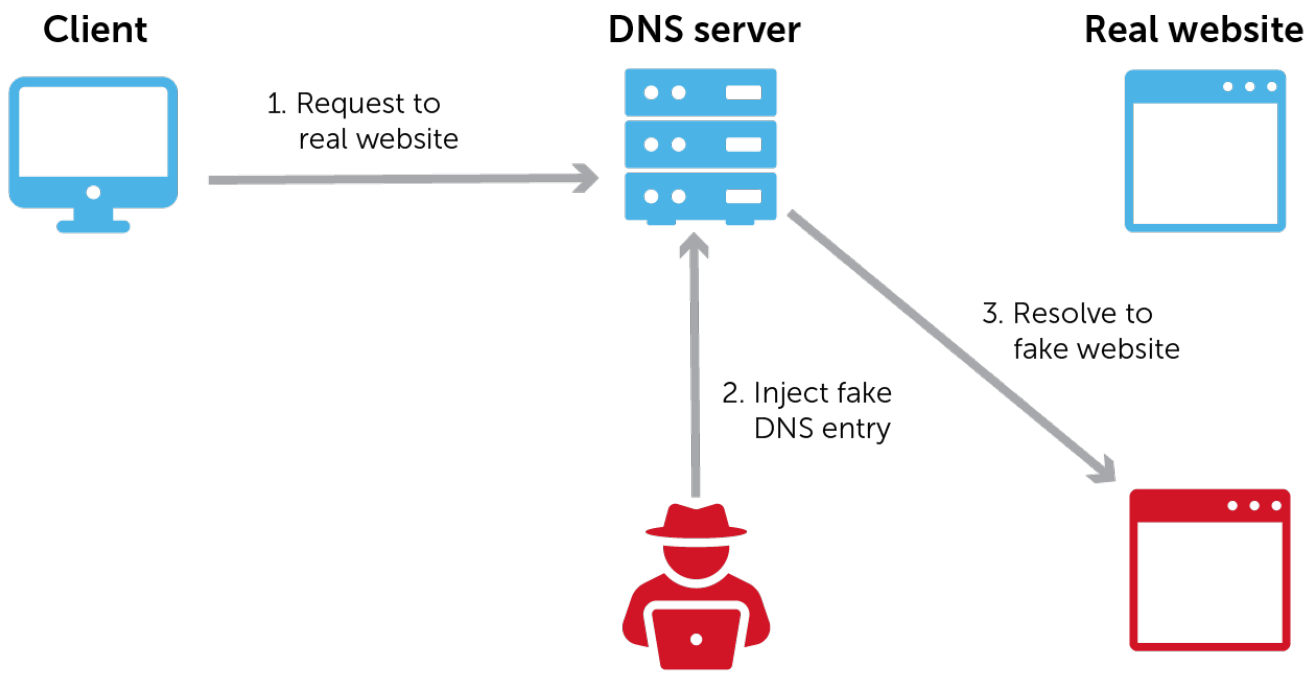

Figure 2: Cache poisoning attack

DNS functionalities in router

- Create a separate internal network segment with its own IP address set, allocated to client devices via DHCP.
- Routers need DNS forwarding to ensure clients can always find the correct DNS resolver despite any ISP network configuration changes.

Benefits of DNS forwarders

- Provide benefits like DNS filters, local DNS domains, and security protections, but a previous study found that many routers do not include most of these functionalities and security features.

- Routers implementing DNS forwarders are vulnerable to various DNS attacks, ranging from cache injection to disabling DNSSEC validation.

- Based on the risks associated with DNS components in routers, the recommendation is to remove DNS components from routers as they are the most vulnerable devices to cache poisoning attacks.

Removing DNS from routers

- DNS is a weak spot in routers, and fixing specific software bugs or replacing DNS forwarders does not provide a solution to future vulnerabilities.

- Removing DNS from routers can improve the resilience and security of home networks without a significant loss of performance.

- Removing DNS from routers will eliminate the cache poisoning threat and simplify the routers, without requiring any changes to the clients with less overhead.

- Three Mechanisms
  - Manually configure upstream resolver
  - NAT rule to relay requests to upstream
  - Communicate DNS servers to client devices

Manually configure upstream resolver

- Clients manually configure their systems to send queries to an upstream resolver directly to bypass DNS forwarders in routers.
- This can be done by configuring the IP address in the resolv.config file to the IP address of the ISP.
- Drawback
  - Clients need to configure the IP address of the DNS resolver of the ISP and if new devices added to the LAN will also need to be configured.
  - If the ISP changes the DNS resolver to a different IP address, all client devices need to be reconfigured.
  - Manual configuration can be time-consuming and error-prone, especially for non-technical users.
  - May work for smaller networks with fewer devices, but it may not be practical for larger networks or less technically inclined users.

NAT rule to relay requests to upstream

- Systematic method for implementing DNS forwarding without requiring clients to change their network configurations.
- Implementing a DNS forwarder as a simple Network Address Translator (NAT) with IPtable rule, not as a service running on the router's os.
- Client sends a DNS request to the router's internal network address but it will be directly sent to the ISP's resolver with a firewall rule.
- Whenever the internet connection is re-established or the router is booted, the firewall rule is changed to route the DNS requests to the correct destination.

Communicate DNS servers to client devices

- Use IPV6 stateless-auto-configuration(SLAAC) mechanism via ICMPv6 instead of DHCP protocol which broadcast the network configuration in the local network segment.
- Used to communicate changes in DNS resolver configuration to clients overcoming the synchronization issue.
- ICMPv6 is only available for configuration of IPv6 addresses, routers which support IPv4-only clients cannot use this option and must still implement some form of DNS forwarding service.

Performance Costs

- Measurable performance impact of disabling DNS caching in routers was an increase of 1 RTT for page loading time when a DNS record was requested that was not in the local DNS cache, but was present on the router's cache.
- So removing cache from routers has a negligble impact on performance.
- Records which are recently visited are also cached in the browser's DNS cache.
- TTL values of most records are less than 5 minutes, in most cases clients still have to wait for the query to be recursively resolved by the ISP.

Assumptions

- It is assumed that DNS forwarders are not implemented by router developers but by third-party vendors and these vendors provide cheap and vulnerable forwarders for the sake of multiple functionalities.

- It is assumed that the updates to DNS forwarders by third-party vendors are inconsistent and sub-standard patches.

Critiques

- The DNS forwarders are not necessarily implemented by thirdparty vendors.
  Solution: these forwarders can be implemented by router manufacturers and developers with a firewall feature which mitigates the security risks of DNS forwarders.
- When the forwarders are inhouse developed by the manufacturers, the updates are consistent, timely and follow the latest security guidelines for patches.
  Solution: Following the above assumption, when the forwarders are inhouse developed by the manufacturers, the updates are consistent, timely and follow the latest security guidelines for patches.

Critiques

- Routers in LAN are generally open resolvers, this allows the attacker to perform the cache-poisoning attack. We can implement the cache poisoning attack by injecting records into the DNS cache.
  Solution: These attacks can be prevented by implementing security features like DNSSEC(Domain Name System Security Extensions) protocol. It prevents attackers from manipulating or poisoning the responses to DNS requests.

- Since the addresses are manually configured on each client, it poses a synchronizatio‘n problem in case the internet connection between the routerISP is reset as the client has no way of knowing the change in address of the upstream resolver.
  Solution: We can implement a feature at the router which broadcasts the change in the IP address of the upstream resolver to all the clients present on the LAN.

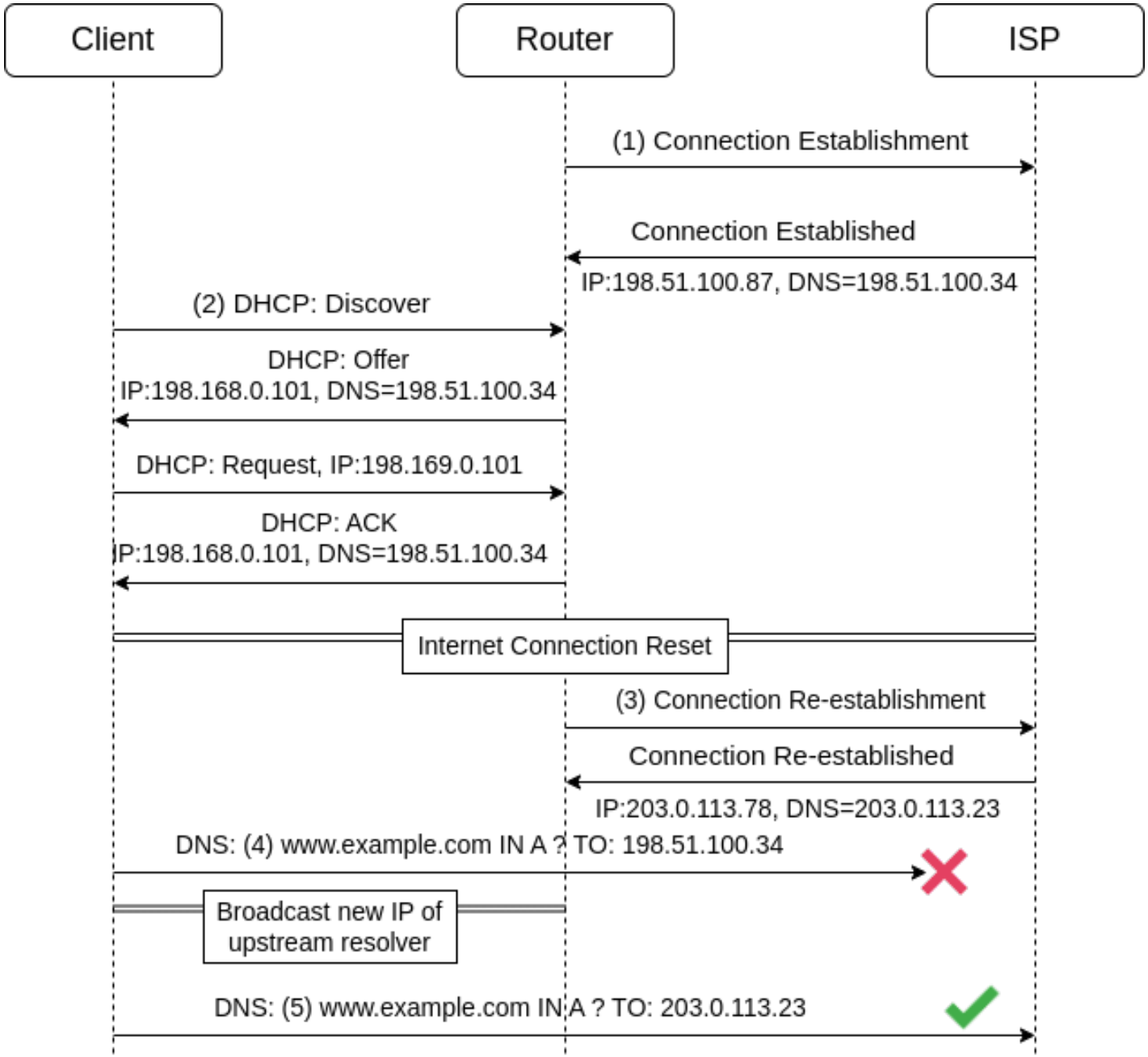

Figure 3: Broadcasting IP of upstream resolver

Critiques

- Network Address Translators(NAT) are not completely immune to attacks. The attacker might try to change the address translations in NAT with malicious IPs.
  Solution: - Instead of NATs, we should implement a mechanism that routes the requests to the ISP's DNS while filtering incoming and outgoing traffic with a firewall validating the source of the incoming request.

- The communicate DNS servers to client devices solution is only applicable to clients using IPv6 addresses and cannot be implemented on routers using IPv4 addresses.

Conclusion

- The paper "DNS in Routers Considered Harmful" proposes an unconventional yet commendable way to solve the security threats posed by DNS forwarders in routers during DNS lookup and resolution.
- It suggests completely removing DNS in routers with alternate solutions as explained above. Not all these solutions are scalable and have their own limitations on the implementational fronts.
- Although the impact on performance cost of removing DNS in most cases(not all) is negligible as mentioned in the paper.
- We have tried to find some problems that challenge the claim that removing DNS substantially increases the security gain and also tried to propose some possible solutions to those challenges.

References

[1.] K. Man, Z. Qian, Z. Wang, X. Zheng, Y. Huang, and H. Duan, "DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels," in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security CCS. ACM, 2020.

[2.] K. Schomp, M. Allman, and M. Rabinovich, "Dns resolvers considered harmful," in Proceedings of the 13th ACM Workshop on Hot Topics in Networks, 2014, pp. 1–7

[3.] P. Jeitner, H. Shulman, L. Teichmann, and M. Waidner, "XDRI Attacks - and - How to Enhance Resilience of Residential Routers," in 31th USENIX Security Symposium (USENIX Security 22), 2022.

[4.] Security Considerations sections of the Internet Engineering Task Force's (IETF's) RFC2663 and RFC2993