IPv6 Operations (v6ops) Working Group
Internet Draft
Intended status: Informational
Expires: Jan. 2022

X. Xiao
Huawei Technologies
E. Metz
KPN
G. Mishra
Verizon Inc.

July 12, 2021

# Isolating Hosts in Layer-2 and Layer-3 to Simplify ND and IPv6 First-Hop Deployments
## draft-xiao-v6ops-nd-deployment-guidelines-00

Abstract

Neighbor Discovery (ND) is an integral part of IPv6 first-hop. Due to limitation of certain L2 media's support to ND, a number of issues can happen in certain scenarios. The corresponding solutions for these issues have also been designed. These issues and solutions are summarized in RFC3756, RFC6583, OPSECv27. However, there is no guideline on how to avoid the issues or how to select the proper solutions.

This document analyzes existing solutions and summarizes the wisdoms embedded in these solutions into an insight: isolating hosts in L2 and L3 can be effective in preventing ND issues. In deployment scenarios where the ND issues can occur, this prevention approach can be more effective than deploying various solutions to solve the issues. Based on this insight, a set of guidelines is proposed for future ND deployments. These guidelines describe where and when to isolate hosts in L2 and L3 to prevent ND issues, and how to select suitable solutions for the remaining issues. This will likely simplify ND deployments. The impact of the guidelines to other components of IPv6 first-hop is also analyzed and appears small. Therefore, the guidelines will likely simplify the overall IPv6 first-hop deployments.

Copyright Notice



Table of Contents

## 1. Introduction

ND is an integral part of IPv6 first-hop. Due to limitation of certain L2 media's support to the protocol, a number of issues have been discovered, and the corresponding solutions for these issues have also been designed. These issues and solutions are dispersed in more than 20 RFCs. [RFC6583] summarized the issues and solutions up to 2012. [OPSECv27] summarized known IPv6 security issues, including ND issues, up to 2021. Wireless ND (WiND) [RFC6775][RFC8505][RFC8928][RFC8929] discussed ND issues and solutions in Low-Power and Lossy Networks (LLNs) [RFC7102]. However, two ND deployment problems still exist:

1. Neither [RFC6583] nor [OPSECv27] or WiND provides guidelines on how to prevent the issues;
2. Some issues have multiple solutions. There is no guideline on how to select the suitable solutions depending on the usage scenarios.

[RFC8273] recommends using "Unique IPv6 Prefix per Host" as a best practice for ND. By doing so, certain ND issues can be prevented. So it partially solved Problem 1 above. But [RFC8273] cannot be used everywhere. In fact, some concerns about [RFC8273] have been expressed in [8273D].

This document aims to solve both problems by providing deployment guidelines for ND. Depending on the usage scenarios, the guidelines first try to prevent the issues as much as possible, then recommend suitable solutions for the remaining issues. This can result in the simplest ND solution for future usage scenarios.

### 1.1. Terminology

Familiarity with [ND] and [SLAAC] are pre-requisite to understand this document. Familiarity with the ND issues and solutions discussed in [RFC6583] and [OPSECv27] Section 2.3 are also essential to understand this document.

Some frequently used terms are defined in this section.

Host isolation in L2 - A host cannot send packets via the L2 medium to any other hosts. The router will be the only node reachable in L2. This can be realized on P2P media, or on multi-access media with Private VLAN [PVLAN] or Split Horizon [TR177] or wireless isolation [W-Iso] to prevent hosts from communicating with each other in L2.

Host isolation in L3 - Separate hosts into different subnets. It is also known as "unique prefix per host" [RFC8273].

NCE - Neighbor Cache Entry, a binding of a neighbor's IPv6 address and link layer address.

## 2. Summary of ND Issues and Existing Solutions

This section summarizes the main ND issues and solutions. More information can be found in [RFC6583][OPSECv27][RFC6775].

### 2.1. Multicast Issues and Solutions

ND uses multicast (L3) extensively for Node Solicitations (NSs), Router Solicitations (RSs) and Router Advertisements (RAs). When multicast messages are sent over an L2 medium, they are usually mapped into L2 broadcast messages. For many wireless media, L2 broadcast may consume more network resources than multiple P2P unicast combined [RFC6775][RFC7668], and have lower probability to be delivered. In addition, multicast has no acknowledgement. Consequently, multicast may cause a number of issues:

- Multicast-resource-consumption issue: multicast in L3 and the resulted broadcast in L2 may consume many times more resources than unicast;
- Multicast-power-consumption issue: multicast consumes more power of the sender; In addition, an L2 broadcast message may reach more nodes than the L3 multicast intended. This may consume some receiving nodes' power unnecessarily. For power constrained nodes, this is an issue;
- Multicast-reliability issue: some multicast messages may not reach the destinations. Sleeping nodes may not respond to a multicast message. As a result, protocol procedures that rely on multicast can be unreliable.

Existing ND solutions that can prevent or address multicast issues include:

. Mobile Broadband IPv6 (MBBv6) and Fixed Broadband IPv6 (FBBv6): MBBv6 is defined in "IPv6 in 3GPP EPS" [RFC6459] and "IPv6 for 3GPP Cellular Hosts" [RFC7066]. MBBv6 isolates each host in L2 by putting it in a P2P link with the router. FBBv6 is defined in "IPv6 in the context of TR-101" [TR177]. FBBv6 also isolates each host in l2, either by putting it in a P2P link with the router, or by implementing split horizon on Ethernet to prevent direct host communication. Note that a host here is either a mobile User Equipment (UE), or a routed Residential Gateway (RG), or a real host (e.g. a computer) behind a bridged RG. The router here is either the mobile gateway or the Broadband Network Gateway (BNG). MBBv6 and FBBv6 also isolate each host in L3 by giving it a unique prefix and thus putting it in its own subnet. Consequently, every host can only communicate with the router in both L2 and L3, and there is effectively no multicast. Because in FBBv6, bridged RG situation is very similar to routed RG situation, except that in the former, the hosts are real hosts (e.g. computers), while in the latter, the hosts are the routed RGs. For description simplicity, bridged RGs will not be further discussed in the document.

. Wireless ND (WiND): the solution is defined in a series of RFCs [RFC6775][RFC8505][RFC8928][RFC8929]. WiND changes host and router behaviors to use multicast only for router discovery and not for other protocol procedures. The key points are (1) hosts use unicast to proactively register their addresses at the routers; (2) routers use unicast to communicate with hosts, and become the central address register and arbitrator for the hosts. Router also proactively installs Neighbor Cache Entries (NCEs) for the hosts; (3)each host communicates only with the router. Consequently, multicast is largely eliminated;

. Unique IPv6 Prefix per Host (UPPH) [RFC8273]: this solution reduces the number of hosts in each subnet to one, as a subnet is defined by a prefix. Multicast is greatly reduced, because (1) a host will not use multicast for address resolution of other hosts, because the router is the only L3 next-hop; (2) downstream multicast from router to hosts are eliminated and turned into unicast ([RFC8273] Section 4). The pros and cons of RFC8273 will be briefly reviewed in Section 3.1. An in-depth discussion can be found in [8273D].

. IP Point to Point Ethernet Subnet Model [P2Peth]: if progressed, this draft may provide a solution similar to RFC8273, making use of unique prefix per host to reduce multicast.

## 2.2. DAD-unreliable Issues and Solutions

Duplicate Address Detection (DAD) uses absence of response as indication of no duplicate. This can be unreliable because either the Neighbor Solicitation or the Neighbor Advertisement messages may be lost in transmission, especially in wireless environment, or the sleeping nodes may not respond. Duplication thus may not be detected.

Existing ND solutions that can prevent or address DAD-unreliable issue include:

. MBBv6 and FBBv6: for MBBv6, the UE's Interface ID (IID) is assigned by the mobile gateway, and is guaranteed to be unique [RFC6459]. There is no need for DAD. For FBBv6, the RG's Global Unicast Address (GUA) prefix is unique. There will be no duplicate for GUA address, and no DAD will be performed. RG will perform DAD for its Link Local Address (LLA), but only to the BNG [TR177]. In such an environment, there is no sleeping node or lossy media. DAD has no reliability issue.

. WiND: every host must register its address at the router before using it. The registration will succeed only if router explicitly approves it, and router will not approve if it is a duplicate. Therefore, the DAD procedure becomes reliable.

. RFC8273: For GUA addresses, since each host is given a different prefix, duplicate address will not exist. For link local address, since each subnet has only one host, there is no possibility of duplication in the subnet. A duplicate link local address may exist in another subnet but that does not matter. Therefore, DAD-unreliable issue is prevented.

## 2.3. On-demand NCE Installation Issues and Solutions

ND address resolution is on-demand. It is done only when a packet needs to be sent but the link layer address of the on-link destination is unknown. Consequently, the packet has to be queued until link layer address of the destination is determined. This increases delay and may affect application performance. For high performance environment, this can be an issue.

Existing ND solutions that can prevent or address on-demand NCE installation issue include:

. MBBv6 and FBBv6: MBBv6 and some FBBv6 use IPv6 over PPP [RFC5072]. In this case, there is no need to find out the link layer address before sending a packet on the interface. In other words, there is no NCE installation issue. Some FBBv6 implementations use IPoE. There is a need for NCE. But because every host is given a unique prefix by the BNG in FBBv6, the BNG needs to know the host's link layer address which uniquely identify the host in order to do so. Therefore, the BNG can install NCE when assigning a prefix to the host, not waiting until a data packet is to be sent to that host. On-demand NCE installation issue is therefore avoided in this case too.

. Wireless ND (WiND): when hosts register their IPv6 addresses, they will also present their link layer address. Therefore, NCE entries can be installed proactively before data packets arrive.

. Gratuitous Neighbor Discovery [GRAND]: this solution changes router and host behaviors to allow routers to proactively create an NCE when a new IPv6 address is assigned to a host, and to recommend hosts sending unsolicited Neighbor Advertisements upon assigning a new IPv6 address. It can be considered as the IPv6 equivalent of Gratuitous ARP in IPv4.

## 2.4. Security Issues and Solutions

ND assumes all nodes can be trusted. Otherwise, ND has various security issues. These issues are described in [RFC3756][RFC6583] and [OPSECv27]. They are briefly summarized here.

The security issues can be classified into two categories:

. Redirect attacks, in which a malicious node redirects packets away from the first-hop router or other legitimate receiver to another node on the link. This is usually done by spoofing the source IPv6 address to pretend to be another node, or by faking Router Advertisement to pretend to be a router. For example:

  o an attacker can send out Router Advertisement claiming itself as the router, and redirect other hosts' traffic to itself.

- an attacker can send Neighbor Advertisements to the first-hop router, spoofing the IPv6 address of another node while using its own link layer address. This will redirect traffic from the router to the victim to the attacker instead.

. Denial-of-Service (DoS) attacks, in which a malicious node prevents communication between the node under attack and all other nodes or a specific destination address. For example:

- Whenever a host performs DAD, an attacker can reply to claim that the selected address is in use. The host will not be able to get an address.

- /64 scan attacks: an attacker sends packets to up to 2**64 mostly non-existing hosts, forcing the first-hop router to try to install NCEs for this huge number of non-existing hosts. If unprotected, the router will run out of resource and stop functioning. Note that for other attacks to happen, the attacker must be on-link. But for this /64 scan attack, the attacker can be off-link.

It is worth noting that redirect attacks are generally considered as more harmful than DoS attacks. Therefore, higher priority is given to protect against redirect attacks.

Existing ND solutions that can prevent or address the security issues include:

. MBBv6 and FBBv6: because every host is isolated in L2, all on-link security issues are prevented. Because every host has its own prefix, and the mobile gateway or BNG maintains state information for the prefixes not for individual IPv6 address, off-link /64 scan attack will not cause harm because the mobile gateway or BNG will not create any NCE when receiving such messages. Such attack messages can simply be dropped.

. WiND: normally, every host is isolated in L2 and can only communicate with the first-hop router. Therefore, all on-link security issues are prevented. But if hosts are not isolated in L2, e.g. when there is a bridge between the hosts and the router, then on-link security issue can happen. Off-link /64 scan attack will not cause harm because in WiND, NCE installation is proactive not reactive. In other words, the router will not create any NCE when receiving such messages. Such attack messages can simply be dropped.

. RFC8273: by giving each host a different prefix and keep track of host-prefix binding, an attacker host cannot change the NCE at the router for another host by sending Neighbor Advertisement with a spoofed source IPv6 address of that host. The attacker thus cannot redirect traffic from router to that host to itself. The router will maintain only one NCE entry for each prefix/host. Therefore, off-link /64 scan attack will not cause harm. RFC8273's protection effect against other security issues depends on whether the hosts are also isolated in L2. If yes, all the on-link security issues will be prevented. If not, certain on-link security issues remain.

. Source Address Validation Improvement [SAVI], Router Advertisement Guard [RA-Guard][RA-Guard+]: these solutions protect against redirect attacks and some DoS attacks. SAVI binds an address to a port, and rejects claims from other ports for that address. Therefore, a node cannot spoof the IP address of another node. RA-Guard and RA-Guard+ only allow RAs from a port that a router is connected. Therefore, nodes on other ports cannot pretend to be a router. In order to protect against some other DoS attacks, e.g. off-link /64 scan attack, other security measures are needed, e.g. rate limiting on NSs, and filtering on NAs/RAs.

. Secure Neighbor Discovery [SeND] and Cryptographically Generated Addresses [CGA]: these solutions have tried to make ND secure, but have not been widely deployed. They will not be further discussed in this document.

## 2.5. Observations on the Solutions and the Insight Learned

MBBv6 and FBBv6 prevent or solve all the ND issues. These solutions have two common characteristics that are effective for preventing or solving ND issues:

(1) Hosts (i.e. UEs or RGs or real hosts) are isolated in both L2 and L3.
(2) The first-hop router (i.e. mobile gateway or BNG) maintains some state information across reboots, e.g. prefix to host binding. The router also maintains some controls over the hosts, e.g. which prefix each host gets.

WiND prevents or solves all the ND issues in its deployment scenarios, e.g. Low power and Lossy Networks (LLNs) [RFC7102]. WiND also has two characteristics:

(1) Hosts are normally isolated in L2 but not in L3. In fact, many hosts are in the same subnet. In the rare cases where hosts are not isolated in L2, e.g. because there is an bridge between the hosts and the router, then some ND issues like on-link security issues may happen, and additional solutions will be needed to address those issues.
(2) The first-hop router maintains some state information across reboots, e.g. host's address registration result including IPv6 address to link layer address binding. The router also uses such state information to maintain some controls over the hosts, e.g. which host wins when there is an address contention.

RFC8273 solves certain ND issues but not all. It has two characteristics:

(1) Hosts are isolated in L3 in their own subnet, but RFC8273 does not specify whether hosts should also be isolated in L2. If hosts are also isolated in L2, all ND issues will be prevented.
(2) The first-hop router maintains some state information across reboots, e.g. prefix-host binding. The router also maintains some controls over the hosts, e.g. which prefix a host gets.

SAVI, RA-Guard, RA-Guard+ and GRAND solve specific ND issues. They have two characteristics:

(1) These solution make no assumptions on isolation of hosts in L2 or L3. They just solve the ND issues that they are designed to solve.
(2) SAVI maintains some state information at the Ethernet switch between the hosts and the first-hop router(s). Such states are learned dynamically from packet snooping, or configured manually. The Ethernet switch uses such state information to control the hosts, e.g., RAs are not allowed from the hosts.

An insight can be learned from observing ND practices in these existing IPv6 first-hop deployments. That is, isolating hosts in L2 and L3 can be effective in preventing ND issues. But isolating hosts in L2 and L3 also has a price to pay. That is, because hosts are isolated and cannot directly coordinate with each other, the router must have new functionality to coordinate on behalf of the hosts, e.g. to be the arbitrator when there is an address contention. In order to do so, the router will also need to maintain some state information, e.g. IP address-link layer address binding for each host. This insight can be used to guide future ND deployments.

# 3. Isolating Hosts in L2 and L3 to Simplify ND Deployments

## 3.1. Applicability of Host Isolation in L2 and L3

This section describes how to isolate hosts in L2 and L3, and the advantages and disadvantages of doing so.

Isolating hosts in L2 can be done by: (1) putting a host in a P2P link with the router, or (2) using private VLAN [PVLAN], or split horizon [TR177], or wireless isolation [W-Iso] on multi-access medium to prevent hosts from communicating with each other. These are a matter of device configuration so it can usually be done as long as the devices support these isolating features.

Isolating hosts in L2 is different from setting ND Prefix Information Option (PIO) L-bit=0. In the former, multicast messages from a host will not reach other hosts in the same L2 broadcast domain. In the latter, a host will not do address resolution for other hosts with that prefix, but multicast messages from the host will be mapped into L2 broadcast, and will reach other hosts in the same L2 broadcast domain.

When hosts are isolated in L2, DAD messages can only reach the router but not other hosts. Therefore, the router must act to prevent hosts from using duplicate GUA or link local address. This functionality is called DAD Proxy [TR177][RFC6957].

The advantages of isolating hosts in L2 include:

- Prevention of on-link security and upstream multicast issues (from hosts), because hosts cannot reach each other directly.

The disadvantage of isolating hosts in L2 include:

- The router must support additional functionality: DAD Proxy.
- Downstream multicast issues, DAD-unreliable issue, On-demand NCE Installation issue and off-link /64 scan issue still remain.
- All host communication must go through the router. In a high performance environment, the router may become the bottleneck.
- Services relying on multicast, e.g. Multicast DNS [mDNS], will not work, unless the router can provide multicast proxy.

- There is additional work (e.g. PVLAN, split horizon or wireless isolation) to isolate hosts in L2 in multi-access media, but this is small amount of work.

From the analysis above, it is clear that L2 isolation alone is not advantageous. The benefits are relatively small while the costs are relatively high. Therefore, L2 isolation is better used with something else, e.g. L3 isolation or some specially designed solutions like WiND.

The known solutions supporting host isolation in L2 include WiND, and in more special cases (i.e. with both L2 and L3 isolation), MBBv6 and FBBv6.

Host isolation in L3 (i.e. Unique Prefix Per Host, or UPPH) can be done either with [DHCPv6], where the prefix can be of any length supported by DHCPv6, or with SLAAC as specified in RFC8273, where the prefix must be /64 or shorter. If [P2Peth] is progressed, it can provide another solution.

In order to isolate hosts in L3, the router must be able to assign a unique prefix to each host and keep track of the prefix-host link layer address binding. This will be referred to as "UPPH support" later in this document. This may be achieved by some mechanism that RFC8273 alluded to but did not specify, or by some other mechanisms if DHCPv6 is used [TR177]. Note that with SLAAC/RFC8273, such router implementation exist [8273D], while with DHCPv6, FBBv6-capable BNG is one of such implementations.

The advantages of isolating hosts in L3 are:

- Downstream Multicast, DAD-unreliable, on-demand NCE installation and off-link /64 scan issues are prevented.

- It is the only way for the router to do subscriber management on the hosts in a SLAAC environment. Imagine a public Wi-Fi scenario where the mobile UEs only support SLAAC. If the router does not give each UE a unique prefix and keep track of UE-prefix binding, network administrators do not know which IPv6 address corresponds to which UE, because each UE picks its own IID and uses the same prefix. Therefore, network administrators cannot keep track of which UE did what. This would be unacceptable from an operation perspective.

The disadvantages of isolating hosts in L3 are:

- The routers must support new functionality: "UPPH support".

- Upstream multicast and on-link security issues can happen, unless the hosts are also isolated in L2

- Many prefixes will be needed instead of just one. But this disadvantage may not as severe as it appears. After all, 3GPP has given every mobile UE a /64 [RFC6459], and BBF has given every routed RG a /56 with DHCPv6 PD [TR177]. Outside of MBB, FBB and IoT, not many scenarios have a large number of hosts. Giving each host a /64 prefix may not be as deficient as it appears.

The known solutions supporting host isolation in L3 include RFC8273, and in more special cases, MBBv6 and FBBv6.

Careful analysis of the advantages and disadvantages of L2 isolation and L3 isolation will reveal that they are synergetic. When they are done together, the advantages are:

- All ND issues are prevented.

- It provides a way for the router to do subscriber management on the hosts in a SLAAC environment.

- DAD Proxy needed for L2 isolation is no longer needed, because with unique prefix per host, GUA cannot be duplicate. For link local address, since each subnet has only one host, there is no possibility of duplication. A duplicate link local address may exist in another subnet but that does not matter. Therefore, there is no need for DAD Proxy to prevent duplicate GUA/LLA addresses.

The disadvantages are:

- The routers must support new functionality: "UPPH support" .

- Many prefixes will be needed instead of just one.

- All host communication must go through the router. In a high performance environment, the router may become the bottleneck.

- Services relying on multicast, e.g. mDNS, will not work, unless the router can provide multicast proxy.

- There is additional work (e.g. PVLAN, split horizon or wireless isolation) to isolate hosts in L2 in multi-access media, but this is small amount of work.

The known solutions supporting host isolation in L2 and L3 include RFC8273, MBBv6 and FBBv6.

### 3.2. Deployment Guidelines

Given the applicability analysis in Section 3.1, network administrators can decide where to use which isolation option. Note that in all the following steps, if DHCPv6 (IA_NA or PD) is supported and desired, use DHCPv6 to assign address prefix, as it may provide more prefix length flexibility. Otherwise, use SLAAC as SLAAC is more widely supported.

1. If isolating hosts in both L2 and L3 is desirable and feasible:

   Based on the applicability discussion in Section 3.1, the scenarios here likely have some or all of the following characteristics: (1) It is a public access environment where subscriber management is needed; (2) Many ND issues can happen and will require solutions. This is why it is desirable to prevent as many issues as possible, to simplify the deployment; (3) Neither high performance communication nor multicast service discovery is applicable here.

   With suitable "UPPH support", all the ND issues will be prevented. Some possible "UPPH support" solutions are:

   a) If the deployment scenario is MBB or FBB, then MBBv6 or FBBv6 can be used.

   b) Otherwise, use a RFC8273 implementation (using SLAAC) to realize "UPPH support". Note that this is a special use case of RFC8273 where each host is not only given a unique prefix, but also isolated from other hosts in L2.

2. Otherwise, if isolating hosts in L2 but not in L3 is considered appropriate:

   In this scenario, hosts are in different links but in the same subnet. This architecture is called Multi-Link SubNet (MLSN). So far only WiND and [OMNI] support MLSN. But OMNI is not widely supported so WiND is the only solution available. Therefore, the scenario here is most likely one that WiND is suitable for, e.g.

Low-power and Lossy Networks (LLNs). Because WiND has more functionalities than DAD Proxy (required by L2 host isolation), e.g. proactively address registration, WiND prevents all ND issues.

3. Otherwise, if isolating hosts in L3 but not in L2 is considered appropriate:

   Based on the applicability discussion in Section 3.1, the scenarios here likely have the following characteristics: (1) Subscriber management is needed. This is likely a public access scenario. (2) Upstream multicast is needed or cannot be avoided (otherwise L2 host isolation would have been selected to prevent more issues), e.g. for service discovery. RFC8273 can be used as the solution here. On-link security is not prevented in this case. Because this is a public access scenario, SAVI/RA-Guard/RA-Guard+ may be needed to address the on-link security issue.

4. Otherwise, no isolation in L2 or L3 is desired or feasible.

   The scenarios here likely have the following characteristics: (1) It is a private environment, because subscriber management is not needed. As such, on-link security is not a big concern. (2) Either multicast service is needed, or this is a high performance scenario, because L2 host isolation is not desired. Either way, multicast and DAD-unreliable are not a concern. Normal ND can be used as the solution. Off-link /64 scan and on-demand NCE installation are the two issues left. Off-link /64 scan issue can be handled by rate limiting or unused-address filtering. If this is indeed a high performance environment, e.g. a DC network, GRAND can be used to enable proactive NCE installation.

In short, the guidelines can be summarized as: if many of the ND issues discussed in Section 3 are valid concerns and need to be addressed, then isolate hosts in L2 and L3 to prevent the issues, and use RFC8273. If the scenario is LLN, use WiND. But if the scenario is a private environment where many ND issues are not real concerns, then just use normal ND, and adds other solutions like GRAND only when needed. Overall, these guidelines will likely result in the simplest ND solution.

## 4. Impact of L2 and L3 Host Isolation to Other Components of IPv6 First-hop

The guidelines should simplify ND deployments. But will they complicate other components of IPv6 first-hop? A preliminary impact analysis is done in this section.

IPv6 first-hop consists of:

- The routers and the hosts, whose requirements & behaviors are defined in [RFC8504];
- Addressing scheme;
- The basic protocol suite: ND, SLAAC, DHCPv6, DNS, ICMPv6, MLD v1/v2;
- Other extended protocols: mDNS.

The impact of host isolation in L2 and L3 to other components of IPv6 first-hop comes from three parts: (1) the special topology introduced by L2 host isolation; (2) the special addressing scheme introduced by L3 host isolation (i.e. unique prefix per host); (3) the new functionalities introduced to the router, i.e. "DAD Proxy" for L2 isolation and "UPPH support" for L3 isolation. (4) When WiND is used, hosts must be changed to support proactive address registration etc. This is a high requirement that can be considered as complicating the IPv6 first-hops. But WiND is the only solution in its applicable scenarios like LLNs. When there is no alternative, there is no need to discuss whether the solution unduly complicates other components of IPv6 first-hop. Therefore, WiND will not be further discussed. Because DAD Proxy is only needed in L2 but not L3 isolation, and this scenario uses WiND which already provides DAD Proxy, DAD Proxy will not be further discussed either.

First, regarding the impact from the special topology:

Isolating hosts should only affect the protocols that rely on multicast, i.e. ND, SLAAC and mDNS, but not the multicast protocols themselves, i.e. MLD v1/v2. As discussed in Sections 2 and 3, the impact on ND and SLAAC are positive. The impact on mDNS can be negative, if new functionality like "multicast proxy at router" has to be introduced. But the guidelines give network administrators the option not to isolate hosts at all. So if network administrators choose to isolate, the benefit must outweigh the cost.

Second, regarding the impact from the special addressing scheme:

IPv6 first-hop should allow any addressing scheme. Other than using more prefixes, it is not clear that unique prefix per host complicates addressing scheme in any way. After all, unique prefix per host is already widely in use in MBBv6 and FBBv6 deployments.

Third, regarding the impact of new router functionality "UPPH support":

The impact of "UPPH support" with RFC8273 using SLAAC has been discussed in [8273D] before RFC8273 became an RFC. The following concerns had been raised:

. RFC8273 makes the router stateful;
. How to reclaim unused prefix is not specified;
. If there are multiple first-hop routers, how the solution works is unspecified: (1) do they assign prefixes to hosts independently? (2) do they need to sync up with each other?
. Resiliency of SLAAC may be reduced as a result of the increased state at the router, i.e. the prefix-host binding.

Given that RFC8273 became an RFC, the rough consensus may have been its benefit outweighs the cost. Because MBBv6 and FBBv6 also support UPPH and are widely deployed, the impact of "UPPH support" is likely manageable.

All things considered, it appears that isolating hosts in L2 and L3 can simplify ND without unduly complicating other components of IPv6 first-hop.

## 5. Applying the Guidelines to Real World Scenarios

The guidelines are intended for future IPv6 first-hop deployments. But if we test the guidelines on well-known IPv6 scenarios to find the solutions, the results will be as follows:

o MBB and FBB will end at Step 1.a: isolating hosts in L2 and L3, with MBBv6 as the solution with SLAAC and FBBv6 as the solution with DHCPv6, respectively;

- Public Wi-Fi network will end at Step 1.b: isolating hosts in L2 and L3, with RFC8273 as the solution with SLAAC, since the hosts here may be mobile UEs that do not support DHCPv6. Note that in Wi-Fi with the Infrastructure Mode [WiFi-inf], each host (i.e. STA) communicates only with the Access Point (AP). With wireless isolation, every host can only communicate with the AP (and the router if the AP is not a router), not directly with other hosts. This is how L2 isolation can be achieved in this scenario. If L2 isolation is not done, then public Wi-Fi will end at Step 3. SAVI/RA-Guard/RA-Guard+ may be needed to address the on-link security issue.

- Low-power and Lossy Networks (LLNs) will end at Step 2: isolating hosts in L2 but not L3, with WiND as the solution with SLAAC. Note that although WiND did not mandate L2 isolation, WiND works better when hosts are isolated in L2. Otherwise, additional mechanisms may be needed to address on-link security issues.

- High speed DC Networks will end at Step 4: using normal ND with GRAND without host isolation in L2 or L3. SAVI, RA-Guard and RA-Guard+ may not be needed as high physical access security is likely maintained.

- Common enterprise LANs with mixed Ethernet and Wi-Fi (not DC networks) will end at:

    - If security is a concern to justify host isolations:

        . Step 1.b: isolating hosts in L2 and L3, with RFC8273 as the solution with SLAAC;.

    - If security is not a concern to justify host isolations:

        . Step 4: using normal ND with no special host isolation. GRAND and SAVI, RA-Guard and RA-Guard+ may not be needed.

- [HomeNet] will end at Step 4: using normal ND with no special host isolation. GRAND and SAVI, RA-Guard and RA-Guard+ are not needed.

These results match current practices in reality. This validates the guidelines to some extent.

## 6. Security Considerations

This document provide guidelines on how and where to isolate hosts in L2 and L3 to prevent ND issues, and how to select existing solutions for the remaining issues. When a solution is selected, the security considerations of that solution apply. This document does not introduce any new mechanisms. Therefore, it does not introduce new security issues.

## 7. IANA Considerations

This document has no request to IANA.

## 8. References

### 8.1. Informative References

[8273D] Discussion on the pros and cons of RFC8273, https://mailarchive.ietf.org/arch/msg/v6ops/M47lN8lyXaWVcx8nitvkxMfbGNA/

[CGA] T. Aura, "Cryptographically Generated Addresses (CGA)" , RFC3972

[DHCPv6] T. Mrugalski M. Siodelski B. Volz A. Yourtchenko M. Richardson S. Jiang T. Lemon T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415.

[GRAND] J. Linkova, "Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers", https://datatracker.ietf.org/doc/html/draft-ietf-6man-grand-07

[HomeNet] T. Chown, J. Arkko, A. Brandt, O. Troan, J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, DOI 10.17487/RFC7368, October 2014, <https://www.rfc-editor.org/info/rfc7368>.

[mDNS] S. Cheshire, M. Krochmal, "Multicast DNS", RFC 6762.

[ND] 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>.

[OMNI] F. Templin, A. Whyman, "Transmission of IP Packets over Overlay Multilink Network (OMNI) Interfaces", https://www.ietf.org/archive/id/draft-templin-6man-omni-interface-99.txt

[OPSECv27] E. Vyncke, K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks", https://datatracker.ietf.org/doc/html/draft-ietf-opsec-v6-27 [PVLAN] https://en.wikipedia.org/wiki/Private_VLAN

[P2Peth] O. Troan, "IP Point to Point Ethernet Subnet Model", https://datatracker.ietf.org/doc/draft-troan-6man-p2p-ethernet/

[RA-Guard] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

[RA-Guard+] F. Gont, "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

[RFC3756] P. Nikander, J. Kempf, E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756.

[RFC5072] S. Varada, D. Haskins, E. Allen, "IP Version 6 over PPP", RFC 5072

[RFC6459] J. Korhonen, J. Soininen, B. Patil, T. Savolainen, G. Bajko, K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459.

[RFC6583] I. Gashinsky, J. Jaeggli, W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583.

[RFC6775] Z. Shelby, S. Chakrabarti, E. Nordmark, C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775.

[RFC6957] F. Costa, J-M. Combes, X. Pougnard, H. Li, "Duplicate Address Detection Proxy", RFC 6957

[RFC7066] J. Korhonen, J. Arkko, T. Savolainen, S. Krishnan, "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts", RFC 7066.

[RFC7102] JP. Vasseur, "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102.

[RFC7668] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC7668.

[RFC8273] J. Brzozowski, G. Van de Velde, "Unique IPv6 Prefix per Host", RFC 8273.

[RFC8504] T. Chown, J. Loughney, T. Winters, "IPv6 Node Requirements", RFC 8504, January 2019, <https://www.rfc-editor.org/info/rfc8504>.

[RFC8505] P. Thubert, E. Nordmark, S. Chakrabarti, C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505.

[RFC8928] P. Thubert, B. Sarikaya, M. Sethi, R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928.

[RFC8929] P. Thubert, C.E. Perkins, E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929.

[RIPE IPv6 security] RIPE NCC, "IPv6 Security Training Course", https://www.ripe.net/support/training/material/ipv6-security/ipv6security-slides.pdf

[SAVI] J. Wu, J. Bi, M. Bagnulo, F. Baker, C. Vogt, "Source Address Validation Improvement (SAVI) Framework", RFC 7039

[SeND] J. Arkko, J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC3971

[SLAAC] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[TR177] S. Ooghe, B. Varga, W. Dec, D. Allan, "IPv6 in the context of TR-101", Broadband Forum, TR-177.

[WiFi-inf] Wi-Fi Infrastructure Mode, https://www.howtogeek.com/180649/htg-explains-whats-the-difference-between-ad-hoc-and-infrastructure-mode/

[W-Iso] Wireless Isolation, https://www.quora.com/What-is-wireless-isolation

## 9. Acknowledgments

The authors would like to thank Eduard Vasilenko, Pascal Thubert, and Ole Troan for the discussion and input.

Authors' Addresses

XiPeng Xiao
Huawei Technologies
Hansaallee 205, 40549 Dusseldorf, Germany

Email: xipengxiao@huawei.com

Eduard Metz
KPN N.V.
Maanplein 55, 2516CK The Hague, The Netherlands

Email: eduard.metz@kpn.com

Gyan Mishra
Verizon Inc.

Email: gyan.s.mishra@verizon.com