IoT Bricks Over v6: Understanding IPv6 Usage in Smart Homes

Tianrui Hu
Northeastern University
Boston, Massachusetts, USA
hu.tian@northeastern.edu

Daniel J. Dubois
Northeastern University
Boston, Massachusetts, USA
d.dubois@northeastern.edu

David Choffnes
Northeastern University
Boston, Massachusetts, USA
choffnes@ccs.neu.edu

Abstract

Recent years have seen growing interest and support for IPv6 in residential networks. While nearly all modern networking devices and operating systems support IPv6, it remains unclear how this basic support translates into higher-layer functionality, privacy, and security in consumer IoT devices. In this paper, we present the first comprehensive study of IPv6 usage in smart homes in a testbed equipped with 93 distinct, popular consumer IoT devices. We investigate whether and how they support and use IPv6, focusing on factors such as IPv6 addressing, configuration, DNS and destinations, and privacy and security practices.

We find that, despite most devices having some degree of IPv6 support, in an IPv6-only network just 20.4% transmit data to Internet IPv6 destinations, and only 8.6% remain functional, indicating that consumer IoT devices are not yet ready for IPv6 networks. Furthermore, 16.1% of devices use easily traceable IPv6 addresses, posing privacy risks. Our findings highlight the inadequate IPv6 support in consumer IoT devices compared to conventional devices such as laptops and mobile phones. This gap is concerning, as it may lead to not only usability issues but also privacy and security risks for smart home users.

CCS Concepts

• **Networks** → **Network measurement**; **Network protocols**; • **Security and privacy**;

Keywords

Smart Home, IoT, IPv6, Measurement, Privacy, Security

ACM Reference Format:

Tianrui Hu, Daniel J. Dubois, and David Choffnes. 2024. IoT Bricks Over v6: Understanding IPv6 Usage in Smart Homes. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3646547.3688457

1 Introduction

The adoption of IPv6 has rapidly increased in recent years as the IPv4 address space is exhausted. Most modern operating systems and networked personal devices, such as home routers, laptops, and mobile phones, now support IPv6 by default [51]. Concurrently, Internet of Things (IoT) devices, which were traditionally seen as a primary driver for IPv6 adoption, are becoming increasingly common in homes, offices, and public spaces. Despite this increase in IoT devices, it remains unclear whether these devices are adequately equipped to handle IPv6 properly.

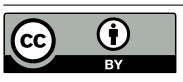
The research community has focused on studying the privacy concerns associated with IPv6 adoption [7, 8, 41, 42] and on developing privacy-enhancing solutions [16, 17, 34] to mitigate these risks. A recent study revealed that if even one of the IoT devices fails to apply the best common practices for IPv6 privacy, it can enable the tracking of users and other IPv6-enabled devices [43]. These studies highlight the need for a better understanding of IPv6 adoption in smart home IoT devices. To address this gap, we conduct a comprehensive measurement study in a US-based IoT testbed containing 93 distinct consumer IoT devices with IPv6 connectivity.

In this paper, we investigate if and how consumer IoT devices support and use IPv6, focusing on factors such as IPv6 addressing, configuration, DNS usage, communication destination, and privacy and security practices. Our study aims to answer research questions around four main areas: (*i*) IPv6 readiness, (*ii*) the extent of IPv6 feature support, (*iii*) the IP version of contacted destinations, and (*iv*) the privacy and security implications. To address these questions, we conduct experiments in six network configurations, featuring various combinations of IPv4 and IPv6 connectivity over a two-week period. We first assess whether the devices function in an IPv6-only environment and then analyze the network traffic they generate to understand supported IPv6 features, IPv6 address resolution, traffic prevalence, and contacted destinations. Additionally, we evaluate privacy and security of their IPv6 implementations, including the use of IPv6 privacy extensions and the services exposed over IPv6.

We discover that in an IPv6-only network, 63.4% of devices support IPv6 traffic, 53.8% assign at least one IPv6 address, 23.7% initiate AAAA DNS queries in IPv6, and 20.4% transmit data to an Internet destination over IPv6. However, only 8.6% remain functional, indicating that typical IoT home deployments are not yet ready for IPv6 networks. A significant portion (16.1%) of devices still use predictable global IPv6 addresses containing MAC addresses, creating potential for user tracking. This contrasts with devices such as laptops and smartphones, which generally have full IPv6 support. Overall, our study sheds light on the current state of IPv6 adoption in smart homes and suggests a need for better alignment with best practices for functionality, privacy, and security.

Our contributions are summarized as follows:

- We conducted the first extensive study of IPv6 usage in smart homes, examining 93 diverse consumer IoT devices across seven categories from 45 manufacturers.
- We experiment with six different network configurations, using various combinations of IPv4 and IPv6 scenarios (§4).
- We determine whether these devices work in IPv6, revealing a significant gap in IPv6 readiness (§5.1).



IMC '24, November 4–6, 2024, Madrid, Spain

ACM ISBN 979-8-4007-0592-2/24/11
https://doi.org/10.1145/3646547.3688457

- We analyze the support for key IPv6 features, identifying a wide range of incomplete support and other differences (§5.2).
- We investigate how and why devices change between using IPv4 and IPv6 when moving from a single-stack network (IPv4 or IPv6) to a dual-stack network (§5.3).
- We explore privacy and security concerns linked to IPv6 in smart devices, potentially leading to user and device tracking, profiling, and targeted attacks (§5.4).

Research Artifacts. To encourage reproducibility and facilitate followup research, we have made our data and analysis artifacts publicly available at [28].

Responsible Disclosure. We responsibly disclosed the use of predictable global IPv6 addresses to the respective vendors. Details are reported in Appendix B.

2 Background

IPv6 represents the latest iteration of the Internet Protocol. Its most significant advantage over the previous version, IPv4, is the vast addressing space. This allows every device, no matter how small, to have its own IP address, making it directly accessible on the network without requiring workarounds or third-party support.

To support IPv6, an IoT device (and its destinations) must have an operating system and application software capable of supporting IPv6, be part of an IPv6-capable network, and be able to resolve destination names to IPv6 addresses. To evaluate how well an IoT device supports IPv6, we examine its support of key features of IPv6, as detailed in Table 1. It is important to notice that although IPv4 and IPv6 are both OSI layer 3 protocols that serve comparable purposes, they are typically not interoperable. However, both protocols can coexist within the same OSI layer 2 network without causing interference. Networks that support both IPv4 and IPv6 are referred to as dual-stack networks. In our research, we conduct experiments on IoT devices operating in both single-stack (either IPv4 or IPv6) and dual-stack (both IPv4 and IPv6) configurations.

3 Research Questions

The goal of this paper is to investigate IPv6 support in consumer IoT devices. At a high level, we are testing the null hypothesis that devices should function identically over IPv4 and IPv6, assuming that the devices are built in a way that is agnostic to the network layer. Specifically, we address the following research questions:

RQ1: Are consumer IoT devices ready for IPv6?
Given the widespread support for IPv6 in networking hardware, we expect IoT devices to support IPv6. We test this by exploring whether popular IoT devices use IPv6 in IPv6-only and dual-stack networks. For devices that do not work or do not use IPv6, we investigate underlying reasons, such as missing support for critical IPv6 features.

RQ2: For IoT devices that have at least partial IPv6 support, to what extent are IPv6 features supported?
When a device supports at least one IPv6 feature, it does not necessarily mean that the feature support is fully implemented or compliant with the latest RFCs. For instance, recent research shows that many devices, including IoT, do not employ IPv6 privacy extensions [43], and others lack DHCPv6 support, such as Android-based devices [51]. We address this by characterizing the IPv6 features each IoT device supports in both dual-stack and IPv6-only setups. Specifically, we assess: (*i*) IPv6 addressing capabilities, including support for address auto-configuration with SLAAC, SLAAC privacy extensions, stateless and stateful DHCPv6, duplicate address detection, and the types of IPv6 addresses used; (*ii*) their DNS capabilities and behaviors, focusing on their ability to utilize IPv6 DNS servers, send AAAA queries, receive valid responses, and the existence of AAAA records for the destinations contacted in IPv4; (*iii*) their IPv6 data transmission behaviors.

RQ3: What IP version do IoT devices use to contact their Internet destinations in a dual stack network?
In a dual-stack network, devices can communicate with remote destinations using either IPv4 or IPv6 if both are available. However, it remains unclear which IP version an IoT device will primarily choose. To determine whether devices prioritize IPv6 or IPv4, we identify the IoT devices' destination domains in dual-stack networks and compare them with those in IPv4-only and IPv6-only networks.

RQ4: Does IPv6 differ in privacy/security from IPv4?
A key feature of IPv6 is address auto-configuration with SLAAC. However, SLAAC addresses may incorporate the device's MAC address, potentially exposing IoT devices to tracking. We investigate this privacy concern by examining whether IoT devices assign EUI-64 addresses and expose them through DNS resolution and data transmissions. Another concern arises from IoT devices running services on open ports that can be exploited by external adversaries, and many devices rely on an IPv4 firewall as part of a home router/NAT—one that may not function the same with IPv6. Given this, understanding open ports and variations between v6 vs v4 is important for identifying potential security threats. Lastly, we explore whether there are differences in contacting tracking domains between IPv6 and IPv4.

4 Methodology

This section describes our experimental methodology (Figure 1) which maps our research questions to experiments and analyses.

4.1 Testbed

We built our testbed Mon(IoT)r Lab to mirror a typical home network configuration, where a gateway router sits between the LAN and the Internet, and all IoT devices are connected to the LAN.

Router. Our router is a custom-built Linux system, with one network interface connected to our ISP and another connected to a LAN where all IoT devices (both Wi-Fi and wired) are connected. The router receives IPv4 connectivity from our ISP, shared with the IoT devices via NAT, where each device is assigned a private IP address by a DHCPv4 server. Our ISP does not support IPv6 natively, so IPv6 connectivity is enabled by a Hurricane Electric IPv6-over-IPv4 tunnel [14], shared with the IoT devices in a routed configuration, where the LAN is managed by the router. To provide DHCPv4, DHCPv6, SLAAC, and RDNSS, we use *dnsmasq*, a common choice in commercial routers (*e.g.,* ones based on OpenWRT). Network traffic from all devices in the LAN is captured using *tcpdump*. For DNS servers, we use the public IPv4 and IPv6 DNS servers provided by Google, given their popularity and reliability.

IPv6 Feature (RFC)	Description
IPv6 Address (RFC 4291 [11])	A 128-bit address consisting of a network and an interface identifier. Global Unicast Addresses (GUAs) are globally routable, Unique Local Addresses (ULAs) are used in private networks, and Link-Local Addresses (LLAs) are restricted to a single link.
Neighbor Discovery Protocol (NDP) (RFC 4861 [47])	A protocol for discovering other nodes, determining their addresses, supporting address self-assignment (with SLAAC), and ensuring address uniqueness (DAD), among other functions.
Stateless Address Autoconfiguration (SLAAC) (RFC 4862 [35], RFC 8504 [5])	Built on top of NDP, allows devices to self-configure an IPv6 address without a server. Without privacy extensions, SLAAC uses the EUI-64 format when self-configuring IPv6 addresses.
Extended Unique Identifier 64 (EUI-64) (RFC 4291 [11])	Used to form the interface identifier in IPv6 addresses from a 48-bit MAC address, creating a 64-bit EUI-64 format, which can pose privacy concerns due to its traceability.
SLAAC Privacy Extensions (RFC 4941 [34], RFC 7217 [16], RFC 8981 [17])	Modifies SLAAC to generate temporary, randomized IPv6 addresses instead of fixed, predictable EUI-64 format addresses to prevent tracking and enhance user privacy. Privacy concerns related to EUI are detailed in RFC 7721 [7] and previous research [15, 41–43, 52].
Router Advertisement-based DNS Configuration (RDNSS) (RFC 8106 [24])	Built on top of NDP, provides DNS server information, allowing IPv6 nodes to obtain DNS information independently of DHCPv6.
Dynamic Host Configuration Protocol version 6 (DHCPv6) (RFC 8415 [32])	Configures IPv6 hosts with necessary network information, including addresses and DNS settings, optionally used alongside SLAAC. If DHCPv6 is configured to assign IPv6 addresses, we refer to it as *stateful* DHCPv6; if not, we refer to it as *stateless* DHCPv6.
Duplicate Address Detection (DAD) (RFC 4862 [35])	Built on top of NDP, ensures that an IPv6 address is unique before it is assigned to an interface.
DNS in IPv6 and AAAA Queries (RFC 3596 [49])	Provides methods for IPv6 nodes to obtain DNS information and resolve AAAA records (the IPv6 equivalent of A records in IPv4 DNS), which map domain names to IPv6 addresses.

Table 1: Summary of the IPv6 features we consider in this paper.

IoT Devices. Our testbed includes 93 IP-based IoT devices, across seven categories and 45 manufacturers. We acquired these devices on popular US stores, selecting them based on their availability and popularity, as indicated by their ranking on retail sites like Amazon.com. To ensure diversity, we included a range of device categories, manufacturers, and generations. The list of devices and their categories can be found in Table 10 (Appendix C).

Functionality Test. Our experiments rely on the ability to verify whether an IoT device is functional. We define that a device is considered functional if its primary function operates as expected during testing, following a similar approach as done in [30]. The primary functions we tested are: (*i*) *toggling state via the companion app* (*e.g.*, on/off and open/close), for most home automation devices, appliances, and smart hubs (toggle a hub-controlled device); (*ii*) *streaming camera feed to the companion app*, for all camera devices; (*iii*) *streaming YouTube*, for all TV/Entertainment devices, except for the Nintendo Switch, where we test the online store; (*iv*) *answering "How is the weather in XXX tomorrow?"*, for devices with a voice assistant, such as smart speakers and the smart fridge; (*v*) *sensor readings from the companion app*, for devices with readable sensors, such as medical devices and certain home automation devices.

We run companion apps on a Google Pixel 7 and an iPhone X when required for the tests. These phones are connected to a different network than the IoT devices, ensuring communication occurs over the Internet rather than locally. For devices that support *only* local network control, we connect the phones to the same network. Bluetooth is disabled to ensure that communication strictly occurs over the IP network. We also update all IoT devices and their companion apps to the latest versions and manually verify that all devices pass our functionality test over IPv4.

4.2 Connectivity Experiments

To address our research questions, we run several connectivity experiments to explore how IoT devices respond under various

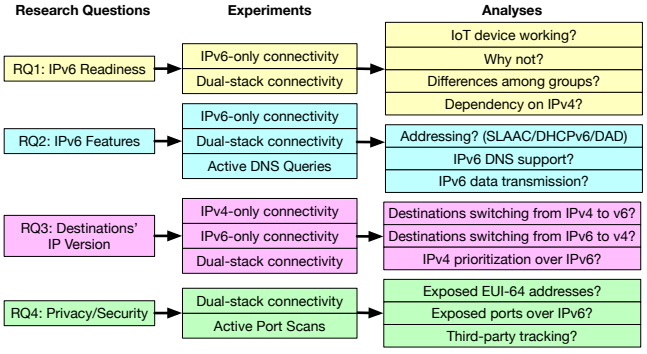


Figure 1: Methodology overview.

IPv4 and IPv6 configurations. For each experiment, we configure the network as specified, reboot all devices, allow at least one hour for them to boot, configure themselves, and register with their cloud services (empirically validated to ensure all devices restore their network connectivity), and then we perform a functionality test on each device. We conducted all connectivity experiments from April 5th 2024 to April 12th 2024. We list the connectivity experiments and their configurations in Table 2.

IPv4-only Experiment. In our first experiment, we enable IPv4 and disable IPv6 connectivity on our router for two purposes: (*i*) to confirm all devices' primary functions work correctly in a standard IPv4 network without malfunctions or service disruptions; (*ii*) to establish a baseline for IPv4 device behavior to compare against IPv6 experiment outcomes.

IPv6-only Experiments. We conduct IPv6-only experiments by completely disabling IPv4 and activating IPv6 in three configurations to assess device functionality in a pure IPv6 environment and the extent of IPv6 feature support. In each of IPv6-enabled experiments, we use our Google Pixel 7 and iPhone X (which support

Experiment	IPv4	SLAAC and RDNSS	Stateless DHCPv6	Stateful DHCPv6
IPv4-only	✔	✗	✗	✗
IPv6-only	✗	✔	✔	✗
IPv6-only (RDNSS-only)	✗	✔	✗	✗
IPv6-only (stateful)	✗	✔	✔	✔
Dual-stack	✔	✔	✔	✗
Dual-stack (stateful)	✔	✔	✔	✔

Table 2: Connectivity experiments configuration.

IPv6) to verify the IPv6 network is configured correctly.

In the initial (baseline) configuration, we enable SLAAC for IPv6 addressing, as mandated by RFC 8504 [5], and both stateless DHCPv6 and RDNSS for DNS server configuration, a common setup in home IPv6 networks, as well as recommended by RFC 8504 to ensure interoperability and are widely supported by major OSes and software suites [51].

To explore less common IPv6 configurations, we perform two variations: a RDNSS-only experiment, and a stateful variation. In the RDNSS-only variation, we modify the baseline configuration by disabling support for stateless DHCPv6, so that DNS server information is only sent to the IoT devices using RDNSS instead of both. This variation is useful to understand what devices are not compatible with RDNSS. In the stateful variation, we modify the baseline configuration by enabling support for stateful DHCPv6, so that our router assigns IPv6 addresses to each IoT device. This experiment helps us understand which addressing methods would IoT devices support and prefer.

Dual-stack Experiments. We perform dual-stack experiments by enabling both IPv4 and IPv6 connectivity. These experiments simulate a more typical home network, which rarely operates on IPv6-only, and allow devices that only partially support IPv6 to demonstrate this capability. We conduct dual-stack experiments in two configurations. The first (baseline) configuration mirrors the baseline setup of the IPv6-only experiments (*i.e.,* SLAAC, DHCPv6, and RDNSS), and the second mirrors the stateful variation, adding stateful DHCPv6 support to the baseline configuration.

4.3 Active Experiments

We perform two active experiments to reveal additional IPv6 support insights and related security implications.

Active DNS Queries. While an IoT device may be fully capable of supporting IPv6, its functionality could still be limited if its destinations do not resolve to an IPv6 address. We analyze the IPv6 support of IoT device destination domains by querying DNS AAAA records for all domains used by the IoT devices, collected from DNS and TLS handshake data across all connectivity experiments.

Active Port Scans. Active port scans provide information about open ports and services on devices in our testbed, beyond those observed passively. Informed by previous work [1, 15, 27], we perform port scans using *nmap* [29]. We extract the latest IPv6 addresses of each device by sending an ICMPv6 Echo Request to the *all-nodes multicast address* and then collect IPv6 addresses from the IPv6 neighbor table on the router. We do this because, due to the use of privacy extensions, self-assigned IPv6 addresses may be temporary. As done in prior work, we run TCP SYN scans on all ports (1-65535), and focus UDP scans on commonly used ports (1-1024) due to the slower nature of UDP scanning compared to TCP.

5 Results

This section presents the results of our study, with each subsection corresponding to a specific research question.

5.1 IPv6 Readiness

In this section, we address RQ1: *Are consumer IoT devices ready for IPv6?* We assess the functionality of IoT devices within our testbed under IPv6-only and dual-stack network configurations to determine their readiness and utilization of IPv6 features. Our analysis begins by evaluating which devices remain functional in IPv6-only settings and identifying the critical IPv6 features that non-functional devices lack. Then, we examine trends across different device categories to understand any patterns in IPv6 support. The section concludes with a comparative analysis between IPv6-only and dual-stack scenarios.

5.1.1 Functional Analysis in IPv6-only Network. In our three IPv6-only configurations, only eight out of 93 devices remain functional, including five smart speakers and three smart TVs, as indicated in Figure 2 and Table 3. These devices successfully perform primary functions such as responding to voice commands and streaming content. However, the vast majority (85 devices) do not function without IPv4, showing a considerable gap in IPv6 readiness.

5.1.2 Unsupported IPv6 Features. In this section we investigate why so many devices are not IPv6-ready by analyzing the specific IPv6 features that non-functional devices fail to support, which limits their operability in IPv6-only environments. We present our results in Figure 2 and Table 3.

Neighbor Discovery Protocol (NDP) Traffic. NDP is an essential protocol to support IPv6 operations, since it is responsible for many low-level operations, including discovering nodes, resolving their addresses (similar to ARP in IPv4), and some optional features such as SLAAC for IPv6 self-assignment. Our results show that 59 out of 93 devices generate NDP traffic. Therefore, the primary reason for most devices not being functional in an IPv6-only network is their lack of support or use of NDP, affecting 36.6% (34) of the devices. Given that most OSes and network stacks can handle IPv6 [51], the absence of NDP traffic on 34 devices may be due to their device configuration or design choices.

IPv6 Address Assignment. Despite 59 devices generating NDP traffic, only 51 have at least one assigned IPv6 address, leaving eight without an address. These eight addresses-less devices use the unspecified address "::" to multicast NDP messages without configuring an IPv6 address.

DNS AAAA Queries. Among the 51 devices that have an IPv6 address, only 22 devices generate DNS AAAA queries in IPv6, with just 19 devices receiving positive AAAA DNS responses. A possible explanation for this is that only 27 devices generate Global Unique Addresses, suggesting that 24 devices lack IPv6 DNS support due to the absence of a global address, and five devices do not support IPv6 DNS despite having a global address.

IPv6 Internet Data Communication. We find that 19 devices transmit data over the global IPv6 network (the same ones that

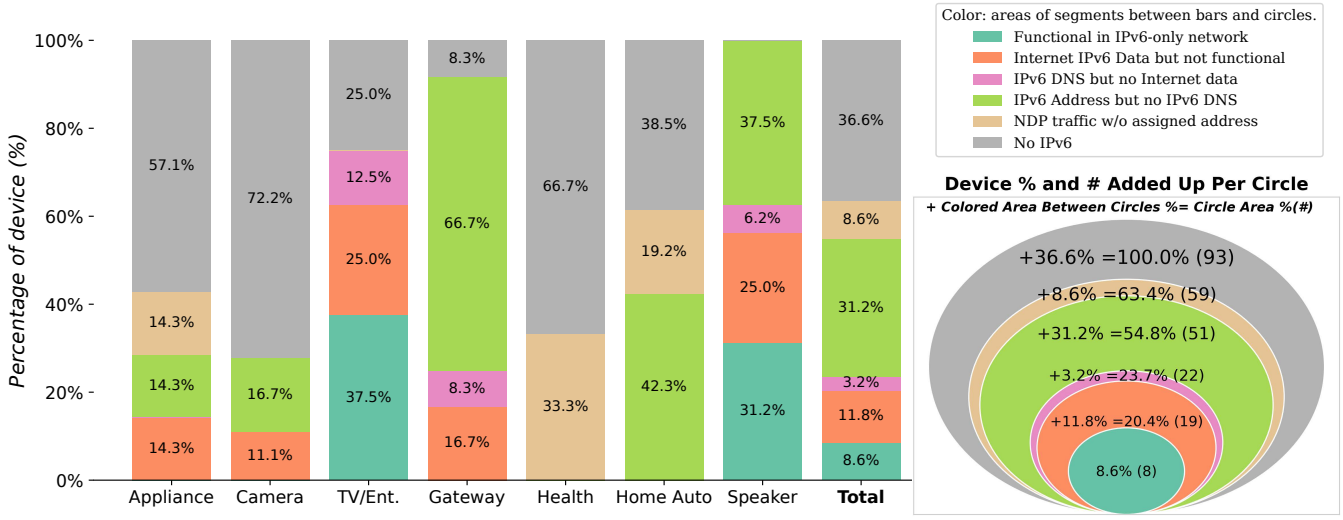


Figure 2: *IPv6-only Experiments:* This figure and Table 3 display the IPv6 functionality of IoT devices, detailing percentages of devices that are fully functional, communicate over IPv6, support IPv6 DNS, assign an IPv6 address, generate NDP traffic, or lack IPv6 traffic. The bottom right aggregates percentages and total counts from functional to non-functional devices. Circles from outermost to innermost match rows ① to ⑥ in Table 3, with colors indicating corresponding areas and rows.

	Appliance	Camera	TV/Ent.	Gateway	Health	Home Auto	Speaker	Total	%
① Total # of Device	7	18	8	12	6	26	16	**93**	100%
- No IPv6	4	13	2	1	4	10	0	34	36.6%
② IPv6 NDP Traffic	3	5	6	11	2	16	16	**59**	63.4%
- NDP Traffic No Addr	1	0	0	0	2	5	0	8	8.6%
③ IPv6 Address	2	5	6	11	0	11	16	**51**	54.8%
○ Global Unique Address	1	2	6	5	0	3	10	27	29.0%
- IPv6 Address but No IPv6 DNS	1	3	0	8	0	11	6	29	31.2%
④ IPv6 DNS (AAAA Req)	1	2	6	3	0	0	10	**22**	23.7%
○ AAAA DNS Response	1	2	6	0	0	0	10	19	20.4%
- IPv6 DNS but No Data	0	0	0	3	0	0	0	3	3.2%
⑤ Internet TCP/UDP Data Comm.	1	2	5	2	0	0	9	**19**	20.4%
- IPv6 Data but Not Func	1	2	2	2	0	0	4	11	11.8%
⑥ Functional over IPv6-only	0	0	3	0	0	0	5	**8**	8.6%

Table 3: *IPv6-only experiments:* This table shows the support of IPv6-related features (# and % of devices) per category. The rows from ① to ⑥ correspond to the circles (from outer to inner) in Figure 2. The colored rows correspond to the colored areas in Figure 2.

	Appliance	Camera	TV/Ent.	Gateway	Health	Home Auto	Speaker	Total	%
② IPv6 NDP Traffic	0	0	0	-1	0	0	0	-1	-1.1%
③ IPv6 Address	0	0	0	-1	+1	+2	0	+2	+2.2%
○ Global Unique Address	0	0	0	-1	+1	+1	+2	+3	+3.2%
④ AAAA DNS Request	0	+5	+1	+3	0	+1	+5	+15	+16.1%
○ AAAA DNS Response	0	+3	+1	+2	0	+1	+5	+12	+12.9%
Internet TCP/UDP Data Comm.	0	0	+1	0	0	0	+2	+3	+3.2%

Table 4: *Dual-stack experiments:* This table shows the differences of IPv6-related feature support (# of devices) per category compared to *IPv6-only experiments*. Positive number and percentage indicate more devices support the feature in *dual-stack experiments* than in *IPv6-only experiments*. Negatives indicate the opposite.

receive proper DNS responses). This suggests that the three devices that generate DNS queries, but lack Internet data communication over IPv6, are non-functional due to a lack of a proper DNS AAAA record response. As mentioned earlier, only eight devices are functional in an IPv6-only network, which means that 11 devices, despite supporting all the features discussed above, are still non-functional. This indicates that their functionality may still depend on IPv4.

5.1.3 Case Study: Non-Functional Devices Supporting All IPv6 Features. To understand why 11 devices support all IPv6 features yet remain non-functional in an IPv6-only network, we analyzed the destinations these devices contact exclusively over IPv4. Specifically, we focus on destinations that are only contacted via IPv4 across all connectivity experiments (§4.2) and check if they have valid AAAA records from our active DNS query experiments (§4.3). We also reference previous research [30] to determine whether these domains are essential for the devices' primary functionality. We find that these devices likely fail in an IPv6-only network due to their reliance on IPv4-only domains. For example, Amazon devices (*e.g.,* Echo Show 5 and 8, Fire TV, and Echo Plus) connect exclusively via IPv4 to first-party domains like *api.amazon.com* and *unagi-na.amazon.com*, which lack valid AAAA records. Previous research [30] confirms that these domains are essential for the functionality of Echo and Fire TV devices. We found similar behavior (with different domains that are required for functionality) for Samsung/SmartThings devices (Aeotec Hub, Fridge, and TV), the HomePod Mini, the Nest Camera, and the Nest Doorbell. The Smartlife Matter Hub connects to a required domain, *a2.tuyaus.com*, over IPv4 only. This domain ironically has valid AAAA records, but they are never queried by the device over IPv6.

In summary, our investigation reveals that the most of the failures over IPv6—when devices fully support IPv6 features—are due to a failure to provide and/or use IPv6 DNS entries.

5.1.4 Category-Wise Analysis. Our analysis of IPv6 support across various device categories reveals significant disparities in capability, as detailed in Figure 2 and Table 3. Notably, smart speakers and TVs are the only categories where devices function in an IPv6-only network, likely because these devices operate on advanced OSes such as Darwin and Android, similar to those used in iPhones and Android phones, which inherently support IPv6.

In contrast, smart appliances, smart cameras, and health devices exhibit the lowest levels of IPv6 support, with only a few generating NDP traffic. This may be explained by the fact that these devices are typically simpler embedded systems with specialized functions. Interestingly, while no smart gateways or home automation devices are functional under IPv6-only conditions, a significant portion of them generate NDP traffic and manage IPv6 address assignment due to their use of local IPv6-based network protocols like HomeKit [3] and Matter [6].

These results reveal a gap in IPv6 support across different device categories. While some devices, particularly smart TVs and smart speakers, are largely prepared for IPv6, other smart devices lag behind, suggesting areas for improvement in the transition to IPv6.

5.1.5 Manufacturer Analysis. The smart devices in our testbed are from 45 manufacturers, with Google and Amazon being the most prevalent. While we observe that devices from Google, Samsung/SmartThings, and Amazon generally have the highest support for IPv6 features, only devices from Google (6), Apple (1), and Meta (1) are functional in an IPv6-only network.

In §5.2.4, we provide a more detailed analysis of the results grouped by manufacturer, platform, and OS. Additionally, Table 12 in Appendix D presents the results based on the purchase year to understand changes in IPv6 support over time. However, our findings indicate that the manufacturer and device category have a more significant impact on IPv6 support than the purchase year.

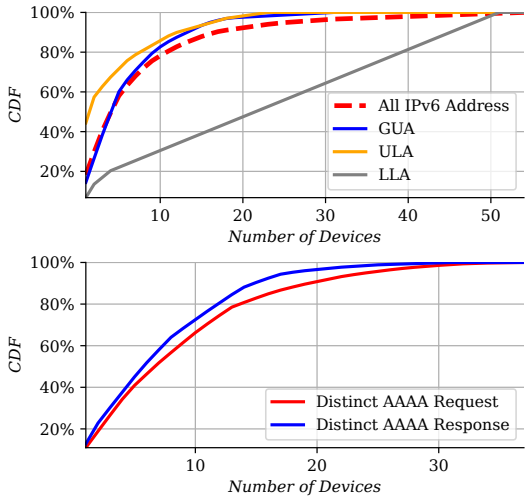


Figure 3: Cumulative Distribution Function (CDF) plot: IPv6 addresses (top) and DNS AAAA queries (bottom).

5.1.6 IPv6-only vs. Dual-Stack Experiments. The comparison between IPv6-only and dual-stack experiments reveals some differences in IPv6 feature support, as detailed in Table 4. Notably, the presence of IPv4 in dual-stack setups led to a marked increase in DNS AAAA queries, with 15 more devices performing these queries compared to the IPv6-only setup. This can be partially explained by the fact some features require IPv4 to function. For example, many IoT devices choose to send AAAA queries exclusively over IPv4 (discussed below in §5.2). Additionally, there was an improvement in IPv6 address assignment, with two more devices assigning IPv6 addresses in the dual-stack experiments. The number of devices transmitting Internet data over IPv6 also increased by three in the dual-stack setup. However, one fewer device produced NDP traffic in the dual-stack experiments, suggesting that some devices might skip certain IPv6 features when they have an IPv4 option. Overall, our results indicate better IPv6 support in smart devices when IPv4 fallback is available.

5.2 Characterization of IPv6 Features

In this section, we address RQ2: *For IoT devices that have at least partial IPv6 support, to what extent are IPv6 features supported?* Specifically, we characterize the support of IPv6 features for the 53 IoT devices in our testbed that have at least one IPv6 address assigned. Additionally, we assess their capabilities in utilizing IPv6 DNS and establishing global communication over IPv6.

5.2.1 IPv6 Address Assignment. We first characterize the support for different methods of IPv6 address assignment.

SLAAC and Privacy Extensions. All 54 devices with an IPv6 address assigned support SLAAC, as required by RFC 4862 [35]. However, as mentioned earlier, it is essential for smart devices to use SLAAC privacy extensions (RFC 8981 [17]) to prevent exposure

	Appliance	Camera	TV/Ent.	Gateway	Health	Home Auto	Speaker	Total	%
Total # of Device	7	18	8	12	6	26	16	93	
IPv6 Addr: Number of Devices Supporting IPv6 Addressing									
IPv6 Addr	2	5	6	11	1	13	16	54	58.1%
Stateful DHCPv6	1	0	2	2	0	6	1	12	12.9%
GUA	1	2	6	5	1	4	12	31	33.3%
ULA	1	2	2	5	1	5	7	23	24.7%
LLA	2	5	6	10	0	11	16	51	54.9%
EUI-64 Addr	1	2	3	7	0	8	10	31	33.3%
DNS in IPv6: Number of Devices Support IPv6 DNS Features									
DNS Over IPv6	1	2	6	3	0	0	10	22	23.7%
A-only Request in IPv6	1	1	5	3	0	0	9	19	20.4%
AAAA Request (v4 or v6)	1	7	7	6	0	1	15	37	39.8%
IPv4-only AAAA Request	1	7	5	5	0	1	14	33	35.5%
AAAA Response	1	5	7	2	0	1	15	31	33.3%
AAAA Req No AAAA Res	1	7	6	6	0	1	13	34	36.6%
Stateless DHCPv6	1	0	3	3	0	6	3	16	17.2%
IPv6 Data Trans: Number of Devices Performing Data Transmission over IPv6									
IPv6 TCP/UDP Trans	1	2	6	6	0	3	11	29	31.2%
Internet Trans	1	2	6	3	0	0	11	23	24.7%
Local Trans	1	2	5	5	0	3	5	21	22.6%

Table 5: *IPv6-only and dual-stack experiments:* the support of IPv6-related features (# and % of device) per category.

	Appliance	Camera	TV/Ent.	Gateway	Health	Home Auto	Speaker	Total
Total # of Device	7	18	8	12	6	26	16	93
IPv6 Addressing (# of Addresses)								
# of IPv6 Addr	19	105	71	150	2	23	314	684
# of GUA Addr	12	74	55	119	1	5	190	456
# of ULA Addr	4	26	6	20	1	7	105	169
# of LLA Addr	3	5	10	11	0	11	19	59
IPv6 DNS (# of Distinct Query Names)								
# of AAAA DNS Req	52	49	390	67	0	6	511	1077
# of A-only Req in IPv6	12	1	16	13	0	0	72	114
# of IPv4-only AAAA Req	4	39	141	22	0	8	120	334
# of AAAA DNS Res	12	26	238	5	0	1	249	531
Fraction of IPv6 Internet Data Transmission in Dual-stack								
IPv6 Fraction of Total Volume (%)	1.2%	3.3%	34.4%	0.0%	0.0%	0.0%	23.3%	22.0%

Table 6: *IPv6-only and dual-stack experiments:* number of IPv6 addresses and DNS queries. *Dual-stack experiments:* fraction of IPv6 Internet data volume over total volume.

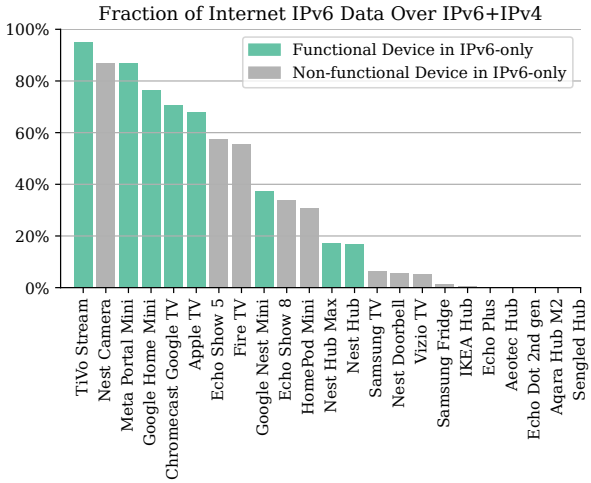


Figure 4: Bar chart showing the fraction of global Internet IPv6 data volume over total Internet data volume.

of their MAC address over the Internet. Of those 54 devices supporting SLAAC, 31 devices generate predictable EUI-64 addresses without using SLAAC privacy extensions (see Table 5), with 15 devices using EUI-64 global unique addresses (GUA), which can be used for tracking over the Internet. We further discuss the privacy implications of using such addresses in §5.4.

Stateful Addressing. Table 5 shows that only 12 devices support stateful DHCPv6 addressing. Of these, only 4 devices actually use their stateful DHCPv6 addresses, though these are not their primary addresses: SmartThings Hub, HomePod Mini, SmartThings Aeotec Hub, Samsung Fridge. This suggests that while stateful DHCPv6 is available, it is not widely utilized, possibly because many IoT home devices are not designed for environments where stateful DHCPv6's granular control is necessary (*e.g.,* enterprises).

IPv6 DNS Configuration. IPv6 DNS Configuration (either stateless DHCPv6 or RDNSS) is supported by 22 devices, evidenced by their generation of IPv6 DNS traffic to the DNS server we configured in our testbed. However, as shown in Table 5, only 16 devices actively send DHCPv6 requests for DNS server information, demonstrating their support for stateless DHCPv6. Notably, 13 Android-based devices do not support stateless DHCPv6 due to Android's

Category	Device #	Domain #	AAAA Res. #	AAAA Res. %
Functional devices in IPv6-only network				
Speaker	5	277	195	70.4%
TV/Ent.	3	451	338	74.9%
Total	8	728	533	**73.2%**
Non-functional devices in IPv6-only network				
Appliance	7	75	16	21.3%
Camera	18	157	44	28.0%
TV/Ent.	5	318	127	39.9%
Gateway	12	100	17	17.0%
Health	6	8	6	75.0%
Home Auto	26	108	23	21.3%
Speaker	11	578	185	32.0%
Total	85	1344	418	**31.1%**

Manufacturer/ Platform	Device #	Domain #	AAAA Res. #	AAAA Res. %
Functional devices in IPv6-only network				
Meta	1	44	39	88.6%
Google	5	380	291	76.6%
Apple	1	165	106	64.2%
Tivo	1	139	97	69.8%
Non-functional devices in IPv6-only network (# of device >=3)				
Samsung/SmartThings	4	200	52	26.0%
Google	3	63	24	38.1%
Ring	4	33	10	30.3%
Amazon	13	483	147	30.4%
TP-Link	5	29	3	10.3%
Tuya	6	36	11	30.6%
Withings	3	3	3	100.0%
Aidot	3	7	0	0.0%
Meross	3	21	4	19.0%

Table 7: DNS AAAA readiness across IPv4&v6 destinations, grouped by device category. The top table shows the number of devices, distinct domains, domains with AAAA records, and their percentage.The bottom table presents the same data grouped by manufacturer or platform.

incomplete IPv6 implementation [18], while 7 devices send DHCPv6 requests but do not generate DNS traffic over IPv6. To identify devices that do not support RDNSS without stateless DHCPv6, we compare results from the baseline IPv6-only experiment and the RDNSS-only variation. We observe that only one device, Vizio TV, does not generate DNS traffic in the RDNSS-only experiment, as it did in the baseline experiment, which has both RDNSS and DHCPv6. This suggests that it may not support RDNSS exclusively and may require DHCPv6 to obtain DNS server information.

IPv6 Address Types. We present the number of devices that use various types of IPv6 addresses in Table 5: Of the 54 devices with at least one assigned IPv6 address, 31 have at least one global unique address (GUA), 23 have at least one unique local address (ULA), and 51 have at least one link-local address (LLA). We observed that 25 out of 54 devices have at least one unused IPv6 address assigned via NDP but never used for any traffic. These unused addresses are not considered active IPv6 addresses in our analysis. For example, three devices use only their GUAs and ULAs, not LLAs, which explains why 54 devices have IPv6 addresses but only 51 have LLAs in the table. Similar to the support for IPv4 address assignment and NDP as discussed in §5.1, smart speakers and TVs exhibit high support for GUAs. Conversely, home automation devices show low support for GUAs but high support for ULAs, due to their use of local network protocols and services such as Matter [6] and HomeKit [3].

Figure 3 (top) depicts the CDF of the number of IPv6 addresses per device. We see that, out of 51 devices with at least one assigned LLAs, 47 have only one LLA. Among these, the Samsung Fridge, Samsung TV, HomePod Mini, and Apple TV are the only devices that rotate their LLAs during our experiment. Additionally, 10 of the devices account for 80% of the GUAs and 90% of the ULAs generated in our experiments. This high frequency of address generation and/or rotation is predominantly observed in devices from Samsung/SmartThings, Google, and Apple (details in Appendix Table 13), likely due to their network configurations which may prompt address rotation in response to network issues within an IPv6-only setting.

Duplicate Address Detection (DAD). RFC 4862 mandates that all unicast addresses be verified using DAD before being assigned to an interface. Nevertheless, our experiments reveal that 18 devices did not perform DAD for at least one of their IPv6 addresses before using it, suggesting non-compliance with the RFC. Specifically, 20 GUAs, 7 ULAs, and 8 LLAs are assigned without performing DAD. Notably, 4 devices (2 Aqara Hubs and 2 home automation devices) do not perform DAD for any of their IPv6 addresses, which all follow the EUI-64 format. These four devices are also the only ones in our study that skip DAD for their EUI-64 formatted addresses, suggesting that these devices may not support DAD at all. RFC 4862 acknowledges that some implementations may only conduct DAD for the link-local address and omit it for global addresses that use the same interface identifier as the LLA. Some devices in our testbed might follow this practice. However, since 2007, the RFC [35] stipulates that such approach is not recommended, and new implementations must not omit DAD for global addresses.

5.2.2 IPv6 DNS Support. As discussed in §5.1, a clear correlation exists between receiving valid DNS AAAA queries and the ability of devices to communicate globally in IPv6-only experiments. Additionally, the presence of IPv4 in dual-stack experiments appears to facilitate better IPv6 DNS resolution, leading to increased Internet IPv6 traffic (§5.1.6). This motivates a deeper analysis to understand how IoT devices use IPv6 DNS, which we outline below.

DNS Query and Response. Our results, detailed in Table 5 and Table 6, show that 37 devices sent a total of 1077 distinct DNS AAAA queries during our experiments. Of these, 22 devices sent 870 distinct queries in IPv6, while 33 devices used IPv4 for 334 distinct AAAA queries, indicating a selective adoption of IPv6 DNS servers alongside IPv4 ones. This suggests that despite the fact that some devices are capable of supporting AAAA records, they appear unable to use IPv6 resolvers for resolving these records, causing a lack of IPv6 DNS support in an IPv6-only network. In the dual-stack experiments, these devices are more likely to send and receive successful DNS AAAA messages, which increases the number of devices transmitting data over IPv6. Additionally, we observe that 19 devices issued only A queries for certain domains, even in an IPv6-only network, totaling 114 distinct queries, which suggests limitations in their support for AAAA queries.

We observe that 31 devices received AAAA DNS responses for 531 (49%) distinct queries (using either IPv4 or IPv6 DNS), 19 devices received 471 (54%) distinct AAAA DNS responses in IPv6, and the rest of AAAA queries receive responses with "`no such name`" error and/or SOA records, suggesting that these domains do not

have AAAA records. Notably, 34 devices have at least one AAAA query that does not receive a response. Beyond AAAA records, we find that five devices (Android or iOS/tvOS-based) also queried for HTTPS records and two Apple devices queried for SVCB (Service Binding) records in IPv6, indicating support for HTTP/3.

The CDF of AAAA queries per device, as depicted in Figure 3 (bottom), reveals that 10 devices are responsible for 70% of the distinct DNS queries, with five devices accounting for almost half. This is primarily because complex devices such as smart TVs and hubs support a wide range of different services and applications that require DNS resolution, while simpler devices like home automation devices and appliances have more limited functionality and contact fewer domains. This observation is also consistent with the results in IPv4 from prior work [21, 38], where a few complex devices generate the majority of DNS queries and traffic.

Smart speakers and TVs exhibit the highest support for DNS in IPv6, with 10 and 6 devices respectively, consistent with our earlier findings. Conversely, devices from other categories demonstrate minimal, if any, support for DNS in IPv6. For example, only 3 out of 10 smart gateways with an IPv6 address support DNS in IPv6. If we consider manufacturer, Google (7 out of 8) and Samsung/SmartThings (4 out of 4) have the highest fraction of devices that support DNS in IPv6 among manufacturer with more than three devices (see §5.2.4).

Destination DNS AAAA Readiness. Due to the limited support for IPv6 DNS across the majority of devices, passive monitoring alone does not provide a complete view of the DNS AAAA readiness of their destination domains. Therefore, we investigate the DNS AAAA readiness by performing active DNS queries (§4.3), *i.e.,* we query the DNS AAAA records for all destination domains utilized by the devices. We extract these domain names from the DNS queries and TLS handshake data, excluding any local domains. Table 7 presents the DNS AAAA readiness of destination domains, grouped by device category and manufacturer/platform. Each one is divided into two main sections: one for IPv6-only functional devices and another for non-functional devices.

Among functional devices, 533 out of 728 domains (73.2%) offer AAAA records, indicating high AAAA DNS compatibility. In contrast, non-functional devices show lower compatibility, with only 418 out of 1344 domains (31.1%) being AAAA-ready. These findings highlight a disparity in DNS AAAA readiness between functional and non-functional devices.

Additionally, IPv6 DNS readiness varies significantly across different device categories and manufacturers/platforms. Gateways have the lowest percentage of AAAA records (17.0%), which is surprising given their support for various IPv6 features, especially local IPv6-based services. Health devices, though small in sample size, have the highest percentage of AAAA records (75.0%) despite limited support for other IPv6 features. Half of these health devices are from Withings, whose destinations are AAAA-ready. This suggests that the IPv6 readiness issue may lie more with the devices themselves rather than their destinations. The percentage of AAAA records for Google devices varies significantly by device type, with non-functional devices showing only 38.1%—half the percentage seen in functional devices (smart speakers and TVs). Ring, owned by Amazon but manufacturing its devices separately, shows a similarly low percentage of AAAA records, like other Amazon devices. These Ring and Amazon devices may have overlapping backend infrastructure.

5.2.3 Data Transmission over IPv6. This section details the extent of TCP or UDP data transmission over IPv6, excluding DNS and DHCPv6 traffic previously discussed. As presented in Table 5, a total of 29 IoT devices have transmitted data using TCP or UDP over IPv6. Among them, 23 devices transmitted data to Internet destinations, while 21 transmitted data to local destinations. Category-wise, 11 out of 16 speakers, as well as 6 devices each from the TV/Entertainment and gateway categories, transmitted data to remote destinations. Conversely, devices lacking Internet data transmission but active in local transmissions predominantly include gateways and home automation devices, aligning with expectations due to their reliance on local IPv6 network services like Matter.

For dual-stack experiments, we show the fraction of Internet data transmitted over IPv6 compared to the total Internet data volume in Table 6. TV/Entertainment and speakers transmit a considerable fraction of data over IPv6, while other device categories show the significantly lower fractions. The detailed results are presented in Figure 4. Remarkably, three devices transmit over 80% of their Internet data via IPv6, yet more than half of the devices with global IPv6 data transmit less than 20% over IPv6, mostly relying on IPv4. This suggests that IPv6 is not the primary choice for their data transmission. Interestingly, one device that is non-functional in IPv6-only (*i.e.,* the Nest Camera) still manages to transmit over 80% of its Internet traffic via IPv6 in dual-stack. As we mentioned in §5.1.3, this is likely because a few domains essential for its primary functionality lack IPv6 support. Consequently, even though a significant portion of the Nest Camera's communication occurs over IPv6 and its destinations support IPv6, the device remains non-functional in an IPv6-only network due to incomplete IPv6 support across all necessary destinations. Conversely, two devices (Nest Hub Max and Nest Hub) that are functional in IPv6-only transmit less than 20% of their traffic via IPv6 in dual-stack. This is likely because these Google's smart displays, running on a customized Fuchsia OS, offer a wide array of services and applications, and the non-Linux-based OS may not fully implement IPv6. While their primary function we tested, Google Assistant, operates effectively in an IPv6-only network, other services and third-party apps available on these devices may not be fully compatible with IPv6.

Overall, while most IoT devices require IPv4 to function, it is promising that some devices primarily use IPv6 for Internet communication in dual-stack networks. This indicates a significant commitment by their vendors to IPv6 support, suggesting the potential for greater adoption in the future.

5.2.4 IPv6 Features by Manufacturer, Platform, OS, and Age. **Manufacturer and Platform.** Our experimental setup comprises devices from 45 manufacturers. Table 8 categorizes the IPv6 capability of devices based on their manufacturers, showing only manufacturers that contributed more than three devices to our testbed. Devices from Google, Amazon, and Samsung/SmartThings show good IPv6 feature support. Notably, all Samsung/SmartThings devices and most Google devices support IPv6 addressing, DNS, and data transmission, despite being non-functional in an IPv6-only network. The hardware/firmware platform also plays a crucial role

		Manufacturer/Platform									OS				
	Total	Google	Amazon	Ring	SmartThings /Samsung	Tuya	TPLink	Aidot	Meross	Withings	Tizen	FireOS (Android)	Android -based	Fuchsia	iOS/tvOS
Device #	93	8	13	4	4	6	5	3	3	3	2	11	5	2	2
Functional over IPv6-only	8	5	0	0	0	0	0	0	0	0	0	0	5	2	1
IPv6 Address	54	8	11	0	4	5	2	3	2	0	2	11	5	2	2
Stateful DHCPv6	12	1	0	0	4	0	2	0	1	0	2	0	0	0	2
GUA	31	7	7	0	4	3	2	0	1	0	2	7	5	2	2
ULA	23	6	1	0	4	4	2	0	1	0	2	1	3	2	2
LLA	51	8	11	0	4	2	2	3	2	0	2	11	5	2	2
GUA EUI-64 Address	15	3	5	0	3	1	1	0	1	0	1	5	2	0	0
DNS over IPv6	22	7	5	0	4	1	0	0	0	0	2	5	5	2	2
A-only Req in IPv6	19	5	4	0	4	1	0	0	0	0	2	4	4	2	2
AAAA Req (v4 or v6)	37	8	10	1	4	1	0	0	0	0	2	10	5	2	2
IPv4-only AAAA Req	33	8	9	1	3	1	0	0	0	0	2	9	4	2	1
EUI-64 Addr DNS Req	8	3	2	0	3	0	0	0	0	0	1	2	2	0	0
AAAA Response	31	8	10	0	2	0	0	0	0	0	2	10	5	2	2
AAAA Req No AAAA Res	34	7	9	1	4	1	0	0	0	0	2	9	4	2	2
Stateless DHCPv6	16	3	0	0	4	0	2	0	1	0	2	0	0	2	2
IPv6 TCP/UDP Trans	29	7	6	0	4	1	2	0	1	0	2	6	5	2	2
Internet Trans	23	7	6	0	3	1	0	0	0	0	2	6	5	2	2
Local Data Trans	21	7	0	0	4	1	2	0	1	0	2	0	4	2	2
EUI-64 Internet Trans	5	1	4	0	0	0	0	0	0	0	0	4	0	0	0

Table 8: *IPv6-only and dual-stack experiments:* the support of IPv6-related features (# of devices) per manufacturer or platform(# of device >= 3) and OS (# of devices >=2). This table is comparable to Table 5.

in determining the IPv6 support. For example, many manufacturers use Tuya's IoT solutions to develop their devices, which we can identify via their companion apps. We found that such Tuya-supported devices exhibit similar levels of limited IPv6 support. Additionally, we observe that Ring devices, a subsidiary of Amazon, show no IPv6 support, likely because they continue to be designed separately from other Amazon devices even after the acquisition.

OS. The OSes of the devices significantly influence their IPv6 support. However, we often lack direct access to detailed OS, firmware, or hardware information for most devices, so we must rely on limited public information from manufacturer websites or companion apps. For example, we know that most of the smart TVs are based on Android or Android-based OSes, which have fully implemented IPv6 support [51]. In contrast, non-Android-based OSes such as Fuchsia OS [19] used by Nest Hubs might not have a fully supported IPv6 ecosystem. This likely explains why Nest Hubs have a lower fraction of Internet communication over IPv6 compared to Android-based devices (Figure 4), despite functioning in IPv6-only networks. An unusual example is the Amazon Echo devices, which are based on Amazon's proprietary Fire OS [2]. Despite being Android-based, these devices have poor support for IPv6 features, and none are functional in an IPv6-only network.

Age, Based on Purchase Year. Table 12 in Appendix D categorizes devices by their year of purchase to understand changes in IPv6 support over time. There is no clear trend, so we cannot conclude that newer (or older) devices inherently offer better IPv6 support. Further details are provided in Appendix D.

5.3 IP Version for Contacted Destinations

This section addresses RQ3: *What IP version do IoT devices use to contact their Internet destinations in a dual stack network?* As shown in Table 9, the 93 devices contact 2,083 destination domains, with 36.9% of destinations contacted over IPv6 and 75.0% over IPv4. Some domains appear only in specific experiments due to factors such as CDN usage or the particular functions being tested. However, when focusing on domains common to both the IPv4-only and dual-stack experiments, as well as between the IPv6-only and dual-stack experiments, most domains consistently use the same IP version.

A notable fraction of domains, however, either partially extend their communication to use both IPv6 and IPv4, or switch entirely to one IP protocol when the network transitions from IPv4-only or IPv6-only to dual-stack, indicating a preference for one over the other. This behavior suggests varying levels of support or preference for IP protocols among the devices, as discussed below. To answer RQ3, we investigate whether devices prioritize IPv6 over IPv4, or vice versa, when both options are available.

IPv4 Switching to IPv6. We check the common destination domains contacted by the devices over IPv4 in the IPv4-only network and contacted in the dual-stack. When IPv6 becomes available, we observe that 124 domains (18.2% of the common domains in both experiments) partially extend to IPv6 communication in the dual-stack setting; 37 domains (5.4%) switch exclusively to IPv6, without IPv4 communication. Category-wise, TV/Ent. and speaker devices show the highest number of domains that partially extend to IPv6 or fully switch to IPv6. This is probably due to their more robust IPv6 support and the IPv6 destination availability from large vendors compared to other device categories.

IPv6 Switching to IPv4. Conversely, when comparing the IPv6-only and dual-stack experiments, 138 common domains (59.5%) extend their IPv6 communication to IPv4, and 26 domains (11.2%) switch entirely to IPv4, eliminating any IPv6 traffic, despite the availability of IPv6 in the dual-stack configuration. This significant percentage of common domains extending to IPv4 suggests that even though smart devices and their destinations support IPv6, many still rely on (or even prefer, for certain destinations) IPv4.

IPv4 not Switching to IPv6. In the dual-stack configuration, 32 domains (2.8% of the IPv4-only domains in the dual-stack experiment) have valid AAAA records. Despite this potential for switching

	Appliance	Camera	TV/Ent.	Gateway	Health	Home Auto	Speaker	Total
Destinations contacted over IPv6 and IPv4								
# IPv6 Dest. Domain (% of Total)	10 (13.9%)	23 (8.6%)	426 (54.0%)	20 (21.5%)	0	0	290 (40.3%)	769 (36.9%)
# IPv4 Dest. Domain (% of Total)	65 (90.3%)	268 (91.4%)	457 (46.0%)	77 (78.5%)	16	121	559 (59.7%)	1563 (75.0%)
# of Dest. Domain	72	269	789	96	16	121	720	2083
IPv4 Dest. Transition to IPv6 in Dual-stack (% over common dest. between IPv4-only and dual-stack)								
# IPv4 dest. partially extending to IPv6	1 (2.9%)	15 (14.0%)	29 (17.7%)	1 (3.2%)	0 (0.0%)	0 (0.0%)	78 (27.5%)	124 (18.2%)
# IPv4 dest. fully switching to IPv6	0 (0.0%)	0 (0.0%)	20 (12.2%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	17 (6.0%)	37 (5.4%)
IPv6 Dest. Transition to IPv4 in Dual-stack (% over common dest. between IPv6-only and dual-stack)								
# IPv6 dest. partially extending to IPv4	2 (28.6%)	7 (100.0%)	40 (46.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	89 (68.5%)	138 (59.5%)
# IPv6 dest. fully switching to IPv4	0 (0.0%)	3 (42.9%)	15 (17.2%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	8 (6.2%)	26 (11.2%)
IPv4-only Destinations in Dual-stack with AAAA Record (% over IPv4-only dest. in dual-stack)								
# IPv4-only Dest. w/ AAAA	0 (0.0%)	1 (0.5%)	18 (6.2%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	13 (3.3%)	32 (2.8%)

Table 9: Summary of destination domains switching between IPv4 and IPv6 in dual-stack experiments, including the number of domains that partially extend their communication to use both IPv6 and IPv4 or fully switch IP versions. Fractions in parentheses represent the percentage of total common destinations between single-stack and dual-stack configurations that change IP versions. The last row lists the number of IPv4-only domains with valid AAAA records in dual-stack experiments.

to IPv6, 14 devices in our testbed continue to utilize IPv4 for these domains, demonstrating a preference for IPv4 communication.

Takeaways. Our results show that in dual-stack scenarios, devices contact IPv4 destinations more often than IPv6, reinforcing the finding that smart homes are not yet fully ready for IPv6. Some destinations do switch to IPv6 or continue using IPv6 in dual-stack networks, following RFC 6724, which recommends prioritizing IPv6 over IPv4 [12]. However, the fact that other destinations revert to IPv4 or do not switch to IPv6 when they can suggests a shortfall in proper IPv6 adoption. This may likely be due to suboptimal configuration by device manufacturers.

5.4 IoT Privacy and Security in IPv6

This section focuses on IoT privacy and security concerns due to IPv6 adoption (RQ4). Namely, we discuss the exposure of IoT devices MAC address from devices relying on EUI-64 global addresses (a privacy risk), unusual differences in exposed ports/services between IPv4 and IPv6 (a potential security risk), and changes in third-party tracking activity (a privacy concern). For party characterization we use these definitions, similar to [40]: first-party destinations are the ones related to the device vendor (plus YouTube, in the case of TV devices, since we tested the YouTube app), support-party destinations are cloud services and CDNs, and everything else are third-party destinations (*e.g.,* tracking companies).

5.4.1 EUI-64 IPv6 Address Exposure. As discussed in §5.2, 16.1% of IoT devices (15) use global EUI-64 addresses in our experiments. This is a privacy concern as it exposes the device's MAC address to the network, enabling tracking and fingerprinting of the user and home network [15, 43, 52]. Moreover, the organizationally unique identifier (OUI) within the MAC address can also reveal the device's manufacturer.

We illustrate the number of devices using GUA EUI-64 addresses in Figure 5 (left). As mentioned in §5.2, many assigned IPv6 addresses, including GUA EUI-64 addresses, are never used. Specifically, 18 devices assign but never use GUA EUI-64 addresses. Among the 15 devices that use GUA EUI-64 addresses, we observe 8 using them for DNS resolution; of these, three never receive valid AAAA responses, while five use them for communication over the Internet.

In Figure 5 (right), we show the number of domains contacted by these five devices and the DNS query names from the three Samsung/SmartThings devices that only use EUI-64 addresses for DNS. Although these three devices have not initiated data communication due to the lack of AAAA responses, there is a potential risk they may do so in the future, exposing their EUI-64 addresses to resolved destinations. The five devices exposed their EUI-64 addresses to 27 domains, including 24 first-party domains, one third-party domain (an analytics service), and two support-party domains (NTP). The three devices using EUI-64 only for DNS queried 30 domains: 20 first-party, eight third-party (including analytics services), and two support-party domains. Besides destination domains and DNS resolvers, networks along the path, such as ISPs, can also see the EUI-64 addresses, leading to additional privacy concerns.

5.4.2 Open port scans. Upon scanning the IPv4 and IPv6 addresses of each device for open ports, we found that six devices have open ports in IPv4 that are not open in IPv6, indicating that more services are available in IPv4 than in IPv6. This is expected, as most of the devices in our testbed do not fully support IPv6 to the extent they support IPv4. However, particularly noteworthy is the case of one device, the Samsung Fridge, which has three open ports (37993, 46525, 46757) in IPv6 that are not open in IPv4. We could not identify the services offered through these ports using Nmap; therefore, we do not know whether they are intentional or a result of an IPv6 firewall misconfiguration. Since none of the devices we have tested advertise additional functionality when used in IPv6 as opposed to IPv4, we believe these additional open ports in IPv6 require further investigation to determine whether they pose a security risk.

5.4.3 Tracking Domains. We analyzed the domains contacted by the eight functional devices in the IPv6-only setup and found that, compared to the IPv4-only setup, 129 domains and 31 second level domains (SLDs) were used only in IPv4 but not in the IPv6-only network. Among them, 13 are third-party SLDs, including tracking domains such as *app-measurement.com*, *omtrdc.net*, and *segment.io*.

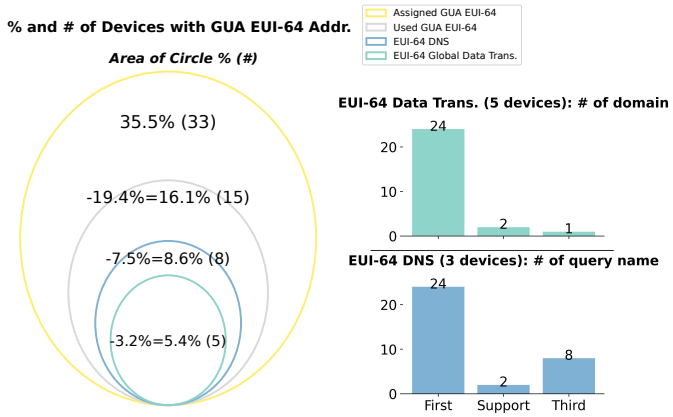


Figure 5: Left: % and # of devices assigning GUA EUI-64 addresses, using them, using them for DNS, and for Internet data transmission. Right: # of domains contacted or queried by devices using GUA EUI-64 addresses per domain organization party.

This is likely due to third-party libraries not supporting IPv6, missing AAAA records, or lack of IPv6 support from destination servers. While a reduction in communication with third-party tracking domains is a privacy advantage for using IPv6, we also note that the vast majority of devices are not functional over IPv6, so this advantage potentially comes at the cost of devices not working.

6 Discussion

The Smart Home is Not Fully Ready for IPv6. Our results indicate that only eight IoT devices from our testbed function in an IPv6-only network, with all others requiring IPv4 available to function properly. Even in dual-stack settings, most devices with global IPv6 addresses still predominantly rely on IPv4, indicating they are not fully leveraging IPv6. However, users can still utilize these global addresses to access their devices from the Internet, a primary benefit of IPv6. One explanation for incomplete support for IPv6 is the many parties that all need to support it across the network. Specifically, network providers, device vendors, and network administrators all must develop and maintain IPv6 support, potentially costing more than they are willing to invest. For many manufacturers, particularly those producing low-cost devices, the cost of implementing IPv6 may be prohibitive. Smaller companies may lack the resources or expertise to implement IPv6 properly, leading to the observed lack of IPv6 support in devices from non-major manufacturers. Another reason that may affect IPv6 readiness is that IPv4 still meets the connectivity needs of most IoT devices and will continue to do so for the foreseeable future, further making it difficult to justify the cost of maintaining IPv6 support.

Additionally, many IoT devices rely on proprietary protocols, legacy systems, or third-party platforms/tools, making IPv6 integration more complex and potentially leading to interoperability issues. In contrast, devices with good support for IPv6, *e.g.,* smart TVs and speakers, is likely due to their reliance on open and well maintained Android or Android-based OSes, which come with built-in IPv6 support. Power consumption is unlikely to be a primary factor limiting IPv6 adoption in smart homes, as IPv6-based protocols like Thread [20] are designed to operate efficiently on low-power devices in IoT environments.

Privacy and Security Considerations. We discovered that IPv6 offers a privacy benefit by reducing unnecessary exposure of information to third parties in an IPv6-only network. However, as IPv6 adoption grows, it is likely that trackers will also adapt to IPv6. Additionally, this benefit is difficult to leverage since most devices do not operate effectively on an IPv6-only network. We also noted potential privacy and security issues in our testbed, where some IoT devices expose their MAC addresses within their IPv6 addresses and open ports over IPv6 that are not open in IPv4. Since we lack internal device insights, we cannot definitively state whether these open IPv6 ports pose a security risk, but they certainly deserve further investigation. The static and predictable IPv6 addresses we observed could be exploited by adversaries to track users, launch attacks, and potentially defeat other IPv6 privacy practices of the network, such as the ISP-deployed prefix rotation [43].

New IPv6-based Standards. On a positive note, the latest IP-based IoT standards are pushing new generations of IoT devices to support IPv6, at least locally. Standards like HomeKit [3] and Matter [6] require that any device certified under them must implement essential local IPv6 features, such as SLAAC, to ensure compatibility and interoperability with other devices using these protocols. This creates a commercial incentive for IoT vendors to enhance IPv6 compatibility in their devices. Despite this, our findings reveal that even devices certified for HomeKit and Matter continue to depend on IPv4 for cloud-based companion app access, the primary function we tested. However, with most of the IPv6 stack already implemented on devices, we are optimistic that with further development and enhanced support from destinations, these devices could eventually transition to functioning in an IPv6-only network.

Policymakers Role in Supporting IPv6 Adoption. IPv6 offers advantages for IoT users, including global Internet reachability and potentially reduced reliance on cloud services. For this reason, consumers are exposed to harm when IoT devices ignore IPv6 in a dual-stack network, or become unusable in IPv6-only networks. To promote IoT IPv6 adoption, policymakers can compel disclosure of IPv6 support, similar to the existing IoT privacy/security labels [36].

7 Limitations and Future Work

Opaque-box Assumption. We treat our IoT devices as opaque boxes, analyzing only observable signals like network traffic. However, future research could benefit from adopting a clear-box strategy on select devices to gain deeper insights.

Network Configurations. Our experiments were conducted under typical home network configurations, focusing on common setups. We did not explore less common configurations, such as scenarios where DHCPv6 operates without SLAAC, which might be relevant in enterprise environments.

Location. Our study is limited to IoT devices and networks within the United States. As such, our results do not generalize to other locations or markets. IPv6 adoption can vary significantly by region due to factors such as ISP infrastructure, regional policies, and cloud service support. For example, regions with more advanced IPv6

deployments, like parts of Europe or Asia, may see higher rates of IPv6 adoption in smart homes. Future studies should consider expanding this research to additional places of interest.

Timeframe. Our experiments spanned two weeks to account for the frequent updates in IoT devices, networks, and DNS records, minimizing variability for consistent results. However, it limits our ability to observe long-term behavior and stability.

Functionality Tests. When testing our IoT devices, we test only the primary function, as discussed in §4.1. For limited-purpose devices (the majority in our testbed), this suffices as it covers most functionality. However, for complex IoT devices such as smart speakers and smart TVs that offer a broader range of functionality, many functions remain untested. To mitigate this, and ensure the reliability of functionality tests, we conducted additional tests on such complex devices, noting that the rest of the functionality we tested also works. Despite our efforts, there may still be instances where untested features behave differently in an IPv6 network. Future research could explore the IPv6 functionality of complex IoT devices and their associated app ecosystems in greater depth.

Service Outages. During our experiments, some devices sporadically lost their Internet connections on both IPv4 and IPv6, despite confirmed Internet connectivity with smartphones to rule out testbed issues. We could not pinpoint the exact causes of these disconnections. However, we repeated tests with affected devices to ensure the reliability of our results and mitigate any potential impact.

Reachability of IPv6 Destinations. We focus on the IPv6 features of IoT devices, including the resolution of IPv6 addresses via DNS. However, having an IPv6 address does not guarantee the destination is reachable, which explains why some devices still use IPv4 despite having AAAA records.

Companion Apps. We use companion apps to test the primary functionality of more than half of our IoT devices. For these devices to function properly in an IPv6-only network, their companion apps must also support IPv6. We assumed that these apps are IPv6-compatible, but this may not always be the case.

Open Port Scanning. Despite our best efforts to scan all IPv4 and IPv6 addresses for all devices, it is possible that some addresses were missed due to the large number of devices, the time-intensive nature of the scans, and the dynamic nature of these addresses.

Key Future Work. Our study identifies several directions for future research. These include exploring alternative network configurations, particularly in enterprise environments, repeating tests in different geographical locations, conducting longitudinal studies to observe long-term IPv6 behavior, understanding the reachability of IPv6 destinations, testing companion apps for IPv6 compatibility, and explore more comprehensive IPv6 port testing approaches.

8 Related Work

IPv6 Measurements. Various aspects of IPv6 have been examined, including address assignment practices [37], IPv6 DNS readiness [48], IPv6 router availability [4], IPv6 security on remote servers and routers [10], and overall IPv6 adoption [9]. However, to the best of our knowledge, no prior work has conducted a comprehensive study of IPv6 usage of consumer IoT devices in smart homes.

Privacy and Security Concerns with IPv6. Previous research has shown that IPv6 can lead to significant privacy leaks, exposing user and device information, and even enabling geolocation tracking [8, 41–43]. Building upon these findings, Zohaib *et al.* provides a tool to analyze the privacy leakage associated with IPv6 addressing of devices within the home network [52]. A recent study [25] also analyzed IPv6-reachable IoT hosts and their TLS security properties using active measurements from the Internet. This work is orthogonal to ours, as most smart home devices reside behind NAT and use proprietary protocols, making them invisible to Internet-based active measurements.

IPv6 in IoT. Previous work has explored various topics on IPv6 for IoT, such as efficient IPv6 communication for IoT [20, 23, 31, 33] and IoT IPv6 addressing strategies [26, 46]. However, these studies focus on the protocol design and applications, rather than assessing how consumer IoT devices support and utilize IPv6.

Smart Home IoT. Various studies have measured the security, privacy, and behaviors of smart home IoT ecosystems [1, 13, 15, 21, 22, 27, 30, 38–40, 44, 45, 50]. Recent research [15] found that IoT devices' MAC addresses and even router BSSIDs can be easily leaked to third parties via local network adversaries. Other studies revealed the dissemination of personal data (*e.g.,* MAC addresses, geolocation) to the cloud [40], or device identification based on network traffic [39, 44]. This information, combined with tracking through EUI-64 based IPv6 addresses, further enables targeted attacks, user profiling, and household fingerprinting. Additionally, previous research identified relatively low IPv6 usage among IoT backend servers through active scanning, highlighting that the adoption of IPv6 within IoT ecosystems remains limited [45]. Our work extends smart home research by exploring how IoT devices utilize IPv6, and their privacy and security implications.

9 Conclusion

In this paper, we explored the adoption of IPv6 in consumer IoT devices within typical home network settings. We find that enabling an IPv6-only network causes the vast majority of devices to malfunction, even those supporting all the IPv6 features analyzed. However, in dual-stack networks, many devices replace some IPv4 activities with IPv6, indicating notable progress toward adoption. Additionally, one-third of the devices configure public IPv6 addresses, which could facilitate easier Internet access compared to IPv4. However, we also observed concerning issues, such as devices that publicly expose their MAC addresses and having additional open ports in IPv6. These findings motivate the need for researchers to continue to study this issue, and for standards bodies and policymakers to provide incentives for consumer IoT vendors to improve IPv6 support. We hope that in doing so we will move to an environment where IoT devices are fully functional in an IPv6-only world.

Acknowledgments

We thank our shepherd and the anonymous reviewers for their constructive feedback. We thank Nikhil Manikonda for his help with preliminary experiments. This research was supported by the National Science Foundation (ProperData 1955227, SPHERE 2330066). The opinions, findings, conclusions, and recommendations expressed are those of the authors and do not necessarily reflect the views of any of the funding bodies.

References

[1] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. 2019. Sok: Security evaluation of home-based IoT deployments. In *2019 IEEE symposium on security and privacy (sp)*. IEEE, 1362–1380.

[2] Amazon. [n. d.]. Amazon Fire OS. https://developer.amazon.com/docs/fire-tv/fire-os-overview.html. Accessed on May 11, 2024.

[3] Apple. [n. d.]. HomeKit by Apple. https://www.apple.com/ios/home/. Accessed on May 11, 2024.

[4] Robert Beverly, Matthew Luckie, Lorenza Mosley, and Kc Claffy. 2015. Measuring and characterizing IPv6 router availability. In *Passive and Active Measurement: 16th International Conference, PAM 2015, New York, NY, USA, March 19-20, 2015, Proceedings 16*. Springer, 123–135.

[5] Tim Chown, John A. Loughney, and Timothy Winters. 2019. IPv6 Node Requirements. RFC 8504. https://doi.org/10.17487/RFC8504

[6] Connectivity Standard Alliance. [n. d.]. Matter standard. https://csa-iot.org/all-solutions/matter/. Accessed on May 11, 2024.

[7] Alissa Cooper, Fernando Gont, and Dave Thaler. 2016. Security and Privacy Considerations for IPv6 Address Generation Mechanisms. RFC 7721. https://doi.org/10.17487/RFC7721

[8] Tianyu Cui, Gaopeng Gou, Gang Xiong, Zhen Li, Mingxin Cui, and Chang Liu. 2021. SiamHAN: IPv6 address correlation attacks on TLS encrypted traffic via siamese heterogeneous graph attention network. In *30th USENIX Security Symposium (USENIX Security 21)*. 4329–4346.

[9] Jakub Czyz, Mark Allman, Jing Zhang, Scott Iekel-Johnson, Eric Osterweil, and Michael Bailey. 2014. Measuring ipv6 adoption. In *Proceedings of the 2014 ACM Conference on SIGCOMM*. 87–98.

[10] Jakub Czyz, Matthew Luckie, Mark Allman, Michael Bailey, et al. 2016. Don't forget to lock the back door! A characterization of IPv6 network security policy. In *Network and Distributed Systems Security (NDSS)*.

[11] Dr. Steve E. Deering and Bob Hinden. 2006. IP Version 6 Addressing Architecture. RFC 4291. https://doi.org/10.17487/RFC4291

[12] R. Draves and D. Thaler. 2012. Default Address Selection for Internet Protocol Version 6 (IPv6). RFC 6724. https://doi.org/10.17487/RFC6724

[13] Daniel J Dubois, Roman Kolcun, Anna Maria Mandalari, Muhammad Talha Paracha, David Choffnes, and Hamed Haddadi. 2020. When speakers are all ears: Characterizing misactivations of iot smart speakers. *Proceedings on Privacy Enhancing Technologies* 2020, 4 (2020), 255–276.

[14] Hurricane Electric. [n. d.]. IPv6 Tunnel Broker. https://tunnelbroker.net. Accessed on May 15, 2024.

[15] Aniketh Girish, Tianrui Hu, Vijay Prakash, Daniel J Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David Choffnes, et al. 2023. In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes. In *Proceedings of the 2023 ACM on Internet Measurement Conference*. 437–456.

[16] Fernando Gont. 2014. A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC). RFC 7217. https://doi.org/10.17487/RFC7217

[17] Fernando Gont, Suresh Krishnan, Dr. Thomas Narten, and Richard P. Draves. 2021. Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6. RFC 8981. https://doi.org/10.17487/RFC8981

[18] Google. 2012. Google Issue Tracker: Support for DHCPv6 (RFC 3315). https://issuetracker.google.com/issues/36949085?pli=1. Accessed on May 1, 2024.

[19] Google. [n. d.]. Fuchsia OS. https://fuchsia.dev/. Accessed on May 11, 2024.

[20] Thread Group. [n. d.]. What is Thread. https://www.threadgroup.org/What-is-Thread/Overview. Accessed on May 11, 2024.

[21] Tianrui Hu, Daniel J Dubois, and David Choffnes. 2023. Behaviot: Measuring smart home iot behavior using network-inferred behavior models. In *Proceedings of the 2023 ACM on Internet Measurement Conference*. 421–436.

[22] Danny Yuxing Huang, Noah Apthorpe, Frank Li, Gunes Acar, and Nick Feamster. 2020. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 2 (2020), 1–21.

[23] Antonio J Jara, Miguel A Zamora, and Antonio Skarmeta. 2012. Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things. *Mobile Information Systems* 8, 3 (2012), 177–197.

[24] Jaehoon Paul Jeong, Soohong Daniel Park, Luc Beloeil, and Syam Madanapalli. 2017. IPv6 Router Advertisement Options for DNS Configuration. RFC 8106. https://doi.org/10.17487/RFC8106

[25] Peter Jose, Said Jawad Saidi, and Oliver Gasser. 2023. Analyzing IoT Hosts in the IPv6 Internet. *arXiv preprint arXiv:2307.09918* (2023).

[26] Aljosha Judmayer, Johanna Ullrich, Georg Merzdovnik, Artemios G Voyiatzis, and Edgar Weippl. 2017. Lightweight address hopping for defending the IPv6 IoT. In *Proceedings of the 12th international conference on availability, reliability and security*. 1–10.

[27] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. 2019. All Things Considered: An Analysis of IoT Devices on Home Networks.. In *USENIX Security Symposium*. 1169–1185.

[28] Mon(IoT)r Lab. 2024. Research artifacts. https://moniotrlab.khoury.northeastern.edu/publications/iot-ipv6/.

[29] Gordon Lyon. 1997. Nmap: The network mapper. https://nmap.org/. Accessed on May 21, 2023.

[30] Anna Maria Mandalari, Daniel J Dubois, Roman Kolcun, Muhammad Talha Paracha, Hamed Haddadi, and David Choffnes. 2021. Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic. *Proceedings on Privacy Enhancing Technologies* (2021).

[31] Gabriel Montenegro, Christian Schumacher, and Nandakishore Kushalnagar. 2007. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919. https://doi.org/10.17487/RFC4919

[32] Tomek Mrugalski, Marcin Siodelski, Bernie Volz, Andrew Yourtchenko, Michael Richardson, Sheng Jiang, Ted Lemon, and Timothy Winters. 2018. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 8415. https://doi.org/10.17487/RFC8415

[33] Geoff Mulligan. 2007. The 6LoWPAN architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*. 78–82.

[34] Dr. Thomas Narten, Richard P. Draves, and Suresh Krishnan. 2007. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941. https://doi.org/10.17487/RFC4941

[35] Dr. Thomas Narten, Tatsuya Jinmei, and Dr. Susan Thomson. 2007. IPv6 Stateless Address Autoconfiguration. RFC 4862. https://doi.org/10.17487/RFC4862

[36] National Institute of Standards and Technology. 2022. Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf. Accessed on May 15, 2024.

[37] Ramakrishna Padmanabhan, John P Rula, Philipp Richter, Stephen D Strowes, and Alberto Dainotti. 2020. DynamIPs: Analyzing address assignment practices in IPv4 and IPv6. In *Proceedings of the 16th international conference on emerging networking experiments and technologies*. 55–70.

[38] Muhammad Talha Paracha, Daniel J Dubois, Narseo Vallina-Rodriguez, and David Choffnes. 2021. IoTLS: understanding TLS usage in consumer IoT devices. In *Proceedings of the 21st ACM Internet Measurement Conference*. 165–178.

[39] Roberto Perdisci, Thomas Papastergiou, Omar Alrawi, and Manos Antonakakis. 2020. IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 474–489.

[40] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. 2019. Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach. In *Proc. of the Internet Measurement Conference (IMC'19)*.

[41] Erik Rye, Robert Beverly, and Kimberly C Claffy. 2021. Follow the scent: Defeating IPv6 prefix rotation privacy. In *Proceedings of the 21st ACM Internet Measurement Conference*. 739–752.

[42] Erik C Rye and Robert Beverly. 2023. IPvSeeYou: Exploiting leaked identifiers in IPv6 for street-level geolocation. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 3129–3145.

[43] Said Jawad Saidi, Oliver Gasser, and Georgios Smaragdakis. 2022. One bad apple can spoil your IPv6 privacy. *ACM SIGCOMM Computer Communication Review* 52, 2 (2022), 10–19.

[44] Said Jawad Saidi, Anna Maria Mandalari, Roman Kolcun, Hamed Haddadi, Daniel J Dubois, David Choffnes, Georgios Smaragdakis, and Anja Feldmann. 2020. A haystack full of needles: Scalable detection of iot devices in the wild. In *Proceedings of the ACM Internet Measurement Conference*. 87–100.

[45] Said Jawad Saidi, Srdjan Matic, Oliver Gasser, Georgios Smaragdakis, and Anja Feldmann. 2022. Deep dive into the IoT backend ecosystem. In *Proceedings of the 22nd ACM internet measurement conference*. 488–503.

[46] Teemu Savolainen, Jonne Soininen, and Bilhanan Silverajan. 2013. IPv6 addressing strategies for IoT. *IEEE Sensors Journal* 13, 10 (2013), 3511–3519.

[47] William A. Simpson, Dr. Thomas Narten, Erik Nordmark, and Hesham Soliman. 2007. Neighbor Discovery for IP version 6 (IPv6). RFC 4861. https://doi.org/10.17487/RFC4861

[48] Florian Streibelt, Patrick Sattler, Franziska Lichtblau, Carlos H Ganán, Anja Feldmann, Oliver Gasser, and Tobias Fiebig. 2023. How ready is dns for an ipv6-only world?. In *International Conference on Passive and Active Network Measurement*. Springer, 525–549.

[49] Susan Thomson, Thomas Narten, and Tatuya Jinmei. 2003. DNS Extensions to Support IP Version 6. RFC 3596. https://doi.org/10.17487/RFC3596

[50] Janus Varmarken, JA Aaraj, Rahmadi Trimananda, and Athina Markopoulou. 2022. FingerprinTV: Fingerprinting Smart TV Apps. In *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Vol. 2022. 606–629.

[51] Wikipedia. [n. d.]. Comparison of IPv6 support in operating systems. https://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems. Accessed on May 1, 2024.

[52] Ali Zohaib and Amir Houmansadr. 2023. Automated Detection of IPv6 Privacy Leakage in Home Networks. *Free and Open Communications on the Internet* (2023).

Appendix

A Ethics

This study did not collect any personal data. Experiments were conducted when only the authors were present at an enclosed testbed location, ensuring that no user data could be accidentally recorded by any IoT device sensors.

Generative AI technology was solely utilized to enhance the clarity and presentation of text and LaTeX tables, without generating any original content.

B Disclosure and Response

We responsibly disclosed the use of GUA EUI-64 addresses in smart devices to the respective vendors (Google, Amazon, Samsung) by privately informing them through their vulnerability disclosure programs before publication. At the time of writing, Google had triaged the report as a privacy issue with moderate severity and documented it for potential remediation in a future release; Amazon had validated the report and classified it as low severity; and Samsung acknowledged the report and indicated that they are investigating the issue.

C IoT Devices

Table 10 provide a list of the 93 IoT devices in our testbed, including their categorized device types and the IPv6 features they supported during our IPv6-only and dual-stack connectivity experiments. Additional details and results are available in our public artifacts at https://moniotrlab.khoury.northeastern.edu/publications/iot-ipv6/ [28] or upon request.

Table 11 presents the firmware versions of selected devices. Many devices do not display the exact version number on the device or in their apps, and this information can sometimes be difficult to locate. As a result, we did not record the version numbers for all devices at the experiment time, as there is no scalable way to extract version numbers from all devices or their apps. The table includes only those devices for which public update information was available on manufacturers' websites. However, firmware updates are often rolled out in stages, so the versions listed here reflect those available to the device model at the time of our experiments and may not be accurate for every individual device. It is also possible that some devices received updates during or between our experiments. For devices where firmware information at the time of the experiment was not available, please refer to the date of our experiment mentioned in §4.2 as a reference for their firmware version.

D Additional Manufacturer/Platform, OS, Purchase Year Results

Table 13 shows number of IPv6 address and distinct DNS queries per manufacturer/platform and OS.

Furthermore, Table 12 categorizes devices according to their year of purchase to understand changes in IPv6 support over time. Notably, devices purchased in 2023 and 2024 show the highest overall support for IPv6 features. However, devices purchased in 2021 demonstrate the highest extent of IPv6 functionality in an IPv6-only network, with five devices remain functional. This observation correlates with our purchase of newer devices, many of which support the Matter standard [6], designed specifically for operation over IPv6. The 2021 group includes several smart TVs (Android-based), resulting in the high IPv6 support. Consequently, it is challenging to conclude that newer devices inherently offer better IPv6 support. The type of device and its manufacturer appear to have a more significant impact on the IPv6 support, as we discussed in the paper.

Device	Category	Funtionability IPv6-only	IPv6 NDP Traffic	IPv6 Address	GUA	DNS over IPv6	Global Data Comm
Behmor Brewer	Appliance	✗	✗	✗	✗	✗	✗
Smarter IKettle	Appliance	✗	✗	✗	✗	✗	✗
GE Microwave	Appliance	✗	✓	✓	✗	✗	✗
Miele Dishwasher	Appliance	✗	✓	✗	✗	✗	✗
Samsung Fridge	Appliance	✗	✓	✓	✓	✓	✓
Xiaomi Induction	Appliance	✗	✗	✗	✗	✗	✗
Xiaomi Ricecooker	Appliance	✗	✗	✗	✗	✗	✗
Amcrest Cam	Camera	✗	✓	✓	✗	✗	✗
Arlo Q Cam	Camera	✗	✗	✗	✗	✗	✗
Blink Doorbell	Camera	✗	✗	✗	✗	✗	✗
Blink Security	Camera	✗	✓	✓	✗	✗	✗
D-Link Camera	Camera	✗	✗	✗	✗	✗	✗
ICSee Doorbell	Camera	✗	✗	✗	✗	✗	✗
Lefun Cam	Camera	✗	✓	✓	✗	✗	✗
Microseven Cam	Camera	✗	✗	✗	✗	✗	✗
Nest Camera	Camera	✗	✓	✓	✓	✓	✓
Nest Doorbell	Camera	✗	✓	✓	✓	✓	✓
Ring Camera	Camera	✗	✗	✗	✗	✗	✗
Ring Doorbell	Camera	✗	✗	✗	✗	✗	✗
Ring Wired Cam	Camera	✗	✗	✗	✗	✗	✗
Ring Indoor Cam	Camera	✗	✗	✗	✗	✗	✗
TP-Link Camera	Camera	✗	✗	✗	✗	✗	✗
Tuya Camera	Camera	✗	✗	✗	✗	✗	✗
Wyze Cam	Camera	✗	✗	✗	✗	✗	✗
Yi Camera	Camera	✗	✗	✗	✗	✗	✗
Nintendo Switch	TV/Ent.	✗	✗	✗	✗	✗	✗
Aeotec Hub	Gateway	✗	✓	✓	✓	✓	✓
Aqara Hub	Gateway	✗	✓	✓	✗	✗	✗
Aqara Hub M2	Gateway	✗	✓	✓	✗	✗	✗
Eufy Hub	Gateway	✗	✓	✓	✗	✗	✗
IKEA Gateway	Gateway	✗	✓	✓	✓	✗	✓
Sengled Hub	Gateway	✗	✓	✓	✗	✗	✗
SmartThings Hub	Gateway	✗	✓	✓	✓	✓	✗
SwitchBot Hub	Gateway	✗	✗	✗	✗	✗	✗
Philips Hue Hub	Gateway	✗	✓	✓	✗	✗	✗
SwitchBot Hub 2	Gateway	✗	✓	✓	✗	✗	✗
ThirdReality Bridge	Gateway	✗	✓	✓	✓	✗	✗
SmartLife Hub	Gateway	✗	✓	✓	✓	✓	✓
Blueair Purifier	Health	✗	✓	✗	✗	✗	✗
Keyco Air	Health	✗	✗	✗	✗	✗	✗
ThermoPro Sensor	Health	✗	✓	✓	✓	✗	✗
Withings BPM	Health	✗	✗	✗	✗	✗	✗
Withings Sleep	Health	✗	✗	✗	✗	✗	✗
Withings Thermo	Health	✗	✗	✗	✗	✗	✗
Amazon Plug	Home Auto	✗	✗	✗	✗	✗	✗
Consciot Matter Bulb	Home Auto	✗	✓	✓	✗	✗	✗
Gosund Bulb	Home Auto	✗	✓	✓	✓	✗	✗
Govee Strip	Home Auto	✗	✗	✗	✗	✗	✗
Govee Matter Strip	Home Auto	✗	✓	✓	✗	✗	✗
Meross Dooropener	Home Auto	✗	✗	✗	✗	✗	✗
Meross Matter Plug	Home Auto	✗	✓	✓	✓	✗	✗
MagicHome Strip	Home Auto	✗	✗	✗	✗	✗	✗
Meross Plug	Home Auto	✗	✓	✓	✗	✗	✗
Nest Thermostat	Home Auto	✗	✓	✓	✗	✗	✗
Orein Matter Bulb	Home Auto	✗	✓	✓	✗	✗	✗
Ring Chime	Home Auto	✗	✗	✗	✗	✗	✗
Sengled Bulb	Home Auto	✗	✓	✗	✗	✗	✗
SmartLife Remote	Home Auto	✗	✓	✓	✗	✗	✗
Wemo Plug	Home Auto	✗	✗	✗	✗	✗	✗
TP-Link Kasa Bulb	Home Auto	✗	✗	✗	✗	✗	✗
TP-Link Kasa Plug	Home Auto	✗	✗	✗	✗	✗	✗
TP-Link Tapo Plug	Home Auto	✗	✓	✓	✓	✗	✗
Wiz Bulb	Home Auto	✗	✓	✗	✗	✗	✗
Yeelight Bulb	Home Auto	✗	✗	✗	✗	✗	✗
Tuya Matter Plug	Home Auto	✗	✓	✓	✗	✗	✗
Tapo Matter Bulb	Home Auto	✗	✓	✓	✓	✗	✗
Linkind Matter Plug	Home Auto	✗	✓	✓	✗	✗	✗
Leviton Matter Plug	Home Auto	✗	✓	✓	✗	✗	✗
August Lock	Home Auto	✗	✗	✗	✗	✗	✗
Cync Matter Plug	Home Auto	✗	✓	✗	✗	✗	✗
Echo Dot 2nd gen	Speaker	✗	✓	✓	✓	✗	✓
Echo Dot 3rd gen	Speaker	✗	✓	✓	✗	✗	✗
Echo Dot 4th gen	Speaker	✗	✓	✓	✗	✗	✗

Continue on next page

Device	Category	Funtionability IPv6-only	IPv6 NDP Traffic	IPv6 Address	GUA	DNS over IPv6	Global Data Comm
Echo Dot 5th gen	Speaker	✗	✔	✔	✔	✗	✔
Echo Flex	Speaker	✗	✔	✔	✗	✗	✗
Echo Plus	Speaker	✗	✔	✔	✔	✔	✔
Echo Pop	Speaker	✗	✔	✔	✗	✗	✗
Echo Show 5	Speaker	✗	✔	✔	✔	✔	✔
Echo Show 8	Speaker	✗	✔	✔	✔	✔	✔
Echo Spot	Speaker	✗	✔	✔	✔	✔	✗
Meta Portal Mini	Speaker	✔	✔	✔	✔	✔	✔
Google Home Mini	Speaker	✔	✔	✔	✔	✔	✔
Google Nest Mini	Speaker	✔	✔	✔	✔	✔	✔
HomePod Mini	Speaker	✗	✔	✔	✔	✔	✔
Nest Hub	Speaker	✔	✔	✔	✔	✔	✔
Nest Hub Max	Speaker	✔	✔	✔	✔	✔	✔
Apple TV	TV/Ent.	✔	✔	✔	✔	✔	✔
Google TV	TV/Ent.	✔	✔	✔	✔	✔	✔
Fire TV	TV/Ent.	✗	✔	✔	✔	✔	✔
Roku TV	TV/Ent.	✗	✗	✗	✗	✗	✗
Samsung TV	TV/Ent.	✗	✔	✔	✔	✔	✔
TiVo Stream	TV/Ent.	✔	✔	✔	✔	✔	✔
Vizio TV	TV/Ent.	✗	✔	✔	✔	✔	✔
Total		8	55	54	31	22	23

Table 10: IoT devices with their category and IPv6 features supported in IPv6-only and dual-stack experiments.

Device	**Version**	**Device**	**Version**
Homepod Mini	17.4	Hue Hub	1963171020
Apple TV	tvOS 17.4	IKEA Gateway	1.20.65
Google Home Mini, Google Nest Mini	2.57.375114	Wyze Camera	4.36.11.8391
Nest Hub, Nest Hub Max	Between 12.20230611.1.67 and 16.20231130.3.59	Blink Security	4.5.20
Roku TV	OS 12	Blink Camera 3	Outdoor: 10.65
Chromecast with Google TV	Between STTK.230808.004 and STTE.240315.002	Blink Doorbell	12.67
Aeotec hub, SmartThings Hub	0.52.11	Arlo Q Camera	1.13.0.0_95_a58d08a_db3500
Ring Chime	6.1.10 or higher	Amcrest Camera	V2.400.AC02.15.R
Ring Doorbell, Ring Camera, Ring Doorbell Wired	15.0.13 or higher	Ring Indoor Camera	15.0.8 or higher

Table 11: Firmware versions of select devices in our testbed, obtained from the respective vendor websites.

Purchase Year:	2017	2018	2019	2021	2022	2023	2024
# of Devices	8	16	6	24	15	16	8
IPv6 NDP Traffic	4	10	2	12	10	14	7
IPv6 Address	4	9	2	11	8	13	6
GUA	2	5	0	10	5	5	4
AAAA DNS Request	4	7	1	10	8	5	2
AAAA Response	3	7	1	9	7	3	1
Internet TCP/UDP IPv6 Data	1	4	0	8	5	3	2
Functional over IPv6-only	0	2	0	5	1	0	0

Table 12: Device IPv6-related functionality (# of devices) per purchase year (IPv6-only and dual-stack experiments).

		Manufacturer/Platform									OS				
	Total	Google	Amazon	Ring	SmartThings /Samsung	Tuya	TPLink	Aidot	Meross	Withings	Tizen	FireOS (Android)	Android -based	Fuchsia	iOS/TVOS
IPv6 Address	684	318	35	0	159	11	7	3	5	0	27	35	178	68	90
GUA	456	191	21	0	133	3	2	0	2	0	17	21	92	49	74
ULA	169	119	3	0	20	6	3	0	1	0	6	3	81	17	8
LLA	59	8	11	0	6	2	2	3	2	0	4	11	5	2	8
AAAA Req	1076	261	243	2	163	19	0	0	0	0	135	243	218	134	177
A only Req in IPv6	114	13	52	0	23	6	0	0	0	0	16	52	11	9	10
IPv4-only AAAA Req	334	54	120	2	86	1	0	0	0	0	85	120	24	5	3
AAAA Res	531	177	79	0	45	0	0	0	0	0	45	79	175	72	104

Table 13: Number of IPv6 address and distinct DNS queries per manufacturer/platform, and OS.