RFC 8983
Internet Key Exchange Protocol Version 2 (IKEv2)
Notification Status Types for IPv4/IPv6 Coexistence

Abstract
This document specifies new Internet Key Exchange Protocol Version 2 (IKEv2) notification status types to better manage IPv4 and IPv6 coexistence by allowing the responder to signal to the initiator which address families are allowed.

This document updates RFC 7296.

Status of This Memo
This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8983.

Copyright Notice
Copyright (c) 2021 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

# Table of Contents

1. Introduction
2. Terminology
3. Why Not INTERNAL_ADDRESS_FAILURE?
4. IP6_ALLOWED and IP4_ALLOWED Status Types
5. Update to RFC 7296
6. Security Considerations
7. IANA Considerations
8. References
   8.1. Normative References
   8.2. Informative References

Acknowledgements
Author’s Address

## 1. Introduction

As described in [RFC7849], if the subscription data or network configuration allows only one IP address family (IPv4 or IPv6), the cellular host must not request a second PDP-Context (Section 3.2 of [RFC6459]) to the same Access Point Name (APN) for the other IP address family (AF). The Third Generation Partnership Project (3GPP) network informs the cellular host about allowed Packet Data Protocol (PDP) types by means of Session Management (SM) cause codes. In particular, the following cause codes can be returned:

- cause #50 "PDP type IPv4 only allowed": This cause code is used by the network to indicate that only PDP type IPv4 is allowed for the requested Public Data Network (PDN) connectivity.
- cause #51 "PDP type IPv6 only allowed": This cause code is used by the network to indicate that only PDP type IPv6 is allowed for the requested PDN connectivity.
- cause #52 "single address bearers only allowed": This cause code is used by the network to indicate that the requested PDN connectivity is accepted with the restriction that only single IP version bearers are allowed.
If the requested IPv4v6 PDP-Context is not supported by the network but IPv4 and IPv6 PDP types are allowed, then the cellular host will be configured with an IPv4 address or an IPv6 prefix by the network. It must initiate another PDP-Context activation of the other address family in addition to the one already activated for a given APN. The purpose of initiating a second PDP-Context is to achieve dual-stack connectivity (that is, IPv4 and IPv6 connectivity) by means of two PDP-Contexts.

When the User Equipment (UE) attaches to the 3GPP network using a non-3GPP access network (e.g., Wireless Local Area Network (WLAN)), there are no equivalent IKEv2 capabilities [RFC7296] notification codes for the 3GPP network to inform the UE why an IP address family is not assigned or whether that UE should retry with another address family.

This document fills that void by introducing new IKEv2 notification status types for the sake of deterministic UE behaviors (Section 4).

These notification status types are not specific to 3GPP architectures but can be used in other deployment contexts. Cellular networks are provided as an illustration example.

2. Terminology

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.

This document makes use of the terms defined in [RFC7296]. In particular, readers should be familiar with "initiator" and "responder" terms used in that document.

3. Why Not INTERNAL_ADDRESS_FAILURE?

The following address assignment failures may be encountered when an initiator requests assignment of IP addresses/prefixes:

- An initiator asks for IPvx, but IPvx address assignment is not supported by the responder.
- An initiator requests both IPv4 and IPv6 addresses, but only IPv4 address assignment is supported by the responder.
- An initiator requests both IPv4 and IPv6 addresses, but only IPv6 prefix assignment is supported by the responder.
- An initiator asks for both IPv4 and IPv6 addresses, but only one address family can be assigned by the responder for policy reasons.

Section 3.15.4 of [RFC7296] defines a generic notification error type (INTERNAL_ADDRESS_FAILURE) that is related to a failure to handle an address assignment request. The responder sends INTERNAL_ADDRESS_FAILURE only if no addresses can be assigned. This behavior does not explicitly allow an initiator to determine why a given address
family is not assigned, nor whether it should try using another address family. INTERNAL_ADDRESS_FAILURE is a catch-all error type when an address-related issue is encountered by an IKEv2 responder.

INTERNAL_ADDRESS_FAILURE does not provide sufficient hints to the IKEv2 initiator to adjust its behavior.

4. IP6_ALLOWED and IP4_ALLOWED Status Types

IP6_ALLOWED and IP4_ALLOWED notification status types (see Section 7) are defined to inform the initiator about the responder’s address family assignment support capabilities and to report to the initiator the reason why an address assignment failed. These notification status types are used by the initiator to adjust its behavior accordingly (Section 5).

No data is associated with these notifications.

5. Update to RFC 7296

If the initiator is dual stack (i.e., supports both IPv4 and IPv6), it MUST include configuration attributes for both address families in its configuration request (absent explicit policy/configuration otherwise). More details about IPv4 and IPv6 configuration attributes are provided in Section 3.15 of [RFC7296]. These attributes are used to infer the requested/assigned AFs listed in Table 1.

The responder MUST include the IP6_ALLOWED and/or IP4_ALLOWED notification status type in a response to an address assignment request as indicated in Table 1.

<table>
<thead>
<tr>
<th>Requested AF(s) (Initiator)</th>
<th>Supported AF(s) (Responder)</th>
<th>Assigned AF(s) (Responder)</th>
<th>Returned Notification Status Type(s) (Responder)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv6</td>
<td>None</td>
<td>IP6_ALLOWED</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4</td>
<td>IP4_ALLOWED</td>
</tr>
<tr>
<td>IPv4</td>
<td>IPv4 and IPv6</td>
<td>IPv4</td>
<td>IP4_ALLOWED, IP6_ALLOWED</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>IP6_ALLOWED</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4</td>
<td>None</td>
<td>IP4_ALLOWED</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv6</td>
<td>IP4_ALLOWED, IP6_ALLOWED</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4</td>
<td>IPv4</td>
<td>IP4_ALLOWED</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
<td>IP6_ALLOWED</td>
</tr>
</tbody>
</table>
If the initiator only receives one single IP4_ALLOWED or IP6_ALLOWED notification from the responder, the initiator **MUST NOT** send a subsequent request for an alternate address family not supported by the responder.

If a dual-stack initiator requests only an IPv6 prefix (or an IPv4 address) but only receives an IP4_ALLOWED (or IP6_ALLOWED) notification status type from the responder, the initiator **MUST** send a request for IPv4 address(es) (or IPv6 prefix(es)).

If a dual-stack initiator requests both an IPv6 prefix and an IPv4 address but receives an IPv6 prefix (or an IPv4 address) only with both IP4_ALLOWED and IP6_ALLOWED notification status types from the responder, the initiator **MAY** send a request for the other AF (i.e., IPv4 address (or IPv6 prefix)). In such case, the initiator **MUST** create a new IKE Security Association (SA) and request another address family using the new IKE SA.

For other address-related error cases that have not been covered by the aforementioned notification status types, the responder/initiator **MUST** follow the procedure defined in Section 3.15.4 of [RFC7296].

### 6. Security Considerations

Since the IPv4/IPv6 capabilities of a node are readily determined from the traffic it generates, this document does not introduce any new security considerations compared to the ones described in [RFC7296], which continue to apply.

### 7. IANA Considerations

IANA has updated the "IKEv2 Notify Message Types - Status Types" registry (available at <https://www.iana.org/assignments/ikev2-parameters/>) with the following status types:

<table>
<thead>
<tr>
<th>Value</th>
<th>NOTIFY MESSAGES - STATUS TYPES</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>16439</td>
<td>IP4_ALLOWED</td>
<td>RFC 8983</td>
</tr>
</tbody>
</table>

---

Table 1: Returned Notification Status Types

- If the responder receives only one IP4_ALLOWED or IP6_ALLOWED notification from the initiator, the responder **MUST** return the IP4_ALLOWED or IP6_ALLOWED notification status type.
- If the responder receives both IP4_ALLOWED and IP6_ALLOWED notification status types from the initiator, the responder **MUST** return both notification status types.
- If the responder receives neither IP4_ALLOWED nor IP6_ALLOWED notification status types from the initiator, the responder **MUST** return neither notification status type.

---

Table: Returned Notification Status Types

<table>
<thead>
<tr>
<th>Requested AF(s) (Initiator)</th>
<th>Supported AF(s) (Responder)</th>
<th>Assigned AF(s) (Responder)</th>
<th>Returned Notification Status Type(s) (Responder)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IP4_ALLOWED, IP6_ALLOWED</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 or IPv6 (policy based)</td>
<td>IPv4 or IPv6</td>
<td>IP4_ALLOWED, IP6_ALLOWED</td>
</tr>
</tbody>
</table>

---
8. References

8.1. Normative References


8.2. Informative References


Acknowledgements

Many thanks to Christian Jacquenet for the review.

Thanks to Paul Wouters, Yaov Nir, Valery Smyslov, Daniel Migault, Tero Kivinen, and Michael Richardson for the comments and review.

Thanks to Benjamin Kaduk for the AD review.

Thanks to Murray Kucherawy, Éric Vyncke, and Robert Wilton for the IESG review.

<table>
<thead>
<tr>
<th>Value</th>
<th>NOTIFY MESSAGES - STATUS TYPES</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>16440</td>
<td>IP6_ALLOWED</td>
<td>RFC 8983</td>
</tr>
</tbody>
</table>

Table 2: Updates to "IKEv2 Notify Message Types - Status Types" Registry
Author's Address

Mohamed Boucadair
Orange
35000 Rennes
France
Email: mohamed.boucadair@orange.com