Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-schoen-intarea-unicast-0-04
Updates: 1122, 1812, 2827, 3704 (if approved)
Published: 29 December 2023
Intended Status: Standards Track
Expires: 1 July 2024
Authors: S.D. Schoen
IPv4 Unicast Extensions Project
J. Gilmore
IPv4 Unicast Extensions Project
D. Täht
IPv4 Unicast Extensions Project

Unicast Use of the Formerly Reserved 0/8

Abstract

This document redesignates 0/8, the lowest block in the IPv4 address space, so that this space is no longer reserved. It asks implementers to make addresses in this range fully usable for unicast use on the Internet.

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 1 July 2024.

Table of Contents

1. Introduction

With ever-increasing pressure to conserve IP address space on the Internet, it makes sense to consider where relatively minor changes can be made to fielded practice to improve numbering efficiency. One such change, proposed by this document, is to allow the use of more than 16 million historically reserved addresses at the bottom of the IPv4 address space.

This document provides history and rationale to change the status of the "0/8" or "zeroth" region of the IPv4 address space (historically known as "unspecified network" or "this network") from reserved to unreserved. These addresses are already usable for unicast traffic in some popular TCP/IP implementations today. Standardization as unicast addresses will eventually allow them to be later deployed by Internet stewardship organizations to relieve address space scarcity.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Background

The early Internet reserved many kinds of IPv4 addresses for special purposes. One important such designation involves every IPv4 address beginning with the octet 0 (now "0/8"); all these addresses were designated for use in potential device autoconfiguration features that were to use ICMP messages [RFC0792]. This function was eventually entirely supplanted by other protocols, which, in IPv4, now use only the single address 0.0.0.0.

Autodiscovery of a network-provided configuration came to be handled for IPv4 by DHCP [RFC2131], and formerly by its predecessors BOOTP [RFC0951] and RARP [RFC0903]. In modern practice, the source address of a device seeking an IPv4 configuration from the local network is indicated with a link-layer broadcast in which the network-layer source address 0.0.0.0 and the network-layer destination address is 255.255.255.255.

The reservation of 0/8, despite its obsolescence, has been reiterated in all subsequent IPv4 address allocation RFCs and IANA documents. By 1989, [RFC1122], section 3.2.2.7, for example, noted that this mechanism was already obsolete, even as section 3.2.1.3 continued to expressly prohibit the use of network number 0 for other purposes.

The single special address 0.0.0.0(/32) acquired a variety of related meanings including "unspecified address", "unknown address", "address not set", "address not applicable", etc., while 0.0.0.0/0 means "the default route", which contains every IPv4 host. This single address has remained sufficient for these purposes.

3. Present situation

Today, 0/8 addresses (except for the special address 0.0.0.0) are no longer used in any autoconfiguration protocols. All of this functionality is handled using other distinctly-specified mechanisms and address space, both in IPv4 and IPv6.

The designation of 0/8 as reserved address space is tracked by IANA in the IPv4 Special-Purpose Address Registry [IANA4], as provided for by RFC 6890 [RFC6890]. No known software makes use of this address space in the headers of IPv4 packets transmitted over the wire. While some software already treats it as a potentially valid address, the most common behavior by host and router software when encountering any address within 0/8 is to reject it as a Martian address. These and all other known uses are discussed in the sections "Other Existing Uses of 0/8" and "Compatibility and Interoperability", below.

Since this address space has no existing widespread practical use or interpretation, it can be used for other purposes and help alleviate the shortage of IPv4 addresses. This memo therefore unreserves it, redesignating it as unassigned unicast addresses, available for potential global unicast or other allocation.

4. Change in Status of 0/8

The purpose of this document is to make addresses in the range 0/8 available for active unicast use on the public Internet. This includes supporting them for numbering and addressing networks and hosts, like any other unicast address.

As an exception, the address 0.0.0.0 retains its existing special meanings, as described in the subsection "No Change to Interpretations of 0.0.0.0".

Host and router software SHOULD treat addresses in the 0/8 range, except the host address 0.0.0.0, in the same way that they would treat other unicast IPv4 addresses. Software SHOULD be capable of accepting datagrams from, and generating datagrams to, addresses within this range.

Clients for autoconfiguration mechanisms such as DHCP [RFC2131] SHOULD accept a lease or assignment of an address within 0/8, except the host address 0.0.0.0, whenever the underlying operating system is capable of accepting it.

4.1. No Change to Interpretations of 0.0.0.0

The unqualified address 0.0.0.0 or the individual host address 0.0.0.0/32 has many special meanings which are described in a section "Other Existing Uses of 0/8", below. This document does not make this all-zero address an individually valid unicast address, and it should still not be taken to identify an individual device. As described in prior Internet standards, the address 0.0.0.0 MUST NOT be assigned to an individual interface. This address is valid to appear in both source and destination addresses, with special meanings, in protocols already defined or to be defined in the future.

The network identifier 0.0.0.0/0 also continues to be used to refer to an IPv4 default route (a route which matches any Internet host). This is not inconsistent with the use of explicit routes to individual networks within 0.0.0.0/8. Existing CIDR-based routing logic is readily capable of distinguishing an object like 0.0.0.0/8 (a route referring to a specific /8 whose leftmost octet is always 0) from one like 0.0.0.0/0 (a route including to any IPv4 host); in current routing practice, the default route 0.0.0.0/0 already always

overlaps every more-specific route, regardless of how many zero bits appear at the beginning of a more-specific route's destination.

For avoidance of doubt, we note that all routing implementations MUST permit routes to overlap, and MUST distinguish the default route 0.0.0.0/0 from a more-specific CIDR route such as 0.0.0.0/8 or 0.0.0.0/10, as well as from a leading-zero-octet route such as 0.1.0.0/16. These distinctions are already implied by [RFC4632], section 3.1 (since neither "n" nor "x" is ever stated to be nonzero), and sections 5.1 and 5.2 (describing and requiring generality in the treatment of arbitrary routes, including the default route).

5. Other Existing Uses of 0/8

There are a handful of other uses of 0/8 with special meanings in existing Internet protocols and standards.

A large number of protocols and environments use the special address 0.0.0.0 to mean "unspecified", "unknown", "unset", "not applicable", "any address", "no address", or, as 0.0.0.0/0, the default route containing every IPv4 network. (Two examples, among dozens, are [RFC2131]'s use of 0.0.0.0 in DHCP packets to mean "my IP source address is unknown" and [RFC4541]'s use of 0.0.0.0 to mean "proxied IGMP membership report from a non-Querier".)

All these uses of the address 0.0.0.0 are unchanged by this memo. Due to its variety of special meanings, the address 0.0.0.0 MUST NOT be allocated exclusively to a specific organization or network. Existing standards significantly constrain, but do not preclude, circumstances in which it may appear on the wire.

There are three known non-unicast uses of the 0/8 block as a whole in the RFC series.

* RFC 3338 [RFC3338] (an IPv6 transition mechanism) used 0/8 addresses as synthetic addresses representing surrogate IPv6 addresses, but this practice has already been deprecated by [RFC6535], which indicated that this transition mechanism should switch to RFC 1918 private addresses.

* RFC 7453 [RFC7453] (an MPLS-related SNMP MIB definition) overloads the meaning of addresses in 0/8 by designating them as local identifiers, contrasting with IPv4 addresses. Before production use of 0/8 on the global Internet occurs, this MIB should be updated to provide a separate field for local identifiers and to deprecate the old semantics.

* RFC 6235 [RFC6235] and RFC 8932 [RFC8932] both provide mechanisms for anonymizing network flow datasets that can map addresses into

0/8 in order to obscure them. Implementers SHOULD take into account that source addresses in the future may already lie in this range and will still require anonymization; an IPv4 address SHOULD NOT be assumed to have been anonymized already merely because it is within 0/8.

6. Compatibility and Interoperability

Older Internet standards counseled implementations in varying ways to reject packets from, and not to generate packets to, addresses within 0/8.

Among several standards calling for this behavior, RFC 1122, section 3.2.1.3, and RFC 1812, section 4.2.2.11, say that hosts and routers, respectively, MUST NOT send packets using these addresses, outside of configuration-discovery processes. RFC 1122 implies hosts MUST discard, and RFC 1812 implies routers SHOULD NOT forward, packets whose source address is within 0/8.

RFC 3704 [RFC3704] (BCP 84) cites RFC 2827 [RFC2827] (BCP 38) in asking providers to filter based on source address:

> RFC 2827 recommends that ISPs police their customers' traffic by dropping traffic entering their networks that is coming from a source address not legitimately in use by the customer network. The filtering includes but is in no way limited to the traffic whose source address is a so-called "Martian Address" - an address that is reserved, including any address within 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, or 240.0.0.0/4.

Other RFCs such as 3964, 4380, and 6491 have reiterated specific lists of Martian ranges for other purposes, rather than referring to the subsequently-created IANA Special-Purpose Address Registry. We encourage future RFC authors and implementers to refer to the Special-Purpose Address Registry rather than explicitly providing or using a list of reserved addresses within their documentation.

In this context, RFC 3704 specifies filtering of these addresses as source (not destination) addresses at a network ingress point as a countermeasure against forged source addresses, limiting forwarded packets' source addresses to only the set which have been actually assigned to the customer's network. The RFC's mention of these "Martian Addresses" is based on the assumption that they could never be legitimately in use by the customer network.

Because the 0/8 address space is no longer reserved as a whole, an address within this space is no longer inherently a "Martian" address. Both hosts and routers MUST NOT hard-code a policy of always rejecting such addresses. Hosts and routers SHOULD NOT be

configured to apply Martian address filtering to any packet solely on the basis of its reference to a source (or destination) address in 0/8. Maintainers of lists of "Martian addresses" MUST NOT designate addresses from this range as "Martian". As noted elsewhere, the address 0.0.0.0 retains its special meaning, but is also not a "Martian" address.

The filtering recommended by RFC 3704 is designed for border routers, not for hosts. To the extent that an ISP had allocated an address range from within 0/8 to its customer, RFC 3704 would already not require packets with those source addresses to be filtered out by the ISP's border router.

Since deployed implementations' willingness to accept 0/8 addresses as valid unicast addresses varies, a host to which an address from this range has been assigned may also have a varying ability to communicate with other hosts.

Such a host might be inaccessible by some devices either on its local network segment or elsewhere on the Internet, due to a combination of host software limitations or reachability limitations in the network. IPv4 unicast interoperability with 0/8 can be expected to improve over time following the publication of this document. Before or after allocations are eventually made within this range, "debogonization" efforts for allocated ranges can improve reachability to the whole address block. Similar efforts have already been done by Cloudflare on 1.1.1.1 [Cloudflare], and by RIPE Labs on 1/8 [RIPElabs18], 2a10::/12 [RIPElabs2a1012], and 128.0/16 [RIPElabs128016]. The Internet community can use network probing with any of several measurement-oriented platforms to investigate how usable these addresses are at any particular point in time, as well as to localize medium-to-large-scale routing problems. (Examples are described in [Huston], [NLNOGRing], and [Atlas].) Any network operator to whom such addresses are made available by a future allocation will have to examine the situation in detail to determine how well its interoperability requirements will be met.

7. Unofficial uses of 0/8

Some organizations may be using portions of 0/8 internally as RFC 1918-type private-use address space, for example for internal communications within datacenters. We currently have no publicly-documented examples of this practice. However, future allocations of 0/8 could result in use of this space on the public Internet in ways that overlap these unofficial private-use addresses, creating ambiguity about whether a particular host intended to use such an address to refer to a private or public network (since the address would then have two distinct interpretations with different

addressing scopes). Among other unintended outcomes, hosts or firewalls that have extended greater trust to other hosts based on their use of a certain unofficial network number (that was considered to imply presence on a LAN or within an organization) may eventually receive legitimate traffic from an external network to which this address space has been allocated.

Operators of networks that are making unofficial uses of portions of 0/8 may wish to plan to discontinue these uses and renumber their internal networks, or to request that IANA formally designate certain ranges as additional Private-Use areas.

8. IANA Considerations

This memo unreserves the address block 0/8. It therefore requests IANA to update the IANA IPv4 Special-Purpose Address Registry [IANA4] by removing the entry for 0/8, whose existing authority is RFC 791 [RFC0791], Section 3.2. Additionally, it requests IANA to update the IANA IPv4 Address Space Registry by changing the entry for 000/8 from "IANA - Local Identification, 1981-09, RESERVED" to "Unallocated, Former IANA - Local Identification, [Date of this RFC], UNALLOCATED". Finally, IANA is requested to prepare for this address space to be addressed in the reverse DNS space in in-addr.arpa.

This memo does not effect a registration, transfer, allocation, or authorization for use of these addresses by any specific entity. This memo's scope is to require IPv4 software implementations to support the ordinary unicast use of addresses in the newly unallocated range 0.0.0.1 through 0.255.255.255. During a significant transition period, it would only be prudent for the global Internet to use those addresses for experimental purposes such as de-bogonization testing. After that transition period, a responsible entity such as IETF or IANA could later consider whether, how and when to allocate those addresses to entities or to other protocol functions.

9. Security Considerations

The change specified by this document could create a period of ambiguity about historical and future interpretations of the meaning of host and network addresses in 0/8. Some networks and hosts currently discard all IPv4 packets bearing these addresses, pursuant to statements in prior standards that packets containing these addresses have no agreed-upon meaning and ought not to be sent over the wire.

Disparate filtering processes and rules at present, and in response to the adoption of this document, could make it easier for rogue

network operators to hijack or spoof portions of this address space in order to send malicious traffic.

Live traffic, accepted and processed by other devices, may legitimately originate from 0/8 addresses in the future. Network operators, firewalls, and intrusion-detection systems may need to take account of this change in various regards, including so as to avoid permitting either more or less traffic from such addresses than they expected.

Automated systems generating reports, and human beings reading those reports, SHOULD NOT assume that the use of a 0/8 source address indicates spoofing, an attack, or a new incompatible packet format. At the same time, they SHOULD NOT assume that the use of 0/8 is impossible or will be precluded by other systems' behavior.

Since the Linux kernel has already defaulted to the specified behavior for two years (see "Implementation Status"), it is already possible for deployed systems to disagree about whether packets containing 0/8 may validly appear on the wire. This document offers an opportunity to move to a new consensus in which implementations widely agree that these packets are potentially valid, while giving implementers considerable advance notice ahead of any future deployment of these addresses on the public Internet.

10. Acknowledgements

This document directly builds on prior work by Dave Täht and John Gilmore as part of the IPv4 Unicast Extensions Project. Acknowledgements of contributions to their drafts still need to be transposed here.

11. Normative References

[IANA4] Internet Assigned Numbers Authority, "IANA IPv4 Special-Purpose Address Registry", <https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[RFC0903] Finlayson, R., Mann, T., Mogul, J., and M. Theimer, "A Reverse Address Resolution Protocol", STD 38, RFC 903,

DOI 10.17487/RFC0903, June 1984, <https://www.rfc-editor.org/info/rfc903>.

[RFC0951] Croft, W. and J. Gilmore, "Bootstrap Protocol", RFC 951, DOI 10.17487/RFC0951, September 1985, <https://www.rfc-editor.org/info/rfc951>.

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <https://www.rfc-editor.org/info/rfc1122>.

[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>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC3338] Lee, S., Shin, M-K., Kim, Y-J., Nordmark, E., and A. Durand, "Dual Stack Hosts Using "Bump-in-the-API" (BIA)", RFC 3338, DOI 10.17487/RFC3338, October 2002, <https://www.rfc-editor.org/info/rfc3338>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, DOI 10.17487/RFC4541, May 2006, <https://www.rfc-editor.org/info/rfc4541>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation

Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006, <https://www.rfc-editor.org/info/rfc4632>.

[RFC6235] Boschi, E. and B. Trammell, "IP Flow Anonymization Support", RFC 6235, DOI 10.17487/RFC6235, May 2011, <https://www.rfc-editor.org/info/rfc6235>.

[RFC6535] Huang, B., Deng, H., and T. Savolainen, "Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)", RFC 6535, DOI 10.17487/RFC6535, February 2012, <https://www.rfc-editor.org/info/rfc6535>.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., Ed., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, DOI 10.17487/RFC6890, April 2013, <https://www.rfc-editor.org/info/rfc6890>.

[RFC7453] Mahalingam, V., Sampath, K., Aldrin, S., and T. Nadeau, "MPLS Transport Profile (MPLS-TP) Traffic Engineering (TE) Management Information Base (MIB)", RFC 7453, DOI 10.17487/RFC7453, February 2015, <https://www.rfc-editor.org/info/rfc7453>.

[RFC8932] Dickinson, S., Overeinder, B., van Rijswijk-Deij, R., and A. Mankin, "Recommendations for DNS Privacy Service Operators", BCP 232, RFC 8932, DOI 10.17487/RFC8932, October 2020, <https://www.rfc-editor.org/info/rfc8932>.

12. Informative References

[Atlas] RIPE Network Coordination Centre, "RIPE Atlas", <https://atlas.ripe.net/>.

[Cloudflare] Strong, M., "Fixing reachability to 1.1.1.1, GLOBALLY!", 4 April 2018, <https://blog.cloudflare.com/fixing-reachability-to-1-1-1-1-globally/>.

[Huston] Huston, G., "Detecting IP Address Filters", 13 January 2012, <https://labs.ripe.net/author/gih/detecting-ip-address-filters/>.

[NLNOGRing] NLNOG RING, "10 Years of NLNOG RING", <https://ring.nlnog.net/post/10-years-of-nlnog-ring/>.

[RIPElabs128016] Aben, E., "The Curious Case of 128.0/16", 6 December 2011, <https://labs.ripe.net/author/emileaben/the-curious-case-of-128016/>.

[RIPElabs18] Schwarzinger, F., "Pollution in 1/8", 3 February 2010, <https://labs.ripe.net/author/franz/pollution-in-18/>.

[RIPElabs2a1012]
Aben, E., "The Debogonisation of 2a10::/12", 17 January 2020, <https://labs.ripe.net/author/emileaben/the-debogonisation-of-2a1012/>.

Appendix A. Implementation Status

The behavior specified by this document has been implemented by the Linux kernel since version 5.2, released in July 2019. Accordingly, it has been included in various operating system releases, including Ubuntu 19.10 and Fedora 31 from October 2019, and some Android 11 and 12 devices.

This behavior has also been implemented by the OpenBSD kernel and userspace since May 6, 2022, and hence appears in OpenBSD 7.2, released on October 20, 2022.

This behavior is disabled by default in FreeBSD, but enabled by "sysctl net.inet.ip.allow_net0=1", available in FreeBSD 14.0, released in November 2023. It has been available in development releases since July 13, 2022.

We have prepared a patch which enables this behavior on NetBSD. It has not been merged as of December 2023.

Routing of subnets in the 0/8 range is supported by the Gobgp routing daemon, as of release 3.0.0 in March 2022 (or earlier).

Support for 0/8 addressing may be typical of many DHCP implementations (because the 0/8 address assignment special case has often been handled at the kernel level). If the underlying operating system supports 0/8 assignment to an interface, the final official ISC DHCP release (4.4.3) supports 0/8 allocation as both client and server, as do Busybox DHCP udhcpc/udhcpd (release 1.1.15), and ISC Kea (which currently includes only a DHCP server implementation).

Authors' Addresses

Seth David Schoen
IPv4 Unicast Extensions Project
San Francisco, CA
United States of America

Email: schoen@loyalty.org

John Gilmore
IPv4 Unicast Extensions Project
PO Box 170640-rfc
San Francisco, CA 94117-0640
United States of America

Email: gnu@rfc.toad.com

David M. Täht
IPv4 Unicast Extensions Project
Half Moon Bay, CA
United States of America

Email: dave@taht.net