Default IPv6 Local Only Addressing for Non-Internet Devices
draft-smith-v6ops-local-only-addressing-00

Abstract

For certain types or models of devices it should be clear and obvious that, by default, they should not be reachable from the global IPv6 Internet, or able to reach the global IPv6 Internet, even though the network they are attached to provides global IPv6 Internet connectivity. This memo proposes that these types of devices refuse to configure and use global IPv6 Internet addresses by default.

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 April 16, 2020.

Copyright Notice

Copyright (c) 2019 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
For some types of IPv6 devices, their access to the Internet, and access from the Internet, should be prevented under normal circumstances. Examples of these types of devices are network attached paper printers, local network file and print servers, and various types of "Internet of Things" devices.

As a basic and fundamental prevention measure, these types of devices can have their ability to reach the Internet, or to be reachable from the Internet, prevented by only attaching them to local network links and routers that only support and provide Unique Local Unicast Addresses (ULA) [RFC4193]. These nodes and devices would then only have addresses from within the Link-Local [RFC4291] prefix and ULA prefix(es) available on the link.

In some networks, it may not be possible or easy to use "ULA Only" links to isolate these devices. For example, these devices may need to be attached to the same link as other devices that do have global IPv6 addresses and can reach the Internet. This may be because these local network only devices may need to be discoverable by devices with global Internet addresses via link-only discovery protocols such as multicast DNS (mDNS) [RFC6762].

This memo proposes that when it is clear to a device manufacturer that a device should be isolated from the Internet by default, due its functions and role, the device only configures Link-Local Addresses and non-Internet usable addresses such as ULAs on its...
interfaces, even though the link may support and provide global IPv6
Internet addresses. This memo also proposes that these devices
should have available an override configuration switch that causes
these devices to configure addresses from all prefixes available on
the link, including global IPv6 Internet address prefixes.

These types of devices are known as Local Only Address devices in
this memo.

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. Default Local Only Addresses

By default, a Local Only Address device MUST only configure Link-
Local and non-global IPv6 addresses, currently Unique Local Addresses
[RFC4193], on its network interfaces.

The device SHOULD provide a default override configuration option,
known as Configure All IPv6 Addresses, allowing the device to
configure addresses from all available IPv6 address prefixes on the
link, including global IPv6 addresses.

This Configure All IPv6 Addresses configuration switch SHOULD be
available via a device’s administrative interface. There may be some
devices where it is clear that attachment to the public IPv6 Internet
should never occur; for these devices, this configuration switch SHOULD
be omitted. An example would be IoT devices such as Smart Grid
Advanced Metering Infrastructure (AMI) devices [RFC6272].

(Further thought, there could probably be an RA PIO flag or similar
to override this default for all devices on a link, and a similar
DHCPv6 flag/option. Would mean this ID would be in 6man WG scope
rather than v6ops.)

3. SLAAC Address Configuration

By default, when the Local Only Addresses device is processing IPv6
Router Advertisement Prefix Information Options (PIOs) [RFC4861], to
configure IPv6 interface addresses via SLAAC [RFC4862], the device
MUST only configure addresses using PIOs that provide a prefix that
falls within the Unique Local Unicast Address [RFC4193] address range
of fc::/7, should the A or autonomous address-configuration flag be
set for the FIO.
By default, if there are no ULA prefix PIOs in the received RAs, or no ULA prefix PIOs with the A flag set, the Local Only Addresses device MUST only configure IPv6 Link-Local addresses on its network interface.

By default, if there are ULA prefix PIOs that do not have the A flag set, they MUST be processed per standard RA PIO processing for other flags. For example, a PIO for a ULA prefix, with the A flag unset, and the L or on-link flag set, is still processed, and is asserting that the specified ULA prefix is on-link.

If the Configure All IPv6 Addresses configuration switch is enabled, then the Local Only Addresses device MUST process all IPv6 RA PIOs received for SLAAC address configuration, per [RFC4862], from that point in time onwards.

If the Configure All IPv6 Addresses configuration switch is changed from enabled to disabled, then the Local Only Addresses device MUST immediately remove all global IPv6 addresses from the interface, immediately terminating all upper layer application connections that are using these global IPv6 addresses. This is regardless of any remaining preferred and valid lifetimes for the addresses [RFC4862]. This is immediately enforcing the intention that this Local Address Only device should now be isolated from the global IPv6 Internet.

4. DHCPv6 Address Configuration

By default, if the Local Only Addresses device is using DHCPv6 [RFC8415] for address acquisition and configuration, the device MUST ignore any received IPv6 addresses in either IA_TA or IA_NA options, that not with the ULA prefix of fd00::/7.

By default, if the Local Only Addresses device does not receive any IA_TA or IA_NA options containing addresses from within the ULA prefix of fd00::/7, then the device MUST only configure Link-Local addresses on its interface.

Note that a device using DHCPv6 for address acquisition and configuration could also be using SLAAC for address configuration in parallel. All of the SLAAC Address Configuration procedures described previously will also apply.

If the Configure All IPv6 Addresses configuration switch is enabled, then the Local Only Addresses device MUST then acquire and accept all IPv6 addresses provided by the DHCPv6 server in either IA_NA or IA_TA options.
If the Configure All IPv6 Addresses configuration switch is changed from enabled to disabled, then the Local Only Addresses device MUST immediately remove all global IPv6 addresses from the interface, immediately terminating all upper layer application connections that are using these global IPv6 addresses. This is regardless of any remaining preferred and valid lifetimes for the addresses [RFC4862]. This is immediately enforcing the intention that this Local Address Only device should now be isolated from the global IPv6 Internet. The Local Address Only device should gracefully close its DHCPv6 leases for these global IPv6 addresses, returning them to the DHCPv6 server’s address pool.

5. Permitted Incoming and Outgoing Connections

By default, a Local Address Only device MUST NOT accept any upper layer connections from any global IPv6 addresses. Any connection attempts from global IPv6 addresses MUST be silently ignored, meaning that no connection failure ICMPv6 or transport layer protocol error messages are sent. Connection attempts from other address types, such as Link-Local or ULA addresses are accepted, should other Local Address Only device security policies permit them.

As a Local Address Only device, by default, MUST NOT have any valid global IPv6 addresses, outgoing connections using global IPv6 addresses should not occur.

An application may attempt to overcome this global IPv6 address constraint by constructing packets itself that contain a global IPv6 address source address. These types of packets MUST be dropped by the Local Address Only device, and a system message alerting the Local Only Address device operator to this possible security violation SHOULD be logged with appropriate severity.

If the Configure All IPv6 Addresses configuration switch is changed from disabled to enabled, all incoming and outgoing connections from any type of IPv6 address are permitted, assuming any other Local Address Only device security policies permit them.

6. Example Device Types

The following are some example types of devices for which this default Local Only Address behaviour should be implemented. This is not exhaustive, and should be judged by a vendor on a device by device type basis, by considering the device’s purpose, and most typical and common deployment scenarios.

- Network attached paper printers
o File Server and Network Attached Storage

o IoT devices such as Advanced Metering Infrastructure "smart" electricity meters [RFC6272].

o Networking device Operations, Administration and Maintenance (OAM) and Out-of-Band (OOB) management interfaces, used for and by device monitoring and management protocols such as SNMP [RFC1157].

7. Security Considerations

This memo is specifically about increasing device security by limiting their network accessibility and reachability by default, when it suits the intended use of the device. It is imposing a fundamental truth and constraint that if a device cannot be reached by a packet, the device cannot be attacked by the contents of that packet. By default, suitable devices are not reachable from the Internet, and therefore cannot be attacked from devices on the Internet.

However, this security mechanism is both baseline and coarse. It does not protect against attacks from other devices that can reach the Local Only Address device via ULA or Link-Local addresses.

This mechanism should be considered a minimum measure for suitable devices to implement. It should be combined with other security mechanisms, such as IPsec [RFC4301] for IPv6 layer authentication and application layer authentication.

8. Acknowledgements

Review and comments were provided by YOUR NAME HERE!

This memo was prepared using the xml2rfc tool.

9. Change Log [RFC Editor please remove]

   draft-smith-v6ops-local-only-addressing-00, initial version, 2019-09-15

10. References

10.1. Normative References

10.2. Informative References


Author’s Address