DNS in Routers Considered Harmful: A Literature Review

Priyank Mahour[1], Ujjwal Prakash[1], Prashant Kumar[1]

[1]International Institute of Information Technology, Hyderabad, India
https://www.iiit.ac.in/
{priyank.mahour,ujjwal.prakash,prashant.k}@students.iiit.ac.in

Abstract. Residential routers often exclude various functionalities and security features of DNS to reduce costs. However, they still contain DNS forwarders that act as proxies, directing clients' requests to another address. These forwarders separate the network configuration of the internal client network from that of the ISP, allowing connectivity without synchronization. Nevertheless, the history of cache poisoning attacks reveals that such simplified implementations expose many vulnerabilities. The paper suggests eliminating DNS from routers and demonstrates that the performance impact is minimal, while the security benefits are significant. It also examines several methods for implementing the proposal.

Keywords: Routers · DNS · Attacks · Security.

1 Summary

DNS forwarders facilitate the exchange of packet between client devices(on LAN) and upstream resolver(ISP). These forwarders offer a link between stub resolvers on client devices and the recursive resolver of the upstream provider, which provides comprehensive recursive lookup services along with caching. By storing records from DNS responses locally, DNS forwarders can reduce latency and enhance performance. However, residential routers with DNS forwarders are vulnerable to various types of attacks. Any vulnerability in a DNS forwarder can expose all devices on the LAN to risks, and a DNS cache poisoning attack can redirect client devices to malicious hosts, thus affecting all users.

1.1 DNS functionality in routers

DNS forwarders create a separate internal network segment with its own set of IP addresses, including those of the default gateway and DNS resolver, which are allocated to client devices via DHCP. Routers require DNS forwarding functionality because they cannot simply provide clients with the address of the upstream DNS resolver. This is because the ISP may reassign a different network block to the customer, resulting in a different DNS server configuration. Without a synchronization mechanism, this could lead to connectivity issues, as clients would not know where to send their DNS requests.

1.2 Benefits of DNS forwarders

DNS forwarders implemented in residential routers provide some benefits, such as allowing clients to configure settings like DNS filters, local DNS domains, and security protections like DNS rebinding protection.

1.3 What makes DNS forwarders vulnerable?

Vulnerabilities in DNS forwarders on residential routers are often caused by third-party software that has been integrated into the routers by manufacturers in an effort to offer multiple functionalities while keeping costs low. These implementations are cheap and prone to attack. Unfortunately, patching these vulnerabilities is not straightforward, as patches provided by the router manufacturers do not apply to third-party DNS software.

1.4 Architecture of DNS forwarding and lookup

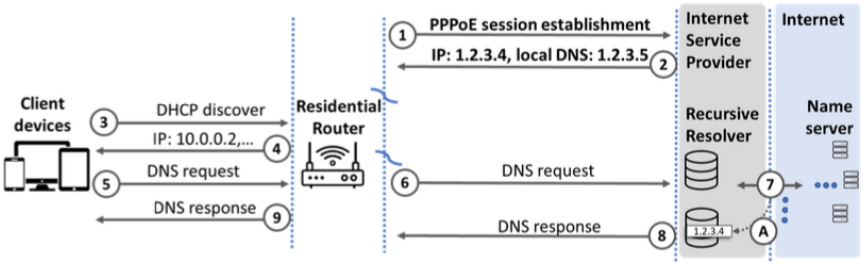

Fig. 1. DNS forwarding in routers

1.5 Removing DNS from routers

- The first approach involves manually configuring upstream resolvers on client devices. This method requires users to configure the IP address of the ISP's DNS resolver in the resolv.conf file on all client devices, which can be time-consuming and prone to error.
- The second approach offers a more systematic solution by implementing DNS forwarding as a NAT rule rather than a service on the router's operating system.
- The third approach involves using the IPv6 stateless-auto-configuration (SLAAC) mechanism via ICMPv6 router advertisements to communicate DNS server addresses to network hosts.

1.6 Performance Costs

The paper states that the only measurable performance impact of disabling DNS caching in routers was an increase of 1 round-trip time (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.

2 Assumptions

- It is assumed that DNS forwarders are not implemented by router developers but by third-party vendors and these third-party vendors provide cheap implementations for the sake of multiple functionalities.
  Critique1 - The DNS forwarders are not necessarily implemented by third-party vendors.
  Solution - These forwarders can be implemented by router manufacturers and developers with a firewall feature which mitigates the security risks of DNS forwarders.
- It is assumed that the updates to DNS forwarders implemented by third-party vendors are inconsistent and sub-standard patches.
  Critique2 - Following the above assumption, when the forwarders are in-house developed by the manufacturers, the updates are consistent, timely and follow the latest security guidelines for patches.

3 Technical Approach

- The router first establishes a session(typically PPPoE/DHCP) and gets the IP address of the recursive resolver of that ISP. The router then assigns an internal segment from the IP network address block to itself and the client receives the IP over DHCP. Typically, the client application initiates a DNS query to an operating system stub resolver. This stub resolver simply forwards the request to a DNS forwarder which also forwards this request to a recursive upstream resolver(of ISP). This resolver recursively iterates nameservers over the internet(typically from root to top-level domains etc). If the answer to the query is not already present in the recursive resolver, the router-dedicated DNS cache is then cached over all the layers and returned to the client.
  Critique3 - 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.

4 Results

The paper proposes a number of simple solutions for removing DNS components from the router.

4.1 Manually configure the upstream resolver

This solution suggests manually configuring the client system to directly send the query to ISP upstream resolver. This is done by configuring the resolve.conf to the IP address of the ISP. This allows us to bypass the DNS forwarder in the router.

Critique4:

- Since the addresses are manually configured on each client, it poses a synchronization problem in case the internet connection between the router-ISP is reset as the client has no way of knowing the change in address of the upstream resolver.
- Manual configuration is time-consuming and error-prone for non-technical users and is not scalable for larger networks.

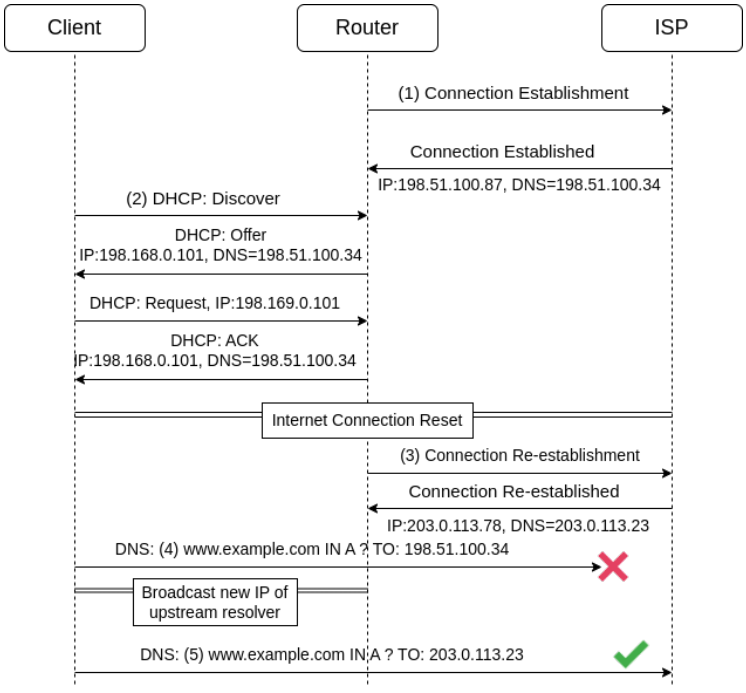

Fig. 2. Broadcasting IP of upstream resolver

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.

4.2 NAT rule to relay requests to upstream

The paper suggests implementing a DNS forwarder as a NAT(Network Address Translation) instead of a service running on router OS. The router then sends the request packets from clients to directly ISP's resolver by replacing their destination address with a firewall rule. Whenever the internet connection is reset, the firewall rule is changed to route DNS requests to the correct(if the IP of the upstream resolver was changed during reset) destination.
Critique5 - Network Address Translators(NAT) are not completely immune to attacks [4]. 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.

4.3 Communicate DNS servers to client devices

This solution suggests using IPv6(SLAAC) mechanism via ICMPv6 router advertisement to continuously broadcast the network configuration in the local network segment. This can be used to communicate changes in DNS resolver configuration to clients overcoming the synchronization issue.
Critique6 - The given solution is only applicable to clients using IPv6 addresses and cannot be implemented on routers using IPv4 addresses.

5 Analysis

The paper states that the ISP resolvers are anyways in close proximity to client networks and hence the latency is in milliseconds. So removing cache from routers has a negligible impact on performance. The records which are recently visited are also cached in the browser which includes the DNS cache. It is shown in **??** that the only performance penalty is 1 RTT measured between the local device and ISP resolver when the cache is removed from the router. DNS records have a time-to-live (TTL) value which specifies how long a DNS resolver can cache a record before it expires. Typically, TTL values for DNS records are set to a few minutes to ensure quick propagation of changes. When a client makes a DNS query, the resolver first checks its local cache for a matching record. If the record is not found or has expired, the resolver must perform a new query to recursively resolve the DNS record. However, a router's DNS cache can save loading time for a web page only if the record is not locally cached and has not yet expired in the router's cache. This means that the user has to load a page that they have not visited for at least the past 5 minutes and that has also been visited by another device on the same local network less than 5 minutes ago.

[3]While the paper is largely correct about the performance impact, in some cases such as for ISP-based resolvers as well as public resolvers, the resolver may not be in close proximity to the users.

6 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. We have 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