Internet Engineering Task Force
Internet-Draft
Updates: 4291,5156 (if approved)
Intended status: Standards Track
Expires: February 18, 2013

M. Smith
IMOT

August 17, 2012

A Larger Loopback Prefix for IPv6
draft-smith-v6ops-larger-ipv6-loopback-prefix-01

Abstract

During the development of a network application, it can be useful to run multiple instances of the application using the same transport layer protocol port on the same development host, while also having network access to the application instances limited to the local host. Under IPv4, this has been possible by using different loopback addresses within 127/8. It is not possible under IPv6, as the loopback prefix of ::1/128 only provides a single loopback address. This memo proposes a new larger loopback prefix that will provide many loopback IPv6 addresses.

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 http://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 February 18, 2013.

Table of Contents

1. Introduction

During the development of a network application, it can be useful to run multiple instances of the application on the same development host. It may also be useful or important for network access to these application instances to be limited to the development host itself.

Networked applications that use fixed transport layer protocol ports will typically accept incoming traffic on that port for any address assigned to the host. This will prevent multiple instances of the application running on the same port. This port reuse limitation can be overcome by having each application instance bind to different individual addresses available on the host.

Under IPv4, the 127/8 loopback prefix [RFC1122] provides many addresses that can be used to run multiple instances of an application on the same port, while also limiting access to the local host.

Under IPv6, the ::1/128 loopback prefix [RFC4291] only provides a single address. Multiple application instances using the the same port, bound to different loopback addresses, is not possible.

The IPv4-Mapped IPv6 Address form of 127/8, ::ffff:127.0.0.0/104 [RFC4291], could be used to provide more host local loopback addresses. However these addresses do not have native IPv6 address properties. For example, they cannot accomodate 64 bit Interface Identifiers.

A Unique Local IPv6 Unicast Address (ULA) prefix [RFC4193] could be used to increase the number of addresses available on the local host. However this prefix would need to be manually generated and configured at least once by a system administrator. Without additonal configuration, traffic towards most addresses within the prefix would not be prevented from leaving the local host, and access may not be limited to the local host. A ULA prefix would not be well known, and would not be convenient to remember and type without violating the randomness requirements of the Global ID component of a ULA prefix.

This memo proposes a new larger IPv6 loopback prefix that provides more loopback addresses and has properties of native IPv6 addresses. This prefix will also suit other uses of multiple loopback addresses that may emerge.

This memo, if published, updates [RFC4291] and [RFC5156].

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. Larger Loopback Prefix Requirements

A new larger loopback prefix should attempt to satisfy all of the following requirements:

- be a well known prefix,
- be within an existing special purpose prefix,
- be easy for a human to remember,
- be easy for a human to type,
- covers the existing loopback prefix,
- supports 64 bit Interface Identifiers,
- provides a large number of /64 subnets.

3. Proposed Larger Loopback Prefix

The proposed larger loopback prefix is:

0001:0000:0000:0000:0000:0000:0000:0000/48

or concisely,

1::/48

This prefix meets all but one of the requirements, as it does not cover the existing ::1/128 loopback prefix. It is not possible for a larger loopback prefix with a length of /64 or shorter to cover ::1/128, as this would also cover both the IPv4 Mapped IPv6 Address prefix, ::ffff:0.0.0.0/96, and the deprecated IPv4-Compatible IPv6 Address prefix, ::0.0.0.0/96 [RFC4291].

Some IP implementations represent or perform the loopback function using a "loopback" virtual link layer interface. 127.0.0.1/8 is usually configured on this interface at system initialisation, even though all addresses within 127/8 are valid loopback addresses.

Similarly, ::1/128 is also usually configured on the loopback interface at system initialisation.

For the new larger loopback prefix, the address automatically configured on a loopback interface should be:

1::1/64

4. Larger Loopback Prefix Processing Rules

4.1. Host Rules

4.1.1. Packets Sent with Larger Loopback Source and/or Destination Addresses

Packets with larger loopback source and/or destination addresses MUST be returned to the originating host for standard processing by the local IPv6 protocol implementation. They MUST NOT be sent over any external links attached to the host.

All destinations within the larger loopback prefix MUST be considered assigned to the local host.

4.1.2. Packets Received Externally With Larger Loopback Source and/or Destination Addresses

Packets with larger loopback source and/or destination addresses received over any of the external links attached to the host MUST be dropped. ICMPv6 error messages, such as Destination Unreachable messages, MUST NOT be generated for these dropped packets.

For these dropped packets, it may be useful to generate an appropriate system log message, indicating a packet with an invalid source or destination address (a "martian") was received over an external interface. By default, these messages should be suppressed. If they are enabled, they should be appropriately rate limited to prevent a system log denial-of-service attack.

4.2. Router Rules

IPv4 loopback packet processing rules for routers, specified in [RFC1812], by default prohibited forwarding of packets with 127/8 destinations, other than those originated locally and returned back to the router itself. A software switch could be provided to disable this prohibition. This special case of allowing forwarding of packets towards 127/8 destinations has been taken advantage of by [RFC4379]. An equivalent function for IPv6 is provided by using the

IPv4-Mapped IPv6 prefix of ::ffff:127.0.0.0/104.

The existing ::1/128 packet processing rules for routers is the same as for IPv6 hosts [RFC4291].

For the new larger loopback prefix, the IPv6 router processing rules are modified to match those of IPv4.

4.2.1. Packets Sent with Larger Loopback Source and/or Destination Addresses

By default, a router MUST follow the host processing rules, described previously, for packets sent with larger loopback source and/or destination addresses.

A software switch may be provided to permit packets with larger loopback source and/or destination addresses to be sent via an external interface. If provided, this software switch MUST default to off.

4.2.2. Packets Received Externally With Larger Loopback Source and/or Destination Addresses

By default, a router MUST follow the host processing rules, described previously, for packets received externally with larger loopback source and/or destination addresses.

A software switch may be provided to permit received packets with larger loopback source and/or destination addresses to be forwarded via an external interface. This software switch MUST default to off.

5. Acknowledgements

Nick Hilliard provided valuable review and comments on this memo.

6. IANA Considerations

IANA is requested to allocate 1::/48 from within 0::/8 of the Internet Protocol Version 6 Address Space, for use as a larger loopback prefix for IPv6, as described in this memo.

7. Security Considerations

During deployment of a new larger loopback prefix, there will be a transition period where some hosts and routers have implemented the

larger loopback processing rules defined in this memo while others haven't. These legacy hosts and routers will forward larger loopback traffic using conventional unicast processing. For traffic towards non-local larger loopback addresses, traffic will most likely leave the legacy originating host via it's default route, and may be forwarded by legacy routers using their default route. This may disclose sensitive information, violating security policy.

Packet filters, matching traffic with larger loopback source and/or destination addresses, should be used to prevent unintended forwarding of loopback traffic. They should be deployed at the following locations:

- on the legacy hosts themselves,
- on legacy routers interconnecting two different networks,
- on appropriate security domain boundary legacy routers within the local network, if not all legacy routers within the local network.

Routes for the new larger loopback prefix should not be announced or accepted if received under any circumstances.

8. Change Log [RFC Editor please remove]

draft-smith-larger-ipv6-loopback-prefix-00, initial version, 2012-07-24

draft-smith-larger-ipv6-loopback-prefix-01, much less verbose version, 2012-08-17

9. References

9.1. Normative References

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[RFC5156] Blanchet, M., "Special-Use IPv6 Addresses", RFC 5156, April 2008.

Author's Address

Mark Smith
In My Own Time
PO BOX 521
HEIDELBERG, VIC 3084
AU

Email: markzzzsmith@yahoo.com.au