IPv6 Maintenance
Internet-Draft
Intended status: Standards Track
Expires: 29 August 2026

C. Ma
C. Xie
China Telecom

25 February 2026

# Updates to DNS64 Functionality Advertisement for DNS RA Option
## draft-ma-6man-ra-dns64-flag-01

## Abstract

This document defines a new flag in the DNS RA Option to advertise the DNS64 functionality. This extension enables automatic configuration of DNS64 resolution, improving deployability in IPv6 transition scenarios.

## 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 August 2026.

Table of Contents



## 1. Introduction

DNS Extensions for Network Address Translation from IPv6 clients to IPv4 servers (DNS64)[RFC6147] is a widely deployed mechanism for IPv6-only networks requiring access to IPv4-only services. [I-D.ma-v6ops-5g-ipv6only]introduce the reasons for using RA to deliver DNS64 address configuration. This document defines a new flag in the DNS RA option[RFC8106] to communicate DNS64 server address to hosts.

### 1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14[RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 2. Use Cases

This section describes the key use cases that motivate the introduction of a new IPv6 Router Advertisement option to explicitly signal the availability of DNS64-capable resolvers.

### 2.1. Use Case 1: Coexistence of IPv6-Only and Dual-Stack Users on the Same Network

Operators may wish to gradually migrate users from dual-stack to IPv6-only without relying on APN isolation or separate network slices. In such scenarios:

IPv6-only users require DNS64 to access IPv4-only content.

Dual-stack users should continue using standard DNS resolvers to avoid unnecessary translation and performance impact on NAT64 gateways.

If both user groups share the same network, the operator needs a mechanism to selectively provide DNS64 server addresses only to IPv6-only hosts. Using RDNSS to distribute DNS server addresses would apply to all users, potentially overloading NAT64 gateways with traffic from dual-stack hosts. The proposed option enables the network to explicitly indicate which resolvers are DNS64-capable, allowing hosts to make informed decisions.

### 2.2. Use Case 2:Phased Rollout of DNS64 Services

Operators often roll out new services gradually to manage risk and validate performance. For example:

Initially, only 10% of IPv6-only users are directed to DNS64 resolvers.

Over time, this percentage is increased until full deployment is achieved.

With RDNSS alone, all users receive the same DNS server addresses, making phased rollout difficult without complex per-user configuration or multiple network slices. The proposed option allows operators to control which hosts receive DNS64 resolver information based on network policies (e.g., by selectively sending Router Advertisements with or without the new option). This enables fine-grained, incremental deployment without requiring per-host configuration changes.

### 2.3. Use Case 3:Multiple DNS Server Tiers with Different Capabilities

In some deployments, operators operate multiple DNS server tiers:

Tier 1: Standard DNS resolvers (non-DNS64) for dual-stack and IPv4-only users.

Tier 2: DNS64-capable resolvers for IPv6-only users.

Both tiers may serve the same network prefix. Without explicit signaling, IPv6-only hosts cannot distinguish which resolvers support DNS64. They would need to either:

Probe each resolver (increasing signaling overhead and latency), or

Be statically configured (reducing operational flexibility).

The proposed option allows the network to explicitly advertise the DNS64 capability, enabling hosts to select the appropriate resolver without additional probing.

### 2.4. Use Case 4: Avoiding Dependency on Host-Side Synthesis

While host-side synthesis (e.g., using Pref64 options as defined in RFC 8781) is a valid approach, it requires host support and may not be available on all devices. In many real-world deployments:

Legacy or constrained devices may not support host-side synthesis.

Operators may prefer centralized translation for policy control, logging, or security reasons.

For such environments, DNS64 remains a necessary component. The proposed option enhances DNS64 deployments by giving operators better control over which hosts use DNS64, without requiring host-side modifications beyond initial implementation of the option.

### 2.5. Summary of Benefits

Need 1: Coexistence of IPv6-only and dual-stack users. Allows selective signaling of DNS64 resolvers to IPv6-only hosts.

Need 2: Phased rollout. Enables incremental deployment without per-host configuration.

Need 3: Multiple DNS server tiers. Lets hosts distinguish DNS64-capable resolvers from standard ones.

Need 4: Centralized translation control. Supports operators who prefer DNS64 over host-side synthesis.

## 3. Relationship with Existing Technologies

This section clarifies how the proposed DNS64 Router Advertisement option relates to existing mechanisms, emphasizing that it is intended as a complementary tool rather than a replacement for established solutions.

### 3.1. Relationship with Pref64 Option (RFC 8781)

The Pref64 option (RFC 8781) is used to advertise the IPv6 prefix used for DNS64-based address synthesis, enabling host-side synthesis. This approach allows IPv6-only hosts to synthesize IPv4-embedded addresses locally without involving a DNS64 server.

The proposed DNS64 option addresses a different problem: it signals which DNS servers are DNS64-capable, enabling hosts to select the appropriate resolver. The two options are complementary:

Pref64 option enables host-side synthesis.

DNS64 option enables network-side DNS64 selection.

Operators may choose to deploy:

Pref64 only (for hosts that support local synthesis),

DNS64 option only (for networks relying on centralized DNS64 translation), or

Both (for networks supporting a mix of host types and deployment strategies).

Neither option replaces the other; they serve different operational needs.

### 3.2. Relationship with RDNSS (RFC 8106)

RDNSS (Recursive DNS Server) is the standard mechanism for distributing DNS server addresses via Router Advertisements. However, RDNSS alone cannot indicate whether a DNS server supports DNS64 functionality. This limitation leads to the operational challenges described in the use cases:

IPv6-only hosts cannot distinguish DNS64-capable resolvers from standard ones.

Dual-stack hosts may unintentionally use DNS64 resolvers, increasing load on NAT64 gateways.

The proposed option extends RDNSS by adding capability signaling. It does not replace RDNSS; rather, it builds upon it to provide richer information to hosts. In implementations, the DNS64 option would typically be carried alongside RDNSS options in the same RA message.

### 3.3. Relationship with PDP Context / APN Isolation

PDP context or APN (Access Point Name) isolation is a mechanism used in mobile networks to separate users into different logical networks. Operators can assign:

IPv4-only PDP contexts,

Dual-stack PDP contexts, or

IPv6-only PDP contexts.

This approach works but has operational trade-offs:

Requires per-user configuration and management.

May increase operational complexity when introducing new service tiers.

Does not easily support per-user percentage-based rollout without complex provisioning systems.

The proposed option operates at the IP layer, not at the PDP context layer. It provides a finer-grained, more flexible mechanism that works within a single network slice or PDP context. Operators can combine both approaches:

Use PDP context for coarse-grained separation (e.g., IPv6-only users in a dedicated context).

Use the proposed option for fine-grained control within that context (e.g., gradually enabling DNS64 for a subset of IPv6-only users).

The option is not a replacement for PDP context isolation, but rather a complementary tool for operators seeking more flexible IPv6-only deployment strategies.

### 3.4. Relationship with Host-Side DNS64 Detection

Some have suggested that hosts could detect DNS64 capability by:

Probing DNS servers (e.g., by querying for AAAA records of known IPv4-only domains), or

Using well-known addresses or special-purpose domains.

While technically possible, these approaches have limitations:

Increased latency: Probing adds delay to DNS resolution.

Signaling overhead: Repeated probes consume network and server resources.

Uncertainty: Results may be ambiguous or change over time.

No network control: The operator cannot centrally control which hosts use DNS64.

The proposed option provides a deterministic, low-overhead, operator-controlled alternative. It does not prohibit hosts from using detection mechanisms; rather, it offers a more efficient and controllable method when network-side signaling is available.

## 4. DNS64 Flag

Based on [RFC8106], this specification introduces a 'T' flag bit allocated in the leftmost bit of the Reserved field to signal the presence of DNS64 server addresses in the option payload. Figure 1 shows the format of the DNS64 option.

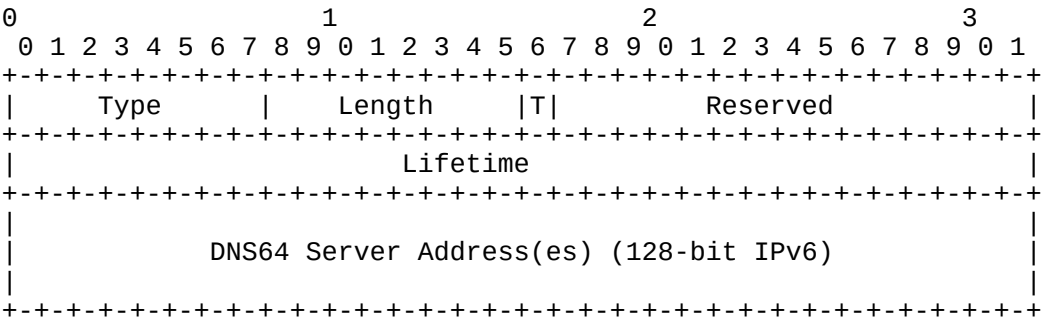


Figure 1:DNS64 RA Option format

Fields:

* Type: 8-bit identifier: 25

* Length: 8-bit unsigned integer.

* Flag T: 1-bit integer. set to indicate DNS64 server addresses are in the option payload.

* Lifetime: 32-bit unsigned integer.

* DNS64 Server Address(es): One or more 128-bit IPv6 addresses of the DNS64.

## 5. Security Considerations

This memo does not introduce any new security problems. Considerations are described in Section 7 in [RFC8106]

## 6. IANA Considerations

This document requests allocation for the Flag T.

## 7. Acknowledgements

Thanks to Lorenzo Colitti, Nick Buraglio, Jordi Palet, Jen Linkova, Philipp S. Tiesel,Ted Lemon for the discussions, the feedback, and all contribution.

## 8. References

### 8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

## 8.2. Informative References

[I-D.ma-v6ops-5g-ipv6only] Ma, C. and C. Xie, "Considerations of Gradual IPv6-only Deployment in 5G Mobile Networks", Work in Progress, Internet-Draft, draft-ma-v6ops-5g-ipv6only-01, 29 August 2025, <https://datatracker.ietf.org/doc/html/draft-ma-v6ops-5g-ipv6only-01>.

## Authors' Addresses

Chenhao Ma
China Telecom
Beiqijia Town, Changping District
Beijing
102209
China
Email: machh@chinatelecom.cn

Chongfeng Xie
China Telecom
Beiqijia Town, Changping District
Beijing
102209
China
Email: xiechf@cernet.edu.cn