Internet Engineering Task Force (IETF)
Request for Comments: 8925
Updates: 2563
Category: Standards Track
ISSN: 2070-1721

L. Colitti
J. Linkova
Google
M. Richardson
Sandelman
T. Mrugalski
ISC

October 2020

IPv6-Only Preferred Option for DHCPv4

Abstract

This document specifies a DHCPv4 option to indicate that a host supports an IPv6-only mode and is willing to forgo obtaining an IPv4 address if the network provides IPv6 connectivity. It also updates RFC 2563 to specify DHCPv4 server behavior when the server receives a DHCPDISCOVER not containing the Auto-Configure option but containing the new option defined in this document.

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/rfc8925.

Table of Contents

1. Introduction

One of the biggest challenges of deploying IPv6-only LANs is that such networks might contain a rather heterogeneous collection of hosts. While some hosts are capable of operating in IPv6-only mode (either because the OS and all applications are IPv6-only capable or because the host has some form of 464XLAT [RFC6877] deployed), others might still have IPv4 dependencies and need IPv4 addresses to operate properly. To incrementally roll out IPv6-only, network operators might need to provide IPv4 on demand, whereby a host receives an IPv4 address if it needs it, while IPv6-only-capable hosts (such as modern mobile devices) are not allocated IPv4 addresses. Traditionally, that goal is achieved by placing IPv6-only-capable devices in a dedicated IPv6-only network segment or Wi-Fi Service Set Identifier (SSID), while dual-stack devices reside in another network with IPv4 and DHCPv4 enabled. However, such an approach has a number of drawbacks, including, but not limited to, the following:

* Doubling the number of network segments leads to operational complexity and impact on performance -- for instance, due to high memory utilization caused by an increased number of Access Control List (ACL) entries.

* Placing a host in the correct network segment is problematic. For example, in the case of 802.11 Wi-Fi, the user might select the wrong SSID. In the case of wired 802.1x authentication, the authentication server might not have all the information required to make the correct decision and choose between an IPv6-only VLAN and a dual-stack VLAN.

It would be beneficial for IPv6 deployment if operators could implement IPv6-mostly (or IPv4-on-demand) segments where IPv6-only hosts coexist with legacy dual-stack devices. The trivial solution of disabling the IPv4 stack on IPv6-only-capable hosts is not feasible, as those clients must be able to operate on IPv4-only networks as well. While IPv6-only-capable devices might use a heuristic approach to learning if the network provides IPv6-only functionality and stop using IPv4 if it does, such an approach might be undesirable in practice. One important reason is that when a host connects to a network, it does not know whether the network is IPv4-only, dual-stack, or IPv6-only. To ensure that connectivity

over whatever protocol is present becomes available as soon as possible, the host usually starts configuring both IPv4 and IPv6 immediately. If hosts were to delay requesting IPv4 until IPv6 reachability is confirmed, that would penalize IPv4-only and dual-stack networks, which does not seem practical. Requesting IPv4 and then releasing it later, after IPv6 reachability is confirmed, might cause errors that are visible to users, as it would be disruptive for applications that have already started using the assigned IPv4 address. Instead, it would be useful to have a mechanism that would allow a host to indicate that its request for an IPv4 address is optional and a network to signal that IPv6-only functionality (such as NAT64 [RFC6146]) is available. This document provides such a solution via a new DHCPv4 option that a client uses to indicate that it does not need an IPv4 address if the network provides IPv6-only connectivity (as NAT64 and DNS64). If the particular network segment provides IPv4 on demand, such clients would not be supplied with IPv4 addresses, while IPv4 addresses would be provided on IPv4-only or dual-stack segments without NAT64 services.

[RFC2563] introduced the Auto-Configure DHCPv4 option and describes DHCPv4 server behavior if no address is chosen for a host. This document updates [RFC2563] to modify server behavior if the DHCPOFFER contains the IPv6-Only Preferred option.

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.

1.2. Terminology

Dual-stack network or device: A network or device that has both versions of the Internet Protocol (IPv4 and IPv6) enabled and operational.

IPv6-only-capable host: A host that does not require an IPv4 address and can operate on IPv6-only networks. More precisely, IPv6-only capability is specific to a given interface of the host: if some applications on a host require IPv4 and the 464XLAT CLAT (customer-side translator) [RFC6877] is only enabled on one interface, the host is IPv6-only capable if connected to a NAT64 network via that interface. This document implies that IPv6-only-capable hosts reach IPv4-only destinations via a NAT64 service provided by the network. Section 4 discusses hypothetical scenarios for other transition technologies being used.

IPv4-requiring host: A host that is not IPv6-only capable and cannot operate in an IPv6-only network providing NAT64 service.

IPv4 on demand: A deployment scenario where end hosts are expected to operate in IPv6-only mode by default and IPv4 addresses can be assigned to some hosts if those hosts explicitly opt in to receive IPv4 addresses.

IPv6-mostly network: A network that provides NAT64 (possibly with DNS64) service as well as IPv4 connectivity and allows the coexistence of IPv6-only, dual-stack, and IPv4-only hosts on the same segment. Such a deployment scenario allows operators to incrementally turn off IPv4 on end hosts, while still providing IPv4 to devices that require IPv4 to operate. But IPv6-only-capable devices need not be assigned IPv4 addresses.

IPv6-only mode: A mode of operation where a host acts as an IPv6-only-capable host and does not have IPv4 addresses assigned (except that IPv4 link-local addresses [RFC3927] may have been configured).

IPv6-only network: A network that does not provide routing functionality for IPv4 packets. Such networks may or may not allow intra-LAN IPv4 connectivity. An IPv6-only network usually provides access to IPv4-only resources via NAT64 [RFC6146].

NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers [RFC6146].

Router Advertisement (RA): A message used by IPv6 routers to advertise their presence, together with various link and Internet parameters [RFC4861].

DNS64: A mechanism for synthesizing AAAA records from A records [RFC6147].

Network attachment event: A link up event, as described by [RFC4957], that results in a host detecting an available network.

Disabling the IPv4 stack on the host interface: Host behavior when the host

* does not send any IPv4 packets from that interface,

* drops all IPv4 packets received on that interface, and

* does not forward any IPv4 packets to that interface.

2. Reasons to Signal IPv6-Only Support in DHCPv4 Packets

For networks that contain a mix of both IPv6-only-capable hosts and IPv4-requiring hosts and that utilize DHCPv4 for configuring the IPv4 network stack on hosts, it seems natural to leverage the same protocol to signal that IPv4 is discretional on a given segment. An ability to remotely disable IPv4 on a host can be seen as a new denial-of-service attack vector. The approach provided in this document limits the attack surface to DHCPv4-related attacks without introducing new vulnerable elements.

Another benefit of using DHCPv4 for signaling is that IPv4 will be disabled only if both the client and the server indicate IPv6-only capability. It allows IPv6-only-capable hosts to turn off IPv4 only upon receiving an explicit signal from the network and operate in

dual-stack or IPv4-only mode otherwise. In addition, the mechanism defined in this document does not introduce any additional delays to the process of configuring an IP stack on hosts. If the network does not support IPv6-only/IPv4-on-demand mode, an IPv6-only-capable host would configure an IPv4 address as quickly as any other host.

Being a client/server protocol, DHCPv4 allows IPv4 to be selectively disabled on a per-host basis on a given network segment. The coexistence of IPv6-only, dual-stack, and even IPv4-only hosts on the same LAN would not only allow network administrators to preserve scarce IPv4 addresses but would also drastically simplify incremental deployment of IPv6-only networks, positively impacting IPv6 adoption.

3. IPv6-Only Preferred Option

3.1. Option Format

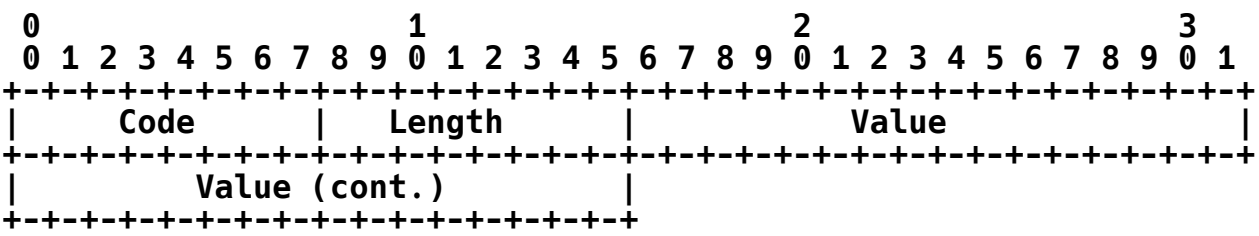

Figure 1: IPv6-Only Preferred Option Format

Fields:

Code: 8-bit identifier of the IPv6-Only Preferred option code as assigned by IANA: 108. The client includes the Code in the Parameter Request List in DHCPDISCOVER and DHCPREQUEST messages as described in Section 3.2.

Length: 8-bit unsigned integer. The length of the option, excluding the Code and Length Fields. The server MUST set the length field to 4. The client MUST ignore the IPv6-Only Preferred option if the length field value is not 4.

Value: 32-bit unsigned integer. The number of seconds for which the client should disable DHCPv4 (V6ONLY_WAIT configuration variable). If the server pool is explicitly configured with a V6ONLY_WAIT timer, the server MUST set the field to that configured value. Otherwise, the server MUST set it to zero. The client MUST process that field as described in Section 3.2.

The client never sets this field, as it never sends the full option but includes the option code in the Parameter Request List as described in Section 3.2.

3.2. DHCPv4 Client Behavior

A DHCPv4 client SHOULD allow a device administrator to configure IPv6-only capability either for a specific interface (to indicate that the device is IPv6-only capable if connected to a NAT64 network via that interface) or for all interfaces. If only a specific

interface is configured as IPv6-only capable, the DHCPv4 client MUST NOT consider the host an IPv6-only-capable host for the purpose of sending/receiving DHCPv4 packets over any other interfaces.

The DHCPv4 client on an IPv4-requiring host MUST NOT include the IPv6-Only Preferred option code in the Parameter Request List of any DHCPv4 packets and MUST ignore that option in packets received from DHCPv4 servers.

DHCPv4 clients running on IPv6-only-capable hosts SHOULD include the IPv6-Only Preferred option code in the Parameter Request List in DHCPDISCOVER and DHCPREQUEST messages for interfaces so enabled and follow the processing as described below on a per-enabled-interface basis.

If the client did not include the IPv6-Only Preferred option code in the Parameter Request List in the DHCPDISCOVER or DHCPREQUEST message, it MUST ignore the IPv6-Only Preferred option in any messages received from the server.

If the client includes the IPv6-Only Preferred option code in the Parameter Request List and the DHCPOFFER message from the server contains a valid IPv6-Only Preferred option, the client SHOULD NOT request the IPv4 address provided in the DHCPOFFER. If the IPv6-Only Preferred option returned by the server contains a value greater than or equal to MIN_V6ONLY_WAIT, the client SHOULD set the V6ONLY_WAIT timer to that value. Otherwise, the client SHOULD set the V6ONLY_WAIT timer to MIN_V6ONLY_WAIT. The client SHOULD stop the DHCPv4 configuration process for V6ONLY_WAIT seconds or until a network attachment event, whichever happens first. The host MAY disable the IPv4 stack completely on the affected interface for V6ONLY_WAIT seconds or until the network attachment event, whichever happens first.

The IPv6-Only Preferred option SHOULD be included in the Parameter Request List in DHCPREQUEST messages (after receiving a DHCPOFFER without this option, for an INIT-REBOOT, or when renewing or rebinding a leased address). If the DHCPv4 server responds with a DHCPACK that includes the IPv6-Only Preferred option, the client's behavior depends on the client's state. If the client is in the INIT-REBOOT state, it SHOULD stop the DHCPv4 configuration process or disable the IPv4 stack completely for V6ONLY_WAIT seconds or until the network attachment event, whichever happens first. It also MAY send a DHCPRELEASE message. If the client is in any other state, it SHOULD continue to use the assigned IPv4 address until further DHCPv4 reconfiguration events.

If the client includes the IPv6-Only Preferred option code in the Parameter Request List and the server responds with a DHCPOFFER message without a valid IPv6-Only Preferred option, the client MUST proceed as normal with a DHCPREQUEST.

If the client waits for multiple DHCPOFFER responses and selects one of them, it MUST follow the processing for the IPv6-Only Preferred option based on the selected response. A client MAY use the presence of the IPv6-Only Preferred option as a selection criterion.

When an IPv6-only-capable client receives the IPv6-Only Preferred option from the server, the client MAY configure an IPv4 link-local address [RFC3927]. In that case, IPv6-only-capable devices might still be able to communicate over IPv4 to other devices on the link. The Auto-Configure option [RFC2563] can be used to control the autoconfiguration of IPv4 link-local addresses. Section 3.3.1 discusses the interaction between the IPv6-Only Preferred option and the Auto-Configure option.

3.3. DHCPv4 Server Behavior

The DHCPv4 server SHOULD be able to configure all or individual pools to include the IPv6-Only Preferred option in DHCPv4 responses if the client included the option code in the Parameter Request List. The DHCPv4 server MAY have a configuration option to specify the V6ONLY_WAIT timer for all or individual IPv6-mostly pools.

The server MUST NOT include the IPv6-Only Preferred option in the DHCPOFFER or DHCPACK message if the selected pool is not configured as IPv6-mostly. The server MUST NOT include the IPv6-Only Preferred option in the DHCPOFFER or DHCPACK message if the option was not present in the Parameter Request List sent by the client.

If the IPv6-Only Preferred option is present in the Parameter Request List received from the client and the corresponding DHCPv4 pool is explicitly configured as belonging to an IPv6-mostly network segment, the server MUST include the IPv6-Only Preferred option when responding with the DHCPOFFER or DHCPACK message. If the server responds with the IPv6-Only Preferred option and the V6ONLY_WAIT timer is configured for the pool, the server MUST copy the configured value to the IPv6-Only Preferred option value field. Otherwise, it MUST set the field to zero. The server SHOULD NOT assign an address from the pool. Instead, it SHOULD return 0.0.0.0 as the offered address. Alternatively, if offering 0.0.0.0 is not feasible -- for example, due to some limitations of the server or the network infrastructure -- the server MAY include in the DHCPOFFER an available IPv4 address from the pool, as per recommendations in [RFC2131]. In this case, the offered address MUST be a valid address that is not committed to any other client. Because the client is not ever expected to request this address, the server SHOULD NOT reserve the address and SHOULD NOT verify its uniqueness. If the client then issues a DHCPREQUEST for the address, the server MUST process it per [RFC2131], including replying with a DHCPACK for the address if it has not been committed to another client in the meantime.

If a client includes both a Rapid Commit option [RFC4039] and an IPv6-Only Preferred option in the DHCPDISCOVER message, the server SHOULD NOT honor the Rapid Commit option if the response to the client would contain the IPv6-Only Preferred option. It SHOULD instead respond with a DHCPOFFER as indicated above.

If the server receives a DHCPREQUEST containing the IPv6-Only Preferred option for the address from a pool configured as IPv6-mostly, the server MUST process it per [RFC2131].

3.3.1. Interaction with RFC 2563

[RFC2563] defines an Auto-Configure DHCPv4 option to disable IPv4 link-local address configuration for IPv4 clients. Clients can support both the IPv6-Only Preferred option and the Auto-Configure option, just one of the options, or neither option. If a client sends both the IPv6-Only Preferred option and the Auto-Configure option, the network administrator can prevent the host from configuring an IPv4 link-local address on an IPv6-mostly network. To achieve this, the server needs to send a DHCPOFFER that contains a 'yiaddr' of 0.0.0.0, and the Auto-Configure flag set to "DoNotAutoConfigure".

However, special care should be taken in a situation where a server supports both options and receives just an IPv6-Only Preferred option from a client. Section 2.3 of [RFC2563] states that if no address is chosen for the host (which would be the case for IPv6-only-capable clients on an IPv6-mostly network), then "If the DHCPDISCOVER does not contain the Auto-Configure option, it is not answered." Such behavior would be undesirable for clients supporting the IPv6-Only Preferred option without supporting the Auto-Configure option, as they would not receive any response from the server and would keep requesting a response instead of disabling DHCPv4 for V6ONLY_WAIT seconds. Therefore, the following update is made to Section 2.3 of [RFC2563].

OLD TEXT:

> However, if no address is chosen for the host, a few additional steps MUST be taken.
>
> If the DHCPDISCOVER does not contain the Auto-Configure option, it is not answered.

NEW TEXT:

> However, if no address is chosen for the host, a few additional steps MUST be taken.
>
> If the DHCPDISCOVER does not contain the Auto-Configure option and the IPv6-Only Preferred option is not present, it is not answered. If the DHCPDISCOVER does not contain the Auto-Configure option but contains the IPv6-Only Preferred option, the processing rules for the IPv6-Only Preferred option apply.

3.4. Constants and Configuration Variables

V6ONLY_WAIT: The time for which the client SHOULD stop the DHCPv4 configuration process. The value MUST NOT be less than MIN_V6ONLY_WAIT seconds. Default: 1800 seconds

MIN_V6ONLY_WAIT: The lower boundary for V6ONLY_WAIT. Value: 300 seconds

4. IPv6-Only Transition Technology Considerations

Until IPv6 adoption in the Internet reaches 100%, communication between an IPv6-only host and an IPv4-only destination requires some form of a transition mechanism deployed in the network. At the time of writing, the only such mechanism that is widely supported by end hosts is NAT64 [RFC6146] (either with or without 464XLAT). Therefore, the IPv6-Only Preferred option is only sent by hosts capable of operating on NAT64 networks. In a typical deployment scenario, a network administrator would not configure the DHCPv4 server to return the IPv6-Only Preferred option unless the network provides NAT64 service.

Hypothetically, it is possible for multiple transition technologies to coexist. In such a scenario, some form of negotiation would be required between a client and a server to ensure that the transition technology supported by the client is the one the network provides. However, it seems unlikely that any new transition technology would arise and be widely adopted in the foreseeable future. Therefore, adding support for non-existing technologies seems to be suboptimal, so this document implies that NAT64 is used to facilitate connectivity between IPv6 and IPv4. In the unlikely event that a new transition mechanism becomes widely deployed, the applicability of the IPv6-Only Preferred option to that mechanism will depend on the nature of the new mechanism. If the new mechanism is designed in such a way that it's fully transparent for hosts that support NAT64 and the IPv6-Only Preferred option, then the option can continue to be used with the new mechanism. If the new mechanism is not compatible with NAT64 and implementation on the host side is required to support it, then a new DHCPv4 option needs to be defined.

It should also be noted that declaring a host (technically, a host interface) IPv6-only capable is a policy decision. For example,

* An OS vendor may make such a decision and configure their DHCPv4 clients to send the IPv6-Only Preferred option by default if the OS has a 464XLAT CLAT [RFC6877] enabled.

* An enterprise network administrator may provision the corporate hosts as IPv6-only capable if all applications that users are supposed to run have been tested in an IPv6-only environment (or if a 464XLAT CLAT is enabled on the devices).

* Internet of Things (IoT) devices may be shipped in IPv6-only-capable mode if they are designed to connect to an IPv6-enabled cloud destination only.

5. IANA Considerations

The IANA has assigned a new DHCPv4 option code for the IPv6-Only Preferred option from the "BOOTP Vendor Extensions and DHCP Options" registry, located at <https://www.iana.org/assignments/bootp-dhcp-parameters/>.

Tag: 108
Name: IPv6-Only Preferred
Data Length: 4
Meaning: Number of seconds that DHCPv4 should be disabled

Reference: RFC 8925

6. Security Considerations

An attacker might send a spoofed DHCPOFFER containing an IPv6-Only Preferred option with the value field set to a large number, such as 0xffffffff, effectively disabling DHCPv4 on clients supporting the option. If the network is IPv4-only, such clients would lose connectivity, while on a dual-stack network without NAT64 service, only connectivity to IPv4-only destinations would be affected. Recovery from such an attack would require triggering a network attachment event. However, it should be noted that if the network does not provide protection from a rogue DHCPv4 server, the similar attack vector can be executed by offering an invalid address and setting the Lease Time option [RFC2132] value field to 0xffffffff. The latter attack would affect all hosts -- not just hosts that support the IPv6-Only Preferred option. Therefore, the security measures against rogue DHCPv4 servers would be sufficient to prevent attacks specific to the IPv6-Only Preferred option. Additionally, such attacks can only be executed if the victim prefers the rogue DHCPOFFER over legitimate offers. Therefore, for the attack to be successful, the attacker needs to know the selection criteria used by the client and be able to make its rogue offer preferable to other offers.

It should be noted that disabling IPv4 on a host upon receiving the IPv6-Only Preferred option from the DHCPv4 server protects the host from IPv4-related attacks and therefore could be considered a security feature, as it reduces the attack surface.

7. References

7.1. 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>.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC2563] Troll, R., "DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients", RFC 2563, DOI 10.17487/RFC2563, May 1999, <https://www.rfc-editor.org/info/rfc2563>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <https://www.rfc-editor.org/info/rfc3927>.

[RFC4039] Park, S., Kim, P., and B. Volz, "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)", RFC 4039, DOI 10.17487/RFC4039, March 2005,

<https://www.rfc-editor.org/info/rfc4039>.

[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>.

7.2. Informative References

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[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>.

[RFC4957] Krishnan, S., Ed., Montavont, N., Njedjou, E., Veerepalli, S., and A. Yegin, Ed., "Link-Layer Event Notifications for Detecting Network Attachments", RFC 4957, DOI 10.17487/RFC4957, August 2007, <https://www.rfc-editor.org/info/rfc4957>.

[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>.

[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>.

[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>.

Acknowledgements

Thanks to the following people (in alphabetical order) for their review and feedback: Mohamed Boucadair, Martin Duke, Russ Housley, Sheng Jiang, Benjamin Kaduk, Murray Kucherawy, Ted Lemon, Roy Marples, Bjorn Mork, Alvaro Retana, Peng Shuping, Pascal Thubert, Bernie Volz, Éric Vyncke, and Robert Wilton. The authors would like to thank Bob Hinden and Brian Carpenter for the initial idea of signaling IPv6-only capability to hosts. Special thanks to Erik Kline, Mark Townsley, and Maciej Zenczykowski for the discussion that led to the idea of signaling IPv6-only capability over DHCPv4.

Authors' Addresses

Lorenzo Colitti
Google
Shibuya 3-21-3, Shibuya, Tokyo

150-0002
Japan

Email: lorenzo@google.com

Jen Linkova
Google
1 Darling Island Rd
Pyrmont NSW 2009
Australia

Email: furry@google.com

Michael C. Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca
URI: https://www.sandelman.ca/

Tomek Mrugalski
Internet Systems Consortium, Inc.
PO Box 360
Newmarket, NH 03857
United States of America

Email: tomasz.mrugalski@gmail.com