v6ops Working Group C. Ma
Internet-Draft C. Xie
Intended status: Informational China Telecom
Expires: 3 September 2026 2 March 2026

Considerations of Gradual IPv6-only Deployment in 5G Mobile Networks
draft-ma-v6ops-5g-ipv6only-02

Abstract

This document describes the approach of gradually deploying 464XLAT based IPv6-only technology on user plane in 3GPP 5G networks. It also discusses the challenges and potential solutions.

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 3 September 2026.

Table of Contents

1. Introduction

Currently, IPv6 has been widely in mobile networks of operators worldwide, and it has even gained the dominant position from the perspective of traffic. However, IPv4 applications still exist in the network, and the support for IPv4 services must still be considered to guarantee the users' experience. Furthermore, operators have begun experimenting with deploying IPv6-only approach in their mobile networks.

The 5G system is defined in the 3GPP standards organization. In the 5G system architecture, the session related to the endpoint's access to the internet is called the Packet Data Unit (PDU) session, and its type determines the IP protocol used for user access. In the 5G standards, the PDU session supports both IPv6 and IPv4 protocols, and it also provides policies to ensure that user equipment (UE) can

access the internet. When a UE only supports the IPv4 protocol while the network supports dual-stack (IPv4 and IPv6), the network will provide an IPv4 protocol stack configuration for the UE. Accordingly, for UE only supporting IPv6,the network will provide an IPv6 protocol stack configuration for the UE. Additionally, there are policy configuration schemes related to static addresses and other aspects, but It does not specify the requirements related to IPv6-only technology.

There are several IPv6-only transition technologies described in [RFC9313] . Most existing deployments utilize 464XLAT technology in cellular network. This document describes the architecture for deploying 464XLAT based IPv6-only technology on user plane in 3GPP 5G system. Based on the field trail, this document also discusses the major issues encountered and potential solutions to address them.

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. Terms and abbreviation

The following terms are defined in this document:

* 464XLAT: IPv6-Only Transition Mechanism (IPv6-to-IPv4 Translation)
* 5GC: 5G Core
* 5GS: 5G System
* AMF: Access and Mobility Management Function
* CLAT: CLAT is customer-side translator (XLAT) that compiles with [RFC6146]
* PLAT: PLAT is provider-side translator (XLAT) that compiles with [RFC7915]
* PDU：Protocol Data Unit
* IMEI: International Mobile Equipment Identity
* SMF：Session Management Function

* UE: User Equipment, e.g., mobile phone.

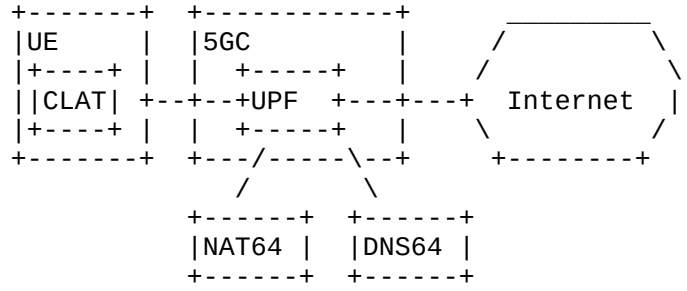
* LBO：Local Break Out

3. 5GS IPv6-only Architecture on User Plane

Examples of 5GS IPv6-only architectures on user plane are shown in the figures in the following sections. In production 5GS network, there is roaming behavior which specifies where the PDU session anchor and its controlling SMF are located in. That decides whether UE’s PDU sessions get IP configuration and access the Internet from home 5GS network or visited 5GS network. Regarding roaming, 5GS contains three scenarios including non-roaming, roaming with home routed, and roaming with local break out.

3.1. Non-roaming Network Scenario

Based on wireless 3GPP network architecture defined in [RFC6877], the non-roaming network architecture is depicted as figure 1. When a mobile network operator run only a 5GC, there is just non-roaming network scenario. In this csae, the CLAT function is deployed on the UE, while the PLAT/stateful NAT64 function and DNS64 function are deployed on the network side.



3.2. Roaming Network Scenario with Home Routed

Generally, large mobile operators run multiple 5GCs divided by administrative divisions or other geographical methods. The roaming network scenario with home routed is shown in figure 2. In this case, UEs acquire IP network configuration and access the Internet in their home 5GS network. The IP address allocation strategy and traffic exit interface are decided by their home 5GC. The CLAT function is deployed on the UE, while the PLAT/stateful NAT64 function and DNS64 function are deployed on the home network.

3.3. Roaming Network Scenario with Local Break Out

The roaming network scenario with LBO is shown in figure 3. In this case, UEs get IP network configuration and access the Internet in the visited network. The CLAT function is deployed on the UE, while the PLAT/stateful NAT64 function and DNS64 function are deployed on the visited network. Home network also need to support NAT64 and DNS64 when UE is in the non-roaming case.

The following table 1 summarizes 5GC's network capabilities where the mobile network shall have to provide IPv6-only connectivity service.

Scenario	UE	Home Network	Visited Network
Non-roaming	CLAT	NAT64 DNS64	
Roaming with Local Breakout	CLAT	NAT64 DNS64	NAT64 DNS64
Roaming with Home Routed	CLAT	NAT64 DNS64	

Table 1. Network Capabilities for IPv6-only 5G Scenarios

4. Deployment Challenges

Based on our practices, for large-size mobile network operators, it's very difficult for operators to deploy IPv6-only capabilities across the whole network at once. There is a transition period that the IPv6-only capability is deployed gradually. This section identifies the major challenges when applying 464XLAT in a production network.

4.1. Roaming Challenge

In the scenario where 5GC A supports IPv6-only capability while 5GC B doesn't. When UE A from 5GC A roams to 5GC B, it only obtains IPv6 configuration and accesses Internet according to the local breakout roaming policy. In this case, the access to IPv4 Internet may fail due to 5GC B lacks NAT64 and DNS64 capabilities.

4.2. UE Challenge

Regarding UE challenge, a significant number of terminals have not enabled CLAT functionality. The vast majority of Android terminals support and have enabled the CLAT functionality. Most new terminals like smart watch do not support this feature. Moreover, Apple's iOS in China does not enable CLAT functionality.

4.3. UP Layer Challenge

When IPv6-only users access IPv4 sites, the actual address they reach is generated by the DNS64 server, which combines a special IPv6 prefix with the IPv4 site address to form an IPv6 address. Existing layer 3&layer 4 content billing rules based on IPv4 addresses will no longer be effective and will need to be adjusted to accommodate the IPv6 addresses formed by DNS64.

4.4. DNS64 Configuration Challenge

After enabling the DNS64 functionality, there is an increase in the processing load due to the additional handling of IPv6 queries and the DNS64 conversion, which consumes some device performance. The extent of this performance demand increase depends on the scale of IPv6 queries. In a 5G network, once the DNS64 functionality is enabled, DNS resolution requests from both IPv6-only and dual-stack users will be processed by the DNS64 server. Even IPv4 resolution requests from dual-stack users will be treated as if they were from IPv6-only users, which place a significant load pressure on the DNS server. This may futher impact the service logic of the existing dual-stack users.

5. Deployment Solutions

5.1. PDP Context / APN Isolation Method

In 3GPP mobile networks, the PDP context (in GPRS/UMTS) or PDN connection (in LTE/5G) represents a logical association between a User Equipment (UE) and a packet data network. Each context is associated with a specific APN or DNN (in 5G), which identifies the external network (e.g., the Internet, a corporate intranet, or an operator’s walled garden) and determines the services and policies applied to that connection. Operators can leverage this architecture to separate users into different logical networks based on their service requirements, including IPv6 capabilities and DNS64 needs.

An operator can configure multiple APNs with distinct characteristics:

APN Type	IP Capabilities	DNS Configuration	Target Users
APN-A	Dual-stack	Standard DNS resolvers	Legacy dual-stack users
APN-B	IPv6-only	DNS64-capable resolvers	IPv6-only early adopters
APN-C	IPv4-only	Standard DNS resolvers	Legacy IPv4-only devices

When a UE attaches to the network, it requests a PDP context for a specific APN. The network can:

Assign users to different APNs based on subscription data (e.g., user profile in HLR/HSS).

Dynamically steer users to different APNs based on device capabilities (e.g., whether the UE supports IPv6-only operation).

Use policy control to selectively enable DNS64 for certain user groups.

Each PDP context can have its own DNS server addresses assigned via:

PCO (Protocol Configuration Options) during context activation.

DHCPv6 or Router Advertisement (for IPv6) within the context.

Stateless address autoconfiguration with RDNSS options.

For IPv6-only contexts, the operator can configure DNS64-capable resolvers; for dual-stack contexts, standard resolvers are used.

In a typical IPv6-only rollout using APN isolation, an operator initially provisions a small pilot group with a dedicated "ipv6only.apn," where their PDP contexts receive IPv6-only addresses and DNS64 resolver addresses via Protocol Configuration Options (PCO). Subsequently, the operator expands deployment by updating subscription profiles to move more users to this IPv6-only APN. Eventually, the IPv6-only APN becomes the default for all new subscriptions, while legacy APNs are retained for backward compatibility. Throughout this phased approach, dual-stack users connected to standard APNs continue using conventional DNS resolvers and never utilize the DNS64 infrastructure, ensuring clean separation between user groups and preventing unnecessary load on NAT64 gateways.

PDP context and APN isolation provide strong separation between different user groups at the bearer level, ensuring that dual-stack users never unintentionally utilize DNS64 resolvers and overload NAT64 gateways. This approach offers operators fine-grained control over which users receive IPv6-only service based on subscription data, device capabilities, or other policy criteria, while maintaining full backward compatibility for legacy devices that continue operating on existing APNs without any modification. Furthermore, User Equipment behaves normally by simply requesting an APN and receiving the appropriate configuration, as this method leverages proven, mature technology that is widely deployed and well understood by mobile operators worldwide, making it a reliable foundation for managing IPv6-only deployments in 3GPP networks.

Despite its strengths, PDP context and APN isolation introduce significant operational complexity, as managing multiple APNs increases the burden on provisioning, billing, and subscription management systems, particularly when moving users between APNs requires updates to individual subscriber profiles that may not be practical for large-scale or dynamic changes. The approach operates at the bearer level rather than the IP flow level, limiting its granularity and making it incapable of supporting percentage-based rollout strategies within a single user group without resorting to complex multi-APN configurations. Additionally, some User Equipment may cache APN information or exhibit unpredictable behavior when multiple APNs are available, and crucially, this method is specific to 3GPP mobile networks and does not apply to fixed broadband or enterprise environments, leaving a gap that must be addressed by complementary solutions.

5.2. IMEI Configuration at Network Side

One solution is to enhance the core network’s capability to configure IP addresses and DNS server addresses based on IMEI number ranges. The IMEI is a unique sequence of 14 to 15 digits assigned to each mobile phone. It serves as a device identification number, enabling service providers to recognize the phone within the network. The primary purpose of the IMEI is to uniquely identify each device, allowing the network to determine whether the UE supports CLAT functionality. By configuring a whitelist of IMEIs that support CLAT functionality in the network, the network can assign an IPv6-only environment to UEs listed in the whitelist.

5.3. Option 108

One possible solution is to use the option108 [RFC 8925] [RFC8925]method, allowing UEs to choose whether to join the IPv6-only network. Additionally, a method for configuring DNS64 server addresses needs to be considered. However, in practical deployments, core network support for DHCPv4 functionality is optional and may not be applicable to all networks.

5.4. Using RA to deliver PREF64 and DNS64 configuration

Another possible solution is to transmit PREF64 and DNS64 address information through the RA option. In 5G systems, RA is used to advertise IPv6 prefixes in SLAAC, which is a mandatory functionality. Transmitting this information through RA is also a logical approach. Currently, the IETF has produced two RFCs, namely [RFC 8106][RFC8106] and [RFC 8781][RFC8781]. In practical implementations, the mobile core network supporting IPv6-only environments (IPv6-only mode) should include these two options in the RA messages. Upon receiving

this message, the UE can abandon the IPv4 interface and operate in IPv6-only mode. In this solution, the core network does not need to be aware of the final protocol stack configuration used by the UE.

6. PREF64 and DNS64 Configuration via Router Advertisement Options

This section specifies a method for advertising PREF64 (NAT64 prefix) and DNS64 configuration to hosts by combining PREF64 RA Option and DNS64 RA Option.

6.1. Option Overview

The mechanism relies on the presence of two distinct Router Advertisement options:

1. PREF64 Option: Carries the IPv6 prefix used by the network's NAT64 gateway for IPv4/IPv6 protocol translation. The format, semantics, and processing rules for this option are defined in [RFC8781].

2. DNS64 Option: Carries the IPv6 address(es) of DNS64 servers capable of synthesizing AAAA records from A records. The format and semantics of this option are defined in RFC 8781[RFC8781] and [I-D.ma-6man-ra-dns64-flag].

A router (e.g., a 5G User Plane Function (UPF), a broadband gateway, or a network router) MUST include both options in its Router Advertisements to fully enable IPv6-only with NAT64/DNS64 functionality on the link.

6.2. Host Behavior

Upon receiving a Router Advertisement message containing both a valid PREF64 Option and a valid DNS64 Option, a host supporting this specification SHOULD:

1. Process the PREF64 Option. This involves:

Extracting the NAT64 prefix and its length.

Calculating the validity of the prefix.

Installing the prefix in its local policy table to be used for detecting synthesized IPv6 addresses.

2. Process the DNS64 Option as follows:

Extract the DNS64 server addresses and their Lifetime. Add these addresses to its list of available recursive DNS resolvers, marking them with a special attribute indicating DNS64 capability.

Prefer DNS64 servers for resolution. The host MAY prioritize these DNS64 servers over other configured DNS servers (e.g., those learned via DHCPv6 or the RDNSS option) to ensure synthesis occurs.

3. Resolution and Communication:

When an application requires name resolution, the host queries the DNS64 server for a AAAA record.

If the DNS64 server returns a synthetic AAAA record (constructed by embedding the IPv4 address from the authoritative A record into the advertised PREF64 prefix), the host will initiate communication using this IPv6 address.

Traffic destined for this synthesized IPv6 address will be routed to the network’s NAT64 gateway, which will perform the necessary protocol translation to reach the target IPv4-only server.

A host MAY use heuristics to discover a NAT64 prefix if only the DNS64 Option is present, as defined in RFC 7050. However, the explicit signaling via the PREF64 Option is the preferred and more reliable method.

6.3. Router Behavior

A router configured to support IPv6-only with NAT64 MUST:

1. Generate periodic and solicited Router Advertisements that include both the PREF64 Option and the DNS64 Option.

2. PREF64 Option Configuration: Populate the PREF64 Option with the correct prefix, prefix length, and lifetime as per network policy and RFC 8781.

3. DNS64 Option Configuration: Populate the DNS64 Option with the IPv6 address(es) of the network’s DNS64 servers and a valid Lifetime.

4. Ensure the lifetime values for both options are aligned to provide a consistent user experience. It is generally advisable to set similar lifetimes for both the NAT64 prefix and the DNS64 servers.

6.4. Backward Compatibility and Coexistence

Hosts that do not support the DNS64 Option will ignore it as specified in RFC 4861. They may rely on other methods (e.g., DHCPv6, RDNSS) to discover DNS servers, but may not achieve full IPv6-only functionality without manual configuration.

This method coexists with the DHCPv6-based method for conveying DNS64 server information. If a host receives both, the source of truth is implementation-specific. It is RECOMMENDED that network administrators ensure consistent configuration across all discovery mechanisms.

The DNS64 Option is distinct from the RDNSS Option (RFC 8106). A router MAY include both an RDNSS Option (pointing to standard DNS servers) and a DNS64 Option (pointing to DNS64 servers). A host that understands the DNS64 Option can then distinguish between servers that perform synthesis and those that do not.

6.5. Deployment Scenarios

This section describes the operational contexts in which the proposed DNS64 Router Advertisement option provides tangible benefits, and clarifies its relationship with existing transition technologies.

1. Coexistence of IPv6-Only and Dual-Stack Users

Many operators are migrating towards IPv6-only access networks while still supporting a large base of dual-stack subscribers. In such a mixed environment, IPv6-only hosts require DNS64 to reach IPv4-only content, whereas dual-stack hosts should continue to use standard (non-DNS64) resolvers to avoid unnecessary load on NAT64 gateways. However, when DNS server addresses are advertised via RDNSS (RFC 8106), all hosts receive the same set of resolvers. Without additional signaling, IPv6-only hosts cannot distinguish which resolvers are DNS64-capable, and dual-stack hosts may inadvertently send queries to a DNS64 server, increasing the traffic that must be translated by the NAT64 device.

2. Phased Rollout of DNS64 Services

Operators often introduce new services incrementally to manage risk and validate performance. For example, an operator may wish to start by directing 10% of its IPv6-only subscribers to a DNS64 resolver and gradually increase that percentage over time. Using RDNSS alone, such a phased rollout would require either complex per-user provisioning (e.g., separate network slices or PDP contexts) or network-wide changes that affect all users simultaneously. The

proposed option can be selectively included in Router Advertisements sent to a subset of hosts, enabling fine-grained, percentage-based deployment without per-host configuration changes. As the rollout progresses, the option can be enabled for more prefixes or more RA instances until full coverage is achieved.

3. Multiple DNS Server Tiers with Different Capabilities

In some networks, operators operate multiple tiers of recursive resolvers. For instance, a set of high-performance resolvers may be dedicated to standard (non-DNS64) queries, while a separate set of resolvers (perhaps with more logging or policy enforcement) are configured to perform DNS64 synthesis. Both sets may share the same IPv6 prefixes, making it impossible for a host to know which resolvers offer DNS64 solely from the addresses themselves. The proposed option provides an explicit signal that a given resolver supports DNS64, enabling hosts to make an informed choice without resorting to probe queries (which add latency and overhead) or static configuration (which reduces flexibility).

4. Networks That Prefer Centralized Translation

While host-side synthesis (e.g., using the Pref64 option defined in RFC 8781) is a powerful tool, it requires host support and may not be available on all devices. Moreover, some operators prefer to keep translation logic centralized for reasons of policy control, logging, security, or ease of troubleshooting. For such environments, DNS64 remains a necessary component of the IPv6-only transition toolkit. The proposed option enhances these deployments by giving operators control over which hosts receive DNS64 resolver information, thereby avoiding the overloading of NAT64 gateways and enabling gradual migration strategies.

7. Security Considerations

To implement PREF64 RA Options, see the security sonsiderations presented in Section 7 of [RFC8781]

To implement DNS64 RA Options, see the security sonsiderations presented in Section 7 of [RFC8106]

8. IANA Considerations

This document doesn’t introduce any IANA considerations.

9. Acknowledgements

The comments and suggestions of the following are gratefully acknowledged: Lorenzo Colitti, Jordi Palet.

10. Normative References

[I-D.ma-6man-ra-dns64-flag]
Ma, C. and C. Xie, "Updates to DNS64 Functionality Advertisement for DNS RA Option", Work in Progress, Internet-Draft, draft-ma-6man-ra-dns64-flag-01, 24 February 2026, <https://datatracker.ietf.org/doc/html/draft-ma-6man-ra-dns64-flag-01>.

[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>.

[RFC3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, DOI 10.17487/RFC3587, August 2003, <https://www.rfc-editor.org/info/rfc3587>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <https://www.rfc-editor.org/info/rfc6877>.

[RFC7915] Bao, C., Li, X., Baker, F., Anderson, T., and F. Gont, "IP/ICMP Translation Algorithm", RFC 7915, DOI 10.17487/RFC7915, June 2016, <https://www.rfc-editor.org/info/rfc7915>.

[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>.

[RFC8781] Colitti, L. and J. Linkova, "Discovering PREF64 in Router Advertisements", RFC 8781, DOI 10.17487/RFC8781, April 2020, <https://www.rfc-editor.org/info/rfc8781>.

[RFC8925] Colitti, L., Linkova, J., Richardson, M., and T. Mrugalski, "IPv6-Only Preferred Option for DHCPv4", RFC 8925, DOI 10.17487/RFC8925, October 2020, <https://www.rfc-editor.org/info/rfc8925>.

[RFC9313] Lencse, G., Palet Martinez, J., Howard, L., Patterson, R., and I. Farrer, "Pros and Cons of IPv6 Transition Technologies for IPv4-as-a-Service (IPv4aaS)", RFC 9313, DOI 10.17487/RFC9313, October 2022, <https://www.rfc-editor.org/info/rfc9313>.

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@chinatelecom.cn