ICANN Controlled Interruption IPv6 Research Study - Summary Report

7th Oct 2025

Overview

Controlled Interruption is a phase in the establishment of a new generic top-level domain that is designed to address the risk of Name Collision. During Controlled Interruption, certain DNS resource records are published at and below the gTLD name that are designed to interrupt resolution processes in such a way as to minimize any harm that arises from such interruption.

Controlled Interruption uses A resource records containing the IPv4 address `127.0.53.53`. This address is within the `127.0.0.0/8` prefix, which is used for “loopback” interfaces (see RFC 1122, Section 3.2.1.2). The use of this prefix ensures that any application that uses the result of a DNS query that returns this IPv4 address will not initiate a network connection. `127.0.53.53` is used instead of `127.0.0.1` so that if a user or administrator performs a web search for this address, they are more likely to be shown links to the Name Collision resources on ICANN’s web site.

When the concept of Controlled Interruption was originally developed in 2014, no suitable equivalent address could be found for IPv6-enabled hosts. While this was noted as a limitation, at the time the impact was limited since fewer than 5% of internet hosts supported IPv6. In the intervening decade, IPv6 adoption has accelerated, and now more than 40% of all internet hosts have IPv6 connectivity. As a result, the lack of an IPv6 solution for Controlled Interruption has a much greater impact.

ICANNs preferred approach would be to use an IPv6 loopback address analogous to the existing IPv4 `127.0.53.53` address, however, IPv6 has only a single loopback address allocated (::1 [RFC 4291]). Two proposals within the IPv6 Operations working group at the IETF to assign a larger loopback prefix have not gained consensus and as a result there is still no

direct equivalent IPv6 address available today. Should such an address become available in the future ICANN would intend to utilize it for Controlled Interruption. In lieu of that, and with a recognition of the current impact of not publishing a AAAA record for Controlled Interruption, an alternative option that can be deployed as an interim solution is highly desirable.

A new research study has been performed to identify one or more IPv6 addresses that may be suitable for use during Controlled Interruption. This study involved a review of the IANA registries for IPv6 to produce a list of candidate addresses, followed by technical tests of popular end-user operating systems to determine whether or not DNS lookups that produce responses containing these addresses result in external network traffic.

Research Study

This document is part of a set of documents covering the results of the study:

- Research Study Stage 1 Report
- Research Study Stage 2 Report
- Research Study Summary Report (this document)

An overview of the results of Stage 1 and 2 are given below.

Stage 1

The study involved a review of all the RFCs published by the IETF that establish or discuss registrations in the Internet Protocol Version 6 Address Space and IANA IPv6 Special-Purpose Address Registry registries, to develop a list of candidate address prefixes. A prefix was considered a candidate if the specifications indicate that packets with a destination address within that prefix would remain local to the host (i.e., packets will not be transmitted outbound from the host).

A range of first class candidate prefixes were identified including

- IPv4 mapped IPv6 address (::ffff:0:0/96) [RFC4291]
- Dummy IPv6 addresses (100:0:0:1::/64) [RFC9780]
- Documentation prefixes (2001:db8::/32 and 3fff::/20) [RFC3849] and [RFC9637]
- Various pre-defined multicast addresses e.g. ff01::1, ff02::1 [RFC4291]

Additionally some second class prefixes were also identified (which didn't meet the specific requirement above, but were included in the testing for completeness)

- Partially unallocated address space (::/128) [RFC4291]
- Unique-Local Unicast (fc00::/10) [RFC4193] [RFC8190]
- Link-Local Unicast (fe80::/10) [RFC4291]

This set of candidate prefixes was put through basic testing to observe the traffic generated and only 3 candidate prefixes generated no network traffic in these tests:

- IPv4 mapped IPv6 address (::ffff:0:0/96) [RFC4291]
- Various pre-defined multicast addresses e.g. ff01::1, ff02::1 [RFC4291]

- Link-Local Unicast (fe80::/10) [RFC4291]

Stage 2

This subset of candidate prefixes were then put through more extensive testing in a range of benchtop tests across a matrix of factors (including but not limited to):

- Popular end-user operating systems (all not end-of-life versions)
  - Desktop/server OS's (e.g. Ubuntu, macOS, Windows, RedHat, *BSD)
  - Mobile platforms (e.g. iOS, Android)
- Various applications:
  - Command line tools (e.g. `ssh`, `curl`, `nc`, `openssl s_client`)
  - Popular browsers (e.g. Chrome, Safari, Firefox)
  - Proxies and mail servers (e.g. `postfix`, `sendmail`, `nginx`, `HAProxy`)
- Dual stack and IPv6 only environments
  - Note that in the IPv6 only environments tested the hosts still had an IPv4 loopback interface.

The testing involved the following steps:

1. Invocation of the application with a test name (which resolved to the candidate prefix).
2. Traffic capture of the resulting network and loopback traffic
3. Analysis of the traffic to determine if DNS resolution was attempted and also to identify any traffic generated by the application on either interface.
4. Analysis of the application behaviour i.e. connection attempt, timeouts or error messages.

Results

The study concluded that 2 types of candidate prefix met the requirements:

Candidate Type	Candidate Prefix	Description
Mapped Loopback	`::ffff:7f/104`	"IPv4-mapped IPv6 addresses" [Section 2.5.5.2 of RFC4291] corresponding to the IPv4 loopback address space 127.0.0.0/8
Pre-defined Multicast	`ff01::1, ff01::2, ff02::1,...`	Several of the pre-defined multicast addresses with limited scope [Section 2.7.1 of RFC4291]

It was observed in the Stage 2 testing that while the Link Local Unicast candidate prefix generated no traffic with a destination IP address of the candidate address, in certain scenarios ICMPv6 Neighbour Solicitation traffic was generated and so this candidate prefix was ruled out.

From the two remaining types, two specific candidate prefixes were tested across the matrix of factors and are determined to be suitable for use in Controlled interruption AAAA records based on meeting the technical criteria (i.e., packets will not be transmitted outbound from the host).

Candidate	Candidate Prefix	Description
1	`::ffff:7f00:3535`	"IPv4-mapped IPv6 address" [Section 2.5.5.2 of RFC4291] corresponding to the IPv4 address 127.0.53.53
2	`ff01::1`	Node-Local Scope Multicast Address, All Nodes Address [Section 2.7.1 of RFC4291] [IANA]

Of these two, Candidate 1 is preferred as discussed below.

Candidate 1

The address `::ffff:7f00:3535` (also represented as `::ffff:127.0.53.53`) is selected from the Mapped Loopback prefix type since it is the companion address to the existing IPv4 Controlled interruption address `127.0.53.53`.

In testing it behaves similarly (though not identically) to the existing IPv4 Controlled interruption address, in that:

- It generates no packets that are transmitted outbound from the host on the network interface.
- In some test scenarios it generates IPv4 traffic on the loopback interface. This tends to generate connection refused, timeouts or similar errors.
- In other test scenarios it produces an error with no connection attempt such as DNS resolution failure or invalid argument.

As with the existing IPv4 Controlled interruption address, it is anticipated that if a user or administrator performs a web search for this address, they are likely to be shown links to the Name Collision resources on ICANN's web site.

Candidate 2

The Node-Local Scope Multicast Address, All Nodes Address is selected from several pre-defined multicast addresses since it has the narrowest scope of the pre-defined addresses.

In testing it:

- Generates no packets that are transmitted outbound from the host on the network interface.
- Generates no packets on the loopback interface.
- Generates a variety of error messages (connection failures, resolution failures, network unreachable, address not supported, invalid argument).

The major drawback of this address is that it is unlikely to lead a user or administrator performing a web search to the Name Collision resources on ICANN's web site.

Proposal

ICANN proposes to use Candidate 1 (`::ffff:7f00:3535`) as the AAAA record in the next round of Controlled Interruption activities and requests feedback from the community on this.