DNSOP
Internet-Draft
Intended status: Best Current Practice
Expires: 29 November 2025

L. Gong
CNIC
Z. Yan
M. Zhang
K. Dong
CNNIC
C. Long
CNIC

28 May 2025

Enhancing Local-Use Domain Name Resolution within Link-Local Scope
draft-gong-dnsop-enhancing-local-use-domain-00

Abstract

Link-local networks such as home Internet of Things (IoT) and industrial Internet of Things are becoming increasingly prosperous, with a large number of small devices deployed in the link-local networks. These devices discover each other through ".local." domain names of DNS-based zero-configuration network protocol. However, the lack of specialized security operations to supervise link-local DNS resolution leads to some security risks. This memo addresses the potential risks associated with the leakage of link-local DNS traffic to external networks, the lack of identity authentication on ".local." domain requests, and the lack of rate-limiting on ".local." domain responses, which poses the leakage of link-local device information and the risk of DDoS attacks. Furthermore, the document proposes a set of best practices and technical solutions to mitigate these risks and ensure that ".local." domain name resolution remains confined within the local network segment.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 November 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The link-local network is a small local area network, including printers, IoT devices, local storage, etc. Common link-local networks are home IoT, industrial IoT, etc, and have become the end network of the Internet. Small devices inside the link-local network often access the Internet through a gateway (WiFi, VPN gateway, etc) and utilize zero-configuration network protocols for mutual discovery in the link-local network. The ".local." domain name used by zero-configuration network protocol is multicast across the link-local network, allowing each device to obtain a list of currently available services.

The ".local." domain, as specified in RFC 6762([RFC6762]), is a special-use domain name reserved for local network communication without the need for a central DNS server. The ".local." domain containing server information is multicast to port 5353 on the link-local ipv4 address (224.0.0.251) or ipv6 address ([FF02::FB]). RFC

6763([RFC6763]) builds upon this foundation by providing a mechanism for service discovery using DNS records. Obviously, the ".local." domain name are used for link-local service discovery and management.

However, due to the lack of security operations for link-local networks, numerous ".local." domain names are wantonly multicast. Even, some gateways are set up to open port 5353, enabling the local devices to receive ".local." domain queries from the external networks. It can be found that improper handling of ".local." domains can lead to unintended traffic leakage and potential security vulnerabilities. In particular, an attacker can launch an inbound query to obtain multicast DNS traffic in response to the intranet for snooping on device information in the link-local network. Due to the lack of identity authentication on ".local." Domain request, the response packets can be reflected to any IP address. Besides, the rate on ".local." Domain response is not limited. As a result, an attacker can take advantage of above two shortcoming to launch the DoS attacks. In the real world, it is found that a large number of gateway devices with open port 5353, which holds huge security risk potential.

Aiming to maintain the integrity and security of link-local DNS resolution, this document propose some helpful guidance and solutions. Technically, the security content of the protocol needs to be supplemented. In terms of management, it is recommended to close unnecessary open port 5353 to avoid leaks of DNS traffic.

2. Problem Statement

2.1. Leakage of Local Traffic

Normally, ".local." domain queries are requested by link-local devices. However, due to the lack of source address verification, ".local." domain queries can be sent to link-local devices through the gateway with open port 5353 by external entities. When ".local." domain queries are not confined to the local link, sensitive local network information may be exposed to external entities, leading to privacy concerns and potential security breaches. In particular, an external entity can use the "_services._dns-sd._udp.local" to enumerate the link-local device services. Then the external entity can query some particular service’s PTR, SRV, and TXT records. Finally, the external entity could extract the address and port of the intranet service and use network attack methods to access the service.

According to our large-scale measurement and data analysis, we found that 898,517 unique IP addresses worldwide were running mDNS services with open port 5353 in the past year.

Moreover, we used the special wildcard query "_services._dns-sd._udp", which triggers the DNS-SD service to return all actual service types running on the network. This query is crucial because it allows us to gather comprehensive information about the services being advertised within the LAN. The mDNS server responds to this query by providing the relevant service type records, which gives the client a complete view of the available services. With this data, we summarized all discovered service types and found 598 types of services. Furthermore, we can explore the web login page using the query results. For example, we found a device with open port 5353 in Taipei. Then we tried to login a http web service in the local-link network.

2.2. Lack of Rate Limiting

Without rate-limiting mechanisms, external entities could send numerous service enumeration query to gateway and potentially flood the local network with DNS queries, leading to network congestion and potential denial-of-service (DoS) attacks in the link-local network. Besides, due to the lack of identity authentication, external entities can reflect the service enumeration response packets to any IP address. The more the number of intranet services, the more reflective amplification. We found the most number of intranet services is about 5. In the real-world, there are plenty of gateway devices with open port 5353. Once some attack takes advantage of these devices to flood the reflective DNS response to the target, the target’s bandwidth would be exhausted due to the DDoS attack.

3. Proposed Solutions

3.1. Enhanced Gateway and DNS Server Configuration

It is essential to properly configure network gateways so that they can identify and filter out traffic that is designated with the ".local." suffix. This specific measure ensures that such traffic remains confined within the local network and does not accidentally propagate to external networks beyond the intended boundaries. Moreover, it is imperative to set up Access Control Lists (ACLs) on Domain Name System (DNS) servers with meticulous care. These ACLs should be designed to allow and facilitate only local responses for any DNS queries that pertain to the ".local." domain. This practice is in full compliance with the guidelines and specifications outlined in RFC 6762, which addresses the use of multicast DNS and ensures that the local network operates smoothly without interference from external DNS services.

3.2. Technical Measures for Rate Limiting and Traffic Control

Introducing rate-limiting policies for mDNS is a crucial step in managing and regulating the volume and rate of responses for queries related to the ".local." domain. This approach aims to prevent abuse and mitigate potential denial-of-service attacks by imposing restrictions on how frequently and how rapidly DNS servers can respond to ".local." domain queries. By implementing these policies, network administrators can ensure a more stable and secure DNS environment, reducing the risk of overloading the servers and maintaining the integrity of the DNS service.

Furthermore, to enhance the security and reliability of mDNS operations, especially for ".local." domains, it is essential to employ robust authentication methods. These methods serve to verify the authenticity of DNS queries, ensuring that only legitimate and authorized requests are processed. By authenticating DNS queries, administrators can effectively prevent unauthorized access and potential spoofing attacks. This dual strategy of rate-limiting and authentication not only protects the DNS infrastructure but also upholds the trustworthiness and accuracy of the ".local." domain resolution process.

4. Security Considerations

Security enhancement, such as DNSSEC, would serve the purpose of addressing and mitigating the potential risks associated with the inadvertent leakage of sensitive information that could occur when employing the multicast DNS (mDNS) protocol. Additionally, it would aid in alleviating the dangers posed by Denial of Service (DoS) attacks that exploit vulnerabilities within local networks by leveraging queries made to the ".local." domain. By implementing these measures, we can ensure a more secure environment, safeguarding against both accidental data breaches and malicious activities that target local network infrastructures through the use of ".local." domain names.

5. IANA Considerations

This document does not require any actions from IANA.

6. Acknowledgment

This work is supported by the National Key Research and Development Program of China (No.2023YFB3105700).

7. Normative References

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

Authors' Addresses

LiangYi Gong
CNIC
No. 2 Dongsheng South Road, Haidian District
Beijing
Beijing, 100083
China
Email: lygong@cnic.cn

Zhiwei Yan
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing
Beijing, 100190
China
Email: yanzhiwei@cnnic.cn

Man Zhang
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing
Beijing, 100190
China
Email: zhangman@cnnic.cn

Kejun Dong
CNNIC
4 South 4th Street, Zhongguancun, Haidian District
Beijing
Beijing, 100190
China
Email: dongkejun@cnnic.cn

Chun Long
CNIC
No. 2 Dongsheng South Road, Haidian District
Beijing
Beijing, 100083
China
Email: longchun@cnic.cn