Fast IPv6 Network Periphery Discovery and Security Implications

Xiang Li*†, Baojun Liu*✉, Xiaofeng Zheng*‡, Haixin Duan*†‡§, Qi Li*†✉, Youjun Huang*
*Tsinghua University, ‡QI-ANXIN Technology Research Institute
†Beijing National Research Center for Information Science and Technology, §Peng Cheng Laboratory
{x-l19, zxf19, hyj18}@mails.tsinghua.edu.cn, {lbj, duanhx, qli01}@tsinghua.edu.cn

***Abstract*—Numerous measurement researches have been performed to discover the IPv4 network security issues by leveraging the fast Internet-wide scanning techniques. However, IPv6 brings the 128-bits address space and renders brute-force network scanning impractical. Although significant efforts have been dedicated to enumerating active IPv6 hosts, limited by technique efficiency and probing accuracy, large-scale empirical measurement studies under the increasing IPv6 networks are infeasible now.**

To fill this research gap, by leveraging the extensively adopted IPv6 address allocation strategy, we propose a novel IPv6 network periphery discovery approach. Specifically, *XMap*, a fast network scanner, is developed to find the periphery, such as a home router. We evaluate it on twelve prominent Internet service providers and harvest *52M* active peripheries. Grounded on these found devices, we explore IPv6 network risks of the unintended exposed security services and the flawed traffic routing strategies. First, we demonstrate the unintended exposed security services in IPv6 networks, such as DNS, and HTTP, have become emerging security risks by analyzing *4.7M* peripheries. Second, by inspecting the periphery's packet routing strategies, we present the flawed implementations of IPv6 routing protocol affecting *5.8M* router devices. Attackers can exploit this common vulnerability to conduct effective routing loop attacks, inducing DoS to the ISP's and home routers with an amplification factor of $>$*200*. We responsibly disclose those issues to all involved vendors and ASes and discuss mitigation solutions. Our research results indicate that the security community should revisit IPv6 network strategies immediately.

***Index Terms*—IPv6 Security, IPv6 Network Periphery, Internet Measurement, Routing Loop Attack**

I. Introduction

The IPv6 landscape has changed extraordinarily over recent years, along with a remarkably increasing number of networks and end-hosts becoming IPv6-capable. For example, the IPv6 adoption rate for Alexa top 1M websites was only ∼2.7% in 2012, whereas it is ∼17.2% in November 2020 [88]. Similarly, less than 1% of Google's users access the services via IPv6 in 2012, while it has increased to ∼30% as of November 2020 [40]. Besides, APNIC reports that ∼21k Autonomous Systems (ASes) advertise IPv6 prefixes, and the number of active IPv6 BGP entries is ∼101k in November 2020 [44].

IPv6 brings in immensely increased address space, changing address allocation principles and permitting direct end-to-end Internet communication. Specifically, end-users can obtain one or many globally addressable IPv6 prefixes from their Internet Service Providers (ISPs), which shifts the address assignment strategy from "one single address" to "multiple prefixes" [18], [21], [63]. Therefore, it is essential to explore both IPv6 networks' applicability and security issues.

To achieve the goal of large-scale Internet-wide service measurements, fast network scanning techniques have been developed, including ZMap [29] and Masscan [56], which could be used to track botnet's behaviors [4], measure protocol deployment [3], [54], and uncover vulnerabilities [11], [41], [51].

Unfortunately, it has long been recognized [13] that the IPv6 network's enormous address space renders exhaustive probing inordinately expensive. While notable sophisticated techniques have been introduced to find active 128-bits end-hosts by inferring the underlying address patterns and structures [32], [53], [60], [79], [86], passive collection [17], [31], [43], [71], [81], and hitlists [30], [33], [34], which is significantly constrained by either seeds diversity or algorithm complexity, *there is still no effective way to perform global IPv6 network scanning.* It becomes the main obstacle to study the IPv6 network security.

In this paper, we aim to overcome the obstacle by developing an effective IPv6 network scanning technique. Particularly, we discover the critical IPv6 network periphery by leveraging practical scanning and explore its security implications, instead of measuring common 128-bits end-hosts.

The *IPv6 Network Periphery* is the last hop routed infrastructure devices connecting end-hosts or only enable connectivity for itself, such as a Customer Premises Edge (CPE) like a home router and a User Equipment (UE) like a smartphone. Thus, first, the IPv6 network periphery discovery is essential to the completeness of network topology mapping [77]. Further, due to the new IPv6 address assignment policy, the periphery is usually allocated a large IPv6 prefix (e.g., /64 or /60) from its ISP. Unlike the routers using NAT and any IPv4/IPv6 end-host, the IPv6 network periphery functions not only like a forwarding device but also a provisioning system as a gateway. It takes the responsibility to manage the prefixes and guarantee its and downstream device's security, such as packets forwarding and filtering, prefixes and routes functioning [78]. Accordingly, the security community should pay more attention to guaranteeing its security, which has not been well-studied in previous works.

Even though it is impractical to scan the entire IPv6 address space or just sample 64-bits interface identifier (IID) subspace, we show that *probing the sub-prefix space within each ISP's IPv6 block can be surprisingly productive.* Anyone could send a packet to one globally unique address within an IPv6 prefix

✉Corresponding author.

assigned to the periphery. Our major observation is that if the address is not being used (much more likely is the case for the ample IID space), the periphery will respond with a destination unreachable message by itself following RFC 4443 [24]. *That error message exposes the network periphery's IPv6 address and narrows down the search times to discover a periphery from* 2^{128-64} *or larger to* 1. The number of 128-bits addresses in one /64 prefix is theoretically unlimited, whereas the volume of sub-prefixes available for peripheries' assignment is usually numerable. In consequence, this mechanism allows researchers to enumerate the network periphery fast, with every sub-prefix being probed once for one IPv6 block within a feasible period.

To evaluate its feasibility and performance, we conduct real-world controlled network scanning experiments on 15 sample IPv6 blocks within 12 well-known ISPs from India, America, and China. As a result, we discover *52M* IPv6 network peripheries with *<15 Mbps* network uplink bandwidth, following the best practices for good-behavior Internet citizenship [29].

Furthermore, we explore the security implications based on those discovered peripheries, which are previously invisible to security researchers. The first issue is the inadequate protection for application services running on the periphery, which should not be made public to the external IPv6 networks. We discover *4.7M* devices exposing such services to arbitrary users, including *108* device vendors. What is worse, we present that the vast majority of those service software with far lagging versions are released *8-10* years ago, existing potential exploiting security risks. For example, *741k* periphery devices providing the DNS services can be abused as open IPv6 DNS resolvers, and *142k* of those devices are running dnsmasq 2.4x (released ∼8 years ago). At the same time, *1.3M* routers' web management pages could be accessed from the Internet, which would potentially induce unauthorized access and risks of being exploited. Based on our large-scale measurement study, we demonstrate that the network periphery's unintended exposed IPv6 services have become an emerging security risk now.

Secondly, towards the common implementations of the IPv6 packet routing and forwarding strategy, we find the widespread defective implementation existing in plentiful network peripheries. This flaw could result in a routing inconsistency between the periphery and the upstream router. Adversaries can exploit the vulnerable IPv6 routing strategy to carry out traffic routing loop attacks, causing Denial of Services (DoS) to ISP routers and home routers with an amplification factor of *>200*. Our measurement shows that this attack strikes *5.8M* routers from *49* device vendors distributed in *3.8k* ASes and *132* countries. *We test the loop on 99 sample routers from 24 eminent router vendors with up-to-date firmware, which are all vulnerable.*

Finally, we discuss the mitigation solutions and responsibly disclose all issues and vulnerabilities to involved vendors and ASes. *All 24 vendors confirmed the routing loop vulnerability, and we received >106 vulnerability numbers (CNVD/CVE).*

In summary, we make the following contributions:

1) We introduce a novel IPv6 network scanning technique *and develop a fast network scanner XMap* to evaluate it, released at https://netsec.ccert.edu.cn/projects/xmap.
2) We conduct systematical measurements on 7 periphery's essential services that should not be made public to the external IPv6 networks.
3) We find a widespread routing loop vulnerability resulting from the IPv6 routing module's flawed implementation.

II. Background

IPv6 Address Allocation. Different ISPs might adopt various allocation strategies for the IPv6 address. However, as the best practice, the IETF community affirms an important principle for the IPv6 address management in RFC 6177 [63]:

> *End sites always are able to obtain a reasonable amount of address space for their actual and planned usage. In practice, that means at least one /64, and in most cases, significantly more.*

We also find that the Regional Internet Registries indeed implement their own IPv6 address assignment policies following the above principle. For instance, APNIC requires their Local Internet Registries (LIRs) to assign /56 for the small sites, /48 for the larger sites, whereas /64 for where it is known that only a subnet is constructed [5]. RIPE recommends that /64 for the Wide Area Network (WAN) link to the end-user CPE devices, /48 for business customers, /56 for residential subscribers, and /64 for each Packet Data Protocol context of the cellular phone [73], same to LACNIC [49]. Similarly, AFRINIC declares the guidelines that LIRs should assign /48 in the general case, and /64 when only a subnet is required [2], similar to ARIN [10].

To sum up, usually, *the end-users can obtain at least one /64 IPv6 prefix in practice*, which ensures the end-users could hold sufficient addresses space and simplifies network management.

IPv6 Network Periphery. Since IPv6 changes address allocation principles, it makes multi-addressing the norm and brings in the global addressability for the devices in a home network through the vastly increased 128-bits address space [23].

Specifically, in the IPv6 network, an end-user device, such as a CPE router and a UE device, can obtain at least one /64 prefix or a larger prefix like /60. On the one side, the prefix can be used to construct more subnets and extend the Local Area Networks (LANs). On the other side, it raises security issues, such as what strategy should be applied to assign sub-prefixes to internal subnets with proper routes? Also, IPv6 restores the possibility of actually direct end-to-end communication, global addressability, and the elimination of NAT [80], which could potentially expose more nodes. Therefore, the packet filtering and access control policies should be considered carefully.

The IPv6 network periphery, i.e., the last hop routed router connecting end-users in the Internet, plays a critical role in the above processes [78] and becomes one of the crucial routing devices in the whole Internet topology [77]. As a routing device, the IPv6 periphery forwards packets and operates routes. As a gateway device, it provides network access between the Internet and internal hosts and manages the security policies, such as packet filtering and access control. In summary, the periphery device takes all the responsibilities to guarantee the availability and security of the IPv6 end-user network.

III. IPv6 Network Periphery Discovery Methodology

The state-of-the-art technique for IPv6 network space scanning probes with target generation algorithms or hitlists, which is restrained by address seeds diversity, algorithm complexity, accuracy and efficiency. In this paper, we consider this problem from a different perspective and switch the focus of scanning from the 128-bits end-hosts to IPv6 network peripheries. With the extensively adopted IPv6 address allocation strategies, we propose a novel scanning technique that can be used to conduct large-scale and fast IPv6 network periphery discovery.

A. IPv6 Network Periphery Model

We aim to discover the IPv6 network periphery, a crucial infrastructure within end-user networks, whose network security issues with IPv6 have not been studied well formerly.

As described in Section II, the *IPv6 periphery* is not any server and client device, but the last hop routed infrastructure connecting end-hosts or nothing except itself, e.g., a CPE like a home router and a UE like a smartphone. As a provisioning system [78], it not only forwards packets and provides network access services between the Internet and its LAN network but also serves as a security gateway for packet filtering and access control. And it has become one determining device in the home networks. Especially, a UE can turn into the periphery by being assigned an IPv6 prefix from mobile networks [19], [47], [48].

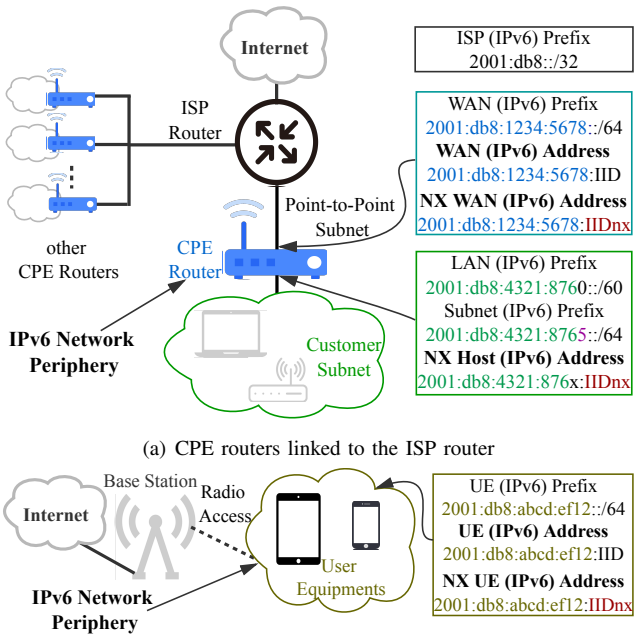
Figure 1 illustrates two topology models of the IPv6 periphery we aim to discover, covering the broadband network (CPE model) and the mobile network (UE model). We describe these two models detailedly in the following.

Customer Premises Edge (CPE) model. In the case of the CPE router model [78], one ISP router connects with a number of CPE routers. There are two primary network interfaces in every CPE router, including the WAN interface and the LAN interface. Each of these interfaces is assigned or delegated an IPv6 prefix (being used to form a subnet) from the ISP's IPv6 block (*ISP (IPv6) Prefix*), such as 2001:db8::/32 in Figure 1.

In general, the subnet between the ISP router and the CPE router is assigned a public IPv6 prefix as the router's WAN interface prefix, such as 2001:db8:1234:5678::/64, named *WAN (IPv6) Prefix* in the rest of this paper. And the customer subnet inside the CPE router's LAN is also delegated one globally addressable prefix different from *WAN Prefix* commonly, named *LAN (IPv6) Prefix*. Specifically, *LAN Prefix* is instantiated as 2001:db8:4321:8760::/60 in Figure 1. In practice, a sub-prefix of *LAN Prefix* is advertised to more than one node on an inside link and shared by the subnet, termed *Subnet (IPv6) Prefix*.

After obtaining a prefix, a CPE often uses Stateless Address Autoconfiguration (SLAAC) [84] algorithm to create the globally unique 128-bits addresses. For instance, the CPE router's *WAN Interface (IPv6) Address* is initiated by appending IID to *WAN Prefix*, whereas *Subnet Prefix* and IID assemble *LAN Interface (IPv6) Address* and *Host (IPv6) Address*.

User Equipment (UE) model. As for the UE model [19], [47], [48], a UE is attached to its provider's radio access network and is assigned one publicly-routed prefix, entitled *UE (IPv6) Prefix*, e.g., 2001:db8:abcd:ef12::/64 in Figure 1. A UE creates *UE (IPv6) Address* by combining *UE Prefix* with IID.



(a) CPE routers linked to the ISP router

(b) UE devices attached to the ratio access network

Fig. 1. The IPv6 Network Periphery Models

These two models are commonly applied to residential and mobile IPv6 networks, according to [19], [47], [48], [78]. And the broadband and mobile network are widely deployed [46], [65]. Similarly, the CPE model exists in enterprise networks.

B. Periphery Discovery Strategy

For IPv4, the most straightforward strategy to discover alive devices is to probe the whole network space. Current scanning techniques enable a single host to scan the entire 32-bits IPv4 address space in <1h [29]. However, it will take 40,000+ years to scan just the 64-bits IPv6 IID space in this fashion, which is prohibitively impracticable and impossible.

However, owing to the characteristic of the global addressability, IPv6 allows direct end-to-end communication between the LAN hosts and devices from the Internet. Depending on the new address allocation principles, the IPv6 network periphery functions as a routing gateway device, forwarding packets and providing network access service for itself and LAN hosts. All the changes aforementioned make IPv6 different from IPv4 on the behaviors of the periphery.

For example, as claimed by RFC 4443 [24], when a packet can not be delivered to the destination address, one ICMPv6 Destination Unreachable message should be generated by the router or by the IPv6 layer in the originating node. Regarding the IPv4 router using NAT, all downstream devices are represented by a public address. Generally speaking, there is no way to send a packet directly to an internal address from outside. However, in the IPv6 network, almost all devices can obtain a public-routed prefix managed by peripheries. Therefore, *the IPv6 periphery would generate one unreachable message for a packet with a nonexistent destination towards such a prefix.*

TABLE I
INFERRED IPV6 SUB-PREFIX LENGTH FOR END-USERS OF TARGET ISPS

Country	Network	ISP	ASN	Block	Length
India	Broadband	Reliance Jio	55836	/32	64
		BSNL	9829	/32	64
	Mobile	Bharti Airtel	45609	/32	64
		Vadafone	38266	/32	64
America	Broadband	Comcast	7922	/24	56
		AT&T	7018	/24	60
		Charter	20115	/24	56
		CenturyLink	209	/24	56
	Mobile	AT&T	20057	/24	64
	Enterprise	Mediacom	30036	/28	56
China	Broadband	Telecom	4134	/24	60
		Unicom	4837	/24	60
		Mobile	9808	/24	60
	Mobile	Unicom	4837	/24	64
		Mobile	9808	/24	64

Leveraging the above mechanism, we could craft one packet with a nonexistent IPv6 destination address, such as *NX WAN Address*, *NX Host Address* or *NX UE Address*, which would be transmitted to the IPv6 network periphery, respectively. Due to large 64-bits IID space, it is nearly impossible to hit an existent 128-bits address. As a result, the periphery will respond with a destination unreachable error message for that crafted packet, exposing its address, such as *WAN Address* or *UE Address*.

Applying this delicate strategy, we could discover the crucial IPv6 network periphery infrastructure, instead of a single common end-host. This method is not curbed by any address seeds diversity or algorithm complexity. What is more important, this technique devotes such a tremendous progress that *the search times is extremely reduced from* 2^{128-64} *or larger to 1, to find a periphery, more effective than existing tools or works* [77].

Scanning Feasibility Analysis. In spite of the fact that it is impossible to scan the entire IPv6 address space or just 64-bits IID space, we shift the search target from 128-bits addresses to less-bits sub-prefixes within each ISP. As shown in Section II and Table I, ISPs tend to allocate prefixes with length at most 64 to their customers, such as /64 for *WAN Prefix*, /60 or short for *LAN Prefix*, and /64 for *UE Prefix* (from Section IV-E).

If a researcher obtains one prefix assigned to any periphery, e.g., a *LAN Prefix* or a *UE Prefix*, with the above strategy, he can find *WAN Address* or *UE Address* of the periphery through sending one packet destined for any nonexistent address within that prefix merely. Further, if the researcher acquires one IPv6 block allocated to any ISP, e.g., a /24 *ISP Prefix*, one 1 Gbps scanner [29], could probe all /64 sub-prefixes (2^{40}) in 8 days and all the /60 sub-prefixes (2^{36}) in 14 hours with each sub-prefix being probed for once, which is totally practical.

In this section, we introduce a novel IPv6 scanning technique to discover the critical IPv6 network periphery. We show it is powerful to expose vast peripheries by feasible scanning, targeting the sub-prefix within each *ISP Prefix*, and leveraging the extensively implemented IPv6 address allocation principle.

IV. EVALUATION AND MEASUREMENT

In this section, we evaluate the fast IPv6 periphery scanning approach on 15 IPv6 blocks within 12 popular ISPs from India, America, and China, shown in Table I and select prefix targets based on the WHOIS databases maintained by APNIC [6] and ARIN [9]. These three countries hold a significant number of IPv6 users, and the 12 ISPs (13 ASes) have large IPv6 users within each country as well, according to the statistics [7], [8] from APNIC Labs. We design and implement an IPv6 network scanner, *XMap*. As a result, leveraging XMap, we harvest *52M* IPv6 peripheries under our experiment setup with <15 Mbps network uplink bandwidth. Besides, we analyze their security properties with IID analysis and application-level information.

A. Scanning Targets

IPv6 Subnet Discovery. A prerequisite is to deduce the length of the sub-prefix assigned to a periphery (the subnet boundary) within an *ISP Prefix*. We develop a very efficient technique to extrapolate it, emanated from the periphery discovery strategy.

We begin with a preliminary scanning to gain one periphery address. This scanning probes a small number of the IPv6 sub-prefixes within one *ISP Prefix*, e.g., 2001:db8::/32 in Figure 1, by combining different /64 prefixes with random IIDs as the target scanning addresses, e.g., 2001:db8:0:1:IID$_{target}$. If we receive an unreachable packet from a periphery-like address, such as 2001:db8:1:1:IID$_{reply}$ of EUI-64 format, we consider it as one valid periphery address and stop this first scanning.

Furthermore, we modify the bits of 2001:db8:0:1:IID$_{target}$ from the 64th to 32nd bit in reverse order to create new target addresses, e.g., 2001:db8:0:8:IID and 2001:db8:0:10:IID, and probe them respectively. If any responded address is different from the former address or does not exist, we conclude that the changed bit position is the subnet boundary. For instance, if we also receive one packet from 2001:db8:1:1:IID$_{reply}$ responding for the packet destined for 2001:db8:0:8:IID and no response for 2001:db8:0:10:IID, the sub-prefix length probably is 60.

We replicate the test several times to ensure the correctness of the inference. If multiplex sub-prefix lengths are found, we choose one primary length for our measurements. Besides, we take /64 as the longest prefix assigned to peripheries depending on the far-ranging address assignment practices described in Section II. The inferred sub-prefix length of the 15 IPv6 blocks is listed in Table I, and all these 12 ISPs assign prefixes with length at most 64 to their customers.

Target Lists. To demonstrate the scanning feasibility, instead of searching the whole *ISP Prefix* space (though it is feasible), we select the 32-bits sub-prefix space per block for evaluation. For example, the address space between the 32nd and 64th bit (/32-64) within a Reliance Jio's IPv6 block will be one of our probe targets. The entire scanning ranges are listed in Table II.

B. XMap: The IPv6 Network Periphery Scanner

Currently, we are lacking tools that have the ability to scan the IPv6 prefix space. So, we introduce *XMap* for performing the Internet-wide IPv6 network research scanning. XMap is re-implemented and improved thoroughly from ZMap [29]. We equip it with modular design, address random generation and exclusion, fast packet processing, and various probe modules.

The key module is the *address generation module*, providing an all address space random permutation. Unlike ZMap, which

TABLE II
RESULTS OF PERIPHERY SCANNING FOR ONE SAMPLE IPV6 BLOCK WITHIN EACH ISP

Cty	Network	Internet Provider	Scan Range	Last Hops (128-bits addr)			/64 prefix		EUI-64 addr		MAC addr	
				# uniq	% same	% diff	# uniq	%	# uniq	%	# uniq	%
IN	Broadband	Reliance Jio	/32-64	3,365,175	**99.8**	0.2	3,363,513	100.0	46,811	1.4	46,742	99.9
		BSNL	/32-64	2,404	34.4	65.6	2,276	94.7	1,844	**76.7**	1,771	96.0
	Mobile	Bharti Airtel	/32-64	22,542,690	**98.9**	1.1	22,340,370	99.1	319,067	1.4	311,567	97.6
		Vadafone	/32-64	2,307,784	**99.8**	0.2	2,307,672	100.0	29,463	1.3	28,558	96.9
US	Broadband	Comcast	/24-56	87,308	0.0	**100.0**	5,694	6.5	82,965	**95.0**	82,964	100.0
		AT&T	/28-60	740,141	0.0	**100.0**	735,958	99.4	94,440	12.8	94,375	99.9
		Charter	/24-56	13,027	1.6	**98.4**	1,573	12.1	80	0.6	80	100.0
		CenturyLink	/24-56	249,835	0.0	**100.0**	233,298	93.4	92,429	**37.0**	91,260	98.7
	Mobile	AT&T	/32-64	1,734,506	**94.5**	5.5	1,730,125	99.7	539	0.0	536	99.4
	Enterprise	Mediacom	/28-56	38,399	0.0	**100.0**	516	1.3	153	0.4	142	92.8
CN	Broadband	Telecom	/28-60	2,122,292	0.2	**99.8**	2,100,034	99.0	258,392	**12.2**	251,592	97.4
		Unicom	/28-60	1,273,075	3.0	**97.0**	1,272,540	100.0	679,108	**53.3**	647,826	95.4
		Mobile	/28-60	7,316,861	2.4	**97.6**	7,315,713	100.0	2,419,951	**33.1**	2,329,720	96.3
	Mobile	Unicom	/32-64	3,696,275	**97.9**	2.1	3,693,605	99.9	15,640	0.4	15,452	98.8
		Mobile	/32-64	7,193,972	**98.4**	1.6	7,188,311	99.9	21,290	0.3	20,995	98.6
-	-	**Total**	-	**52,478,703**	77.2	22.8	**52,086,849**	**99.3**	**3,973,467**	**7.6**	3,832,520	**96.5**

Scan Range: 32-bits space, **uniq**: unique number, **same**: same /64 with probe addr's, **diff**: different /64 from probe addr's Scanning Date: Nov 2020

can only permute the rear segment of the 32-bits IPv4 address, *XMap could permute all the address space with any length and at any position*, such as the space between the 20th and 25th bit of 2001:db8::/20-25 and 192.168.0.0/20-25. We leverage GMP [35] to implement the address generation module. Nonetheless, GMP just provides a big integer library, and all the related data structures and functions should be rewritten, including the tree structure to present addresses, the blocklist structure to ignore addresses, the cyclic module to form a succeeding address, and the expression structure to filter specific fields. In addition, the *IID generation module* is created to fill up the left bits behind the prefix, and all related codes are improved to support IPv6.

XMap is fully compatible with ZMap and works for Linux, macOS, and BSD, with about 15,000 SLOC of C. Researchers could utilize it to conduct large-scale IPv6 network scanning for security assessments, targeting any address or prefix space with affordable network ability and facility. Network administrators can leverage it to evaluate their own networks' security and risks of being exposed. We believe XMap will contribute to the future IPv6 Internet measurement studies and help the security community gain more insights into the IPv6 networks.

C. Limitations

We acknowledge that there are several potential limitations in our experiments. First, owing to various ISP's filtering policies and packet loss, the inferred sub-prefix length might be incorrect. Thus, if an ISP has set up upstream ICMPv6, we could underestimate the discovered devices. However, according to measurement results in Table II, this situation is less common in our study scope. Nevertheless, this case does not introduce any false discovery. Second, there is no explicit ground-truth dataset to determine whether the IPv6 periphery we discover is indeed the last hop. Nonetheless, as described in Section II, the unique /64 prefix tends to be the subnet boundary, and a significant portion of all the periphery addresses are the EUI-64 format addresses. We examine the device types based on the encoded MAC addresses, which turns out to be the CPE and the UE devices in Table IV. Additionally, we also collect application-level information to confirm the periphery to be the last hop from Section V. Although the device owners may modify the information, it has been addressed in [91] and the identifying means is widely used in the community [66], [77].

TABLE III
IID ANALYSIS OF DISCOVERED PERIPHERIES

-	# num	%	-	# num	%
EUI-64	3.97M	7.6	**Randomized**	39.60M	75.5
Low-byte	511.18k	1.0	**Byte-pattern**	5.46M	10.4
Embed-IPv4	2.91M	5.5	**Total**	52.48M	100.0

TABLE IV
TOP APPEARED PERIPHERY VENDORS AND DEVICE NUMBER

CPE	Total (3.9M), China Mobile (2.0M), ZTE (611.5k)
	Skyworth (509.0k), Fiberhome (260.5k), Youhua Tech (146.5k)
	China Unicom (107.9k), AVM (97.9k), Technicolor (46.3k)
	Huawei (41.7k), StarNet (32.2k), TP-Link (1.8k), D-Link (1.5k)
	Xiaomi (994), Hitron Tech (914), Netgear (149), Linksys (147)
	Asus (145), Optilink (127), Tenda (110), MikroTik (50)
UE	Total (1.8k), NTMore (633), HMD Global (282), Vivo (194)
	Oppo (165), Apple (162), Samsung (126), Nokia (107)
	LG (50), Motorola (30), Lenovo (25), Nubia (21), OnePlus (5)

CPE: customer premise edge, e.g., home router (gateway)
UE: user equipment, e.g., smartphone

D. Ethical Considerations

Our network scanning may induce several ethical concerns. Here, we discuss them first before presenting our measurement results. Throughout this research, we acted in accordance with the ethical conventions for network measurement studies, including the best practices [29] and the broad ethical guidelines [12], to minimize the potential impact as much as possible.

For instance, in our measurements, (*i*) we set up web pages on the source probing IPv6 addresses, signal the benign intent of the network scans, and show our contact details; (*ii*) we limit the probing rate and lighten the probing to minimize negative impacts; (*iii*) we restrict ourselves to regular TCP/UDP/ICMP connection attempts followed by RFC-compliant protocols and never undertake to exploit any vulnerabilities; (*iv*) in the end, we also avoid releasing the discovered periphery addresses for privacy concerns and disclose all found weaknesses or vulnerabilities to involved device vendors and network administrators.

E. Periphery Discovery Results

XMap Performance. We performed the measurements from a physical machine with a Xeon Silver 4210 2.2 GHz processor and 16 GB RAM in November 2020. We only take <15 Mbps (25 kpps) uplink bandwidth for sending packets to reduce the load on the target networks. With each sub-prefix being probed once and random permutation, the traffic is spread to different sub-networks. As a result, the scanning for a sample *ISP Prefix* (32-bits space) takes approximately 48 hours.

Volume of Discovered IPv6 Periphery. As shown in Table II, we discover *52.5M* unique, non-aliased last hop IPv6 addresses belonging to *52.1M* distinct /64 prefixes (99.3% of the whole /64 prefixes, column "*/64 prefix*"). This result means that the probing reaches more of the network peripheries for that the IPv6 Internet has /64 subnets at its edge (Section II). The best performing target IPv6 block is from Bharti Airtel, where we find *22M* unique last hops, whereas BSNL produces the fewest number of IPv6 addresses. We attribute the fewness to the less used IPv6 block, false sub-prefix length inference, or adopted filtering policies of the BSNL's sample /32 prefix.

IPv6 Addresses Allocation Analysis. Utilizing the *addr6* tool [37], we scrutinize the IID proportion of all discovered IPv6 addresses, whether it, e.g., (*i*) may be an EUI-64 IID with an embedded MAC address or an IID inserted one IPv4 address, (*ii*) has a run of zeroes followed only by a low number (Low-byte), (*iii*) has some discernible patterns (Byte-pattern) or not (Randomized). In Table II and Table III, the percentages reflect the IID proportion within each ISP and the total number (row).

3.97M (7.6%, column "*EUI-64 Addr*") last hops are EUI-64 format, embedded with *3.83M* exclusive MAC address (96.5% of the MAC addresses appeared once, column "*MAC Addr*"), which denotes a majority of the last hops are different devices.

Besides, the randomized address is the most heavily represented address (*75.5%*), which is usually generated by SLAAC for CPE or end-host devices in practice, recommended by [39].

Periphery Validation. According to Section II, the discovery of the unique /64 sub-prefix is powerfully indicative of discovering the periphery. Moreover, we utilize the embedded MAC address from the EUI-64 format address to identify the device manufacturer [45]. Also, the randomized address is primarily applied to the CPE or end-host device. Furthermore, we collect the application-level information of those last hop devices to extrapolate the device vendors in Section V-A.

We explicitly determine *3.9M* last hops to be the periphery devices with the assistance of the hardware manufacturer and the application-level information, including *3.9M* CPE devices and *1.8k* UE devices. The most common device vendors and their device numbers are listed in Table IV, such as the CPE device vendors like ZTE, TP-Link, and D-Link, and the UE device vendors like NTMore, Samsung, and LG. Besides, the peripheries with application-level services are mostly EUI-64 (*30.4%*) and Randomized addresses (*69.0%*) listed in Table V.

In Table II, the "same" indicates the probe address is from *WAN Prefix* or *UE Prefix*, and the "diff" stands for *LAN Prefix*. As the IPv6 periphery model in Section III-A shows, the larger the "diff" proportion is, probably the more CPEs we discover.

TABLE V
IID ANALYSIS OF PERIPHERIES WITH ALIVE APPLICATION SERVICES

-	# num	%	-	# num	%
EUI-64	1.43M	30.4	**Randomized**	3.24M	69.0
Low-byte	13.93k	0.3	**Byte-pattern**	9.73k	0.2
Embed-IPv4	2.91M	5.5	**Total**	4.69M	100.0

TABLE VI
PROBING REQUESTS AND VALID RESPONSES OF 8 SELECTED SERVICES

Service/Port	Request	Valid Response
DNS (UDP/53)	"A" or version query	answers
NTP (UDP/123)	version query	version reply
FTP (TCP/21)	request for connecting	successful response
SSH (TCP/22)	version, key request	version, key
TELNET (TCP/23)	request for login	response for login
HTTP (TCP/80)	HTTP `GET` request	header, version, body
TLS (TCP/443)	certificate request	certificate, cipher suite
HTTP (TCP/8080)	HTTP `GET` request	header, version, body

Otherwise, a large "same" proportion indicates that more UEs and CPEs (this kind of CPE's *WAN IPv6 Prefix* is the same with the *LAN IPv6 Prefix*) are uncovered.

This section shows that probing the sub-prefix space within one IPv6 block is entirely much more feasible and productive than scanning the enormous 128-bits address. Utilizing XMap, the previously hard-to-find periphery could be discovered fast. Thus, its security issue surfaces are also exposed widely, which have not been well-studied. Therefore, researchers should pay more attention to it. Instantly, we explore its network security issues in the following two sections, including the unintended exposed services and vulnerable routing loops, which can lead to serious security consequences once being exploited.

V. VULNERABLE UNINTENDED EXPOSED SERVICES

Application services, running on the periphery, usually only serve the internal networks, which should not be made public to the Internet. For example, in the IPv4 network, owing to the NAT, the home router's login page and DNS service are merely approachable by the internal devices. Differently, IPv6 brings globally unique addresses for the periphery and potential risks of being accessed by arbitrary users on those services.

In this section, we conduct a systematical measurement on 7 popular and crucial periphery's security services (should not be made public), based on discovered peripheries. Moreover, we discover *4.7M* devices with such *unintended exposed services* open to the Internet, e.g., DNS, HTTP, and TELNET, affecting at least *108* device vendors. Besides, the vast majority of these services are running significantly lagging software released *8-10* years ago, such as *142k* identified DNS resolvers running dnsmasq 2.4x (released ∼*8* years ago) facing the risks of being exploited. The service protection policies on those peripheries are inadequate, and we prompt immediate guarantees for them.

A. Security Services Probing

We probe the services listed in Table VI on all discovered peripheries. These security services are selected because they are (*i*) likely to be running on CPEs (e.g., DNS), (*ii*) critical to the CPE operation (e.g., HTTP, and SSH), or (*iii*) problematic when being exploited (e.g., NTP [75]).

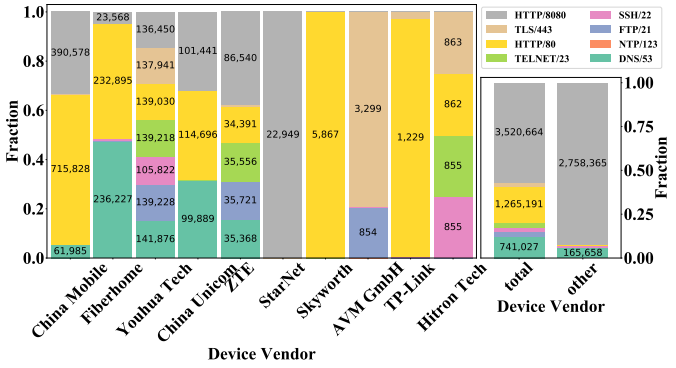


Fig. 2. Results of Top 10 Periphery Device Vendors with Exposed Services

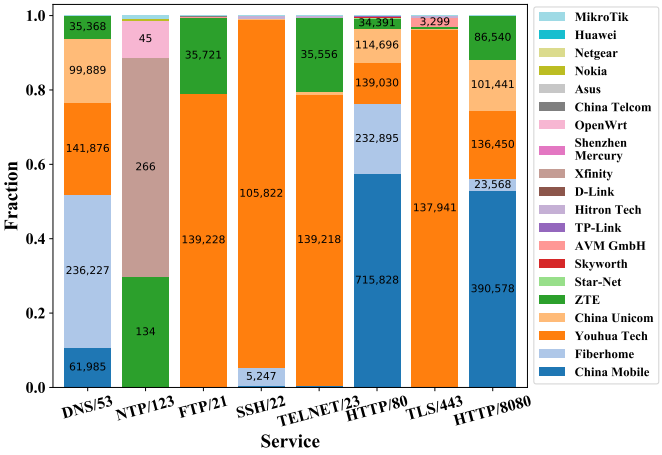


Fig. 3. Results of Top 20 Periphery Device Vendors within Each Service

We only choose seven security services in order to minimize the load on targets. Each service is probed just once, and no >1 services are probed simultaneously at the same target address.

The application-specific requests and valid counterpart responses for each service are listed in Table VI. For TCP, a SYN request is sent firstly to check the port openness. For UDP and open TCP ports, then, we send the application-specific request. If a valid response is received, we conclude that the service on one target is active. We use the ZGrab2 tool [92] to collect the basic application-level information, probing at 1000 pps rate and never attempt to conduct further connecting and weakness exploiting, following all the ethical steps in Section IV-D.

B. Measurement results

Overall, we find unintended exposed services becoming an emerging security risk in IPv6 networks. Specifically, we discover *4.7M* unique IPv6 peripheries (9% of all the peripheries) with as least one service alive. The number and proportion of peripheries within each service and ISP are listed in Table VII. For instance, *741k* (1.4%) devices providing DNS resolution services turn out to be DNS forwarders (home routers). *1.3M* (2.4%) routers' web management pages (HTTP/80) could be accessed by arbitrary external visitors. *138.6k* (0.3%) routers open remote login access (SSH/22) through the IPv6 network.

We use MAC addresses [45] embedded in EUI-64 addresses and application-level provider information to identify the device vendors. Finally, we confirm *1.7M* devices with explicit vendor affiliation, which are from the CPE device providers.

Figure 2 shows the top 10 most-frequently appeared vendors and the number of devices with alive services, which are liable to open. The top two most-opening services are *HTTP (4.8M) and DNS (741k)*. For example, devices from China Mobile are prone to open HTTP/80 (8080) and DNS/53 services to public IPv6 networks, whereas StarNet's devices only tend to expose HTTP/8080 to external visitors. All of the selected 7 services except NTP are accessible for Youhua Tech's devices.

Besides, Figure 3 demonstrates the number and proportion of top 20 vendors within each service and presents which vendor is likely to place some services open. Among the services, several services are contributed by numbers of vendors, e.g., DNS (China Mobile, Fiberhome, Youhua Tech, ZTE), while some are mainly supplied by two or three vendors, e.g., SSH (Fiberhome, Youhua Tech) and TELNET (Youhua Tech, ZTE).

For each service, we discuss its application-level results and possible impacts. The most-frequently used software (version, device number) are listed in Table VIII, including the number of existing CVEs (from CVE database [83]), which are likely leveraged to exploit the device with specific software version.

DNS. The IPv6 hitlist [33] holds ∼300k UDP/53 responsive addresses in Nov 2020 and Hendriks et al. uncover 1,038 IPv6 DNS resolvers [42]. Park et al. find the number of IPv4 open DNS resolvers has decreased significantly from 12M in 2013 to 3M in 2019 [69]. However, we still find *741k* active IPv6 open DNS resolvers within 15 sample IPv6 blocks.

As for the DNS software, we find out the software running on those devices is chiefly dnsmasq with a version from 2.4x to 2.7x, released 2-8 years ago. 16 vulnerabilities could impact such devices, e.g., DoS and buffer overflow bugs. Additionally, accessible DNS service can (*i*) leak internal-only DNS records and cache, and (*ii*) facilitate DDoS attacks for IPv6 [42].

For example, both 28k devices from Reliance Jio and 23k devices from Bharti Airtel are running dnsmasq 2.7x. In China Mobile's broadband network, devices opening DNS services are mainly from Fiberhome (198k), Youhua Tech (142k), and China Mobile (62k). Thereinto, the software on 141k Youhua Tech devices is dnsmasq 2.4x released ∼8 years ago.

HTTP and HTTPS. Respectively, We find *1.3M* (HTTP/80), *3.5M* (HTTP/8080), and *144k* (TLS/443) active devices. The most-frequently adopted web servers are listed in Table VIII, which turn out to be the embedded web applications notorious for vulnerabilities. *1.1M* routers with web management pages enabled on port 80 are accessible from arbitrary external IPv6 networks, which is identified by the login keywords along with manual validation. *3.5M* Jetty servers are approachable for the whole Internet users to access their 8080 ports. Those devices are mainly from China Mobile. Besides, the results show that the security posture is worse on the HTTP services because the web application is commonly deployed in every home router and should not be accessed by arbitrary users through IPv6.

SSH. *138.6k* devices show a serious version lagging on SSH software, including dropbear (*112k*) with version 0.4x released before 2006 and openssh 3.5 (469) released in 2002. 74 CVEs

TABLE VII
RESULTS OF ALIVE SERVICES ON PERIPHERIES WITHIN EACH ISP (DEVICE NUMBER AND PROPORTION OF ALL DISCOVERED PERIPHERIES)

P	DNS-53		NTP-123		FTP-21		SSH-22		TELNET-23		HTTP-80		TLS-443		HTTP-8080		Total	
	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%
1	**30.3k**	0.9	6	0	1	0	9	0	1	0	102	0	0	0	**1.4k**	0	**31.8k**	0.9
2	4	0.2	88	3.7	21	0.9	89	3.7	55	2.3	24	1.0	20	0.8	4	0.2	189	**7.9**
3	**36.6k**	0.2	131	0	27	0	50	0	19	0	**1.0k**	0	0	0	**6.7k**	0	**44.5k**	0.2
4	201	0	39	0	0	0	13	0	2	0	141	0	0	0	623	0	**1.0k**	0
5	9	0	290	0.3	5	0	13	0	50	0.1	54	0.1	64	0.1	319	0.4	423	0.5
6	**3.6k**	0.5	320	0	880	0.1	223	0	13	0	340	0	**3.4k**	0.5	0	0	**8.3k**	**1.1**
7	437	3.4	58	0.4	1	0	46	0.4	3	0	31	0.2	372	2.9	357	2.7	**1.3k**	**9.7**
8	**3.6k**	**1.4**	**14.9k**	**6.0**	**1.0k**	0.4	**1.9k**	0.8	**1.5k**	0.6	38	0	**3.0k**	**1.2**	2	0	**23.8k**	**9.5**
9	0	0	0	0	0	0	3	0	2	0	625	0	625	0	489	0	**1.1k**	0.1
10	93	0.2	129	0.3	14	0	**1.2k**	**3.0**	**1.1k**	**2.7**	**2.6k**	**6.8**	**1.3k**	**3.4**	55	0.1	**3.2k**	**8.3**
11	**63.6k**	**3.0**	146	0	211	0	335	0	240	0	791	0	51	0	7	0	**64.5k**	**3.0**
12	**202.3k**	**15.9**	76	0	**35.8k**	**2.8**	**20.5k**	**1.6**	**36.5k**	**2.9**	**211.0k**	**16.6**	169	0	**229.5k**	**18.0**	**313.3k**	**24.6**
13	**403.0k**	**5.5**	19	0	**139.4k**	**1.9**	**114.2k**	**1.6**	**140.2k**	**1.9**	**1.0M**	**14.3**	**138.2k**	**1.9**	**3.3M**	**44.8**	**4.2M**	**57.5**
14	468	0	21	0	0	0	8	0	5	0	147	0	4	0	176	0	678	0
15	296	0	122	0	0	0	133	0	130	0	96	0	1	0	236	0	718	0
Total	**741.0k**	**1.4**	**16.1k**	0	**176.6k**	0.3	**138.6k**	0.3	**179.7k**	0.3	**1.3M**	**2.4**	**144.2k**	0.3	**3.5M**	**6.7**	**4.7M**	**9.0**

India: **1**: Reliance Jio^{b}, **2**: BSNL^{b}, **3**: Bharti Airtel^{m}, **4**: Vadafone^{m} **America:** **5**: Comcast^{b}, **6**: AT&T^{b}, **7**: Charter^{b}, **8**: CenturyLink^{b}, **9**: AT&T^{m}, **10**: Mediacom^{e}
China: **11**: Telecom^{b}, **12**: Unicom^{b}, **13**: Mobile^{b}, **14**: Unicom^{m}, **15**: Mobile^{m}, **P:** ISP **Network:** ^{b}: Broadband, ^{m}: Mobile, ^{e}: Enterprise Probing Date: Nov 2020

TABLE VIII
TOP SOFTWARE VERSION AND DEVICE NUMBER OF CRUCIAL SERVICES

Service	Top Software & Version (# device)	# CVE
DNS	dnsmasq-2.4x (142k), dnsmasq-2.5x (3.6k) dnsmasq-2.6x (2.4k), dnsmasq-2.7x (52k)	16
HTTP	Jetty (3.5M), MiniWeb HTTP Server (655k) micro_httpd (462k), GoAhead Embedded (2.4k)	24
SSH	dropbear 0.46 (6k), 0.48 (106k), 0.5x (937) 2012.55 (20k), 2017.75 (3k), 2011-2019.x (233)	10
	openssh 3.5 (469), 5.x (27) 6.x (144), 7.x (118), 8.x (35)	74
FTP	GNU Inetutils 1.4.1 (139.3k), Fritz!Box (1.6k)	-
	FreeBSD version 6.00ls (136)	1
	vsftpd 2.2.2, 2.3.4, 3.0.3 (102)	2

could be used to exploit such devices for (*i*) DoS attacks, (*ii*) code execution, and (*iii*) bypassing. Via brute-force password attempts and privileges gaining vulnerability, the adversary can conduct stealthy attacks, e.g., man-in-the-middle attacks.

FTP. 4 FTP software are running on the *176.6k* FTP servers. FreeBSD version 6.00ls and vsftpd are far away from updating, bringing in 3 existing CVEs. The FTP service provides access to fetch the router's file system, potentially representing a back door chance for adversaries to login using a default password.

TELNET. Among *179.7k* TELNET servers, we recognize *37k* devices with forthright vendor banners (China Unicom, Yocto, OpenWrt). Even though there is no software indicating CVEs, the TELNET server itself is a threat for that the plain text and weak passwords can be compromised to gain broader access.

NTP. For the NTP service, we just send a request to check its visibility. All the exposed NTP servers (*16k*) are deployed with NTP version 4 services, and 93% of the servers are located in CenturyLink's networks. Even if there is also no information to imply related vulnerability, NTP can be and has been leveraged for large-scale DDoS attacks with huge amplifiers [26], [75].

Those results show the service discrepancy observed among different vendors' peripheries in practice and the IPv6 network security policy and posture disparity. In any case, the existence of device services accessible by outer undesired users means the security audits and policies are not adequate and appropriate. This also calls on the device vendors to build their devices paying more attention to the IPv6 security protection and the users to operate their routers with more cautions. Otherwise, such devices and services can be exposed quickly, and related vulnerabilities could be leveraged stealthily.

VI. ROUTING LOOP ATTACK

In this section, we find a widespread implementation defect of the IPv6 packet routing and forwarding strategy, which can result in routing inconsistencies between the ISP routers' and the CPE routers' IPv6 routing state. Attackers can exploit this kind of inconsistency to conduct traffic forwarding loop attacks between the ISP routers and the home routers with an amplification factor of *>200*. With the ability to mount fast periphery scanning, first, we carry out a comprehensive measurement to show how widely this routing loop is distributed in the world. Second, based on discovered peripheries, although as a sample, we investigate how many devices and vendors are vulnerable to the routing loop attack. Our results show that *5.8M* routers from at least *49* device vendors distributing in *3.8k* ASes and *132* countries are affected by this *routing loop attack*.

A. Threat Model of Routing Loop Attacks

As Section II and Section III-A describe, the ISPs tend to delegate or assign large IPv6 sub-prefixes (such as /60 and /56) to their subscribers, which shifts the prefix management tasks from the ISP routers to the CPE routers, requiring careful and correct operations. However, due to the new address allocation principles and empirical practices from IPv4 networks, several vendors implement the CPE routers' IPv6 packet routing modules incorrectly, resulting in the traffic routing loop attacks.

As shown in Figure 4, the ISP router P (IPv6p) assigns the *WAN Prefix* and delegates a *LAN Prefix* to the CPE router R (IPv6r) and dispose the next-hop with the CPE's *WAN Address*. The CPE router assigns one *Subnet Prefix* to its LAN network and set the next-hop of it to LAN devices, setting the *Not-used Prefixes* to default the next-hop IPv6p (lacking an unreachable route). Attackers exploit this by crafting a packet routed to an

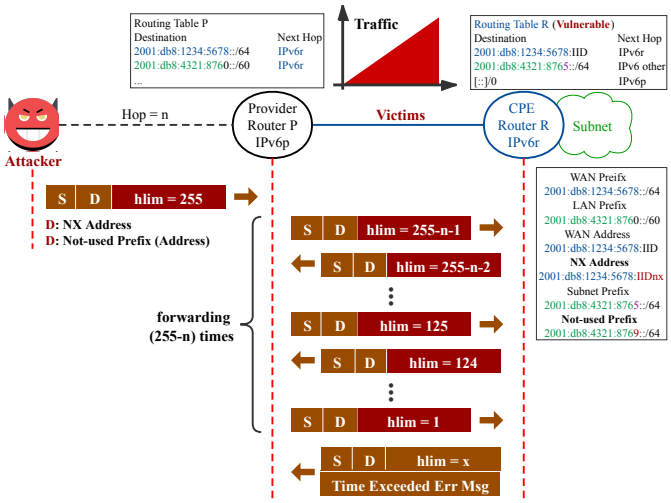


Fig. 4. Illustration of the Routing Loop Attack

address within the *Not-used Prefix* that is not used in the LAN network, e.g., 2001:db8:4321:8769::/64. In that routing state, the ISP router forwards the packet to the CPE router, whereas the CPE router forwards it back to the ISP router. As a result, such a packet's forwarding brings about traffic loops in the link between both routers. These two routers and the link between them become victims of the loop. Similarly, some CPE routers just add a route for its *WAN Address* within the *WAN Prefix* and leave the remaining addresses (*NX Address*) to be matched by the default route when forwarding, inducing the loop as well.

In practice, any routing inconsistency between the upstream router and the downstream router could cause a traffic forwarding loop both in the IPv4 and IPv6 networks. However, *due to the sizeable IPv6 prefix, such a loop is more typical for IPv6.*

A forwarding loop terminates when the *Hop Limit* field in the IPv6 header is zeroed out, called *Time-exceeded* [24]. This field's maximum value is *255*. We assume the hop count prior to the ISP router is *n*, and the remaining count is *255-n*. Each packet will traverse both routers *(255-n)/2* times. So, the loop can be used to amplify traffics with a ratio of *255-n*. Notably, a previous study shows that not every AS adopts source address filtering mechanism [55], which means that by faking source IPv6 address, we can force the response packet to be forwarded to the *Not-used Prefix* as well, doubling the loop times.

B. Measurement Methodology

To measure the affected population and extent of the vulnerable devices, we use XMap to locate the routing loop devices. **Method.** Suppose that we discover a packet forwarding loop, we can deduce something is wrong with the target router. Accordingly, if a device replies with an ICMPv6 Time-exceeded message just in response to a crafted ping packet with a large Hop Limit *h* described in Section VI-A, we send the same crafted packet again but using a Hop Limit *h+2*. If a Time-exceeded packet comes from the same device once again, we conclude the device is vulnerable to the routing loop weakness.

However, a large Hop Limit will potentially result in many routing loop packets, which overwhelm the target device and network. In contrast, a small Hop Limit will cause the missing of vulnerable devices and lead to false results. Thus, a proper Hop Limit must be selected to balance accuracy and negative impact. In [15], Beverly et al. probed the CAIDA target dataset (BGP-advertised IPv6 prefixes) on May 2, 2018, to evaluate Yarrp6's fill mode. They showed that when the Hop Limit was set to *32*, the fill mode produced no additional probes, which means that the hop count between their vantage points and all the target addresses is <32. Besides, we perform a small and similar test on the dataset from [76] and gain the same results. Accordingly, we adjust the probing Hop Limit *h* to 32 for the fact that the hop count between two addresses is commonly <32 on the Internet to reduce the routing loop impact.

Furthermore, we utilize the MAC address (from the EUI-64 address [45]) and the application-level information (HTTP/80, 8080) to extrapolate the device vendors, and use the MaxMind IP geolocation database [57] to identify the AS and country.

Probing. Above all things, to figure out how widely such loops exist, we contrive a probing test for all globally advertised IPv6 BGP prefixes gathered from the BGP system Routeviews [76]. We scan the successive 16-bits sub-prefix space for each prefix. For example, for BGP prefix 2001:db8::/32, we use XMap to probe every /48 sub-prefixes (from the 32nd to 48th bit) with random IID. Moreover, we carry out a depth-first experiment on the sample blocks (32-bits sub-prefix space) in Table II, to see how many devices and vendors are affected by the loop.

We take the same experiment setup from Section IV-E. Besides, we follow the ethical recommendations in Section IV-D.

TABLE IX
FEATURES OF PERIPHERIES DISCOVERED FROM BGP ADVERTISED PREFIXES SCANNING

Last Hops	# unique	# ASN	# Country
Total	4,029,270	6,911	170
with Routing Loop	128,288	3,877	132

TABLE X
IID ANALYSIS OF LAST HOPS WITH ROUTING LOOP VULNERABILITY

-	# num	%	-	# num	%
EUI-64	22,866	18.0	**Randomized**	59,844	46.7
Low-byte	40,603	31.7	**Byte-pattern**	947	0.7
Embed-IPv4	3,042	2.4	**Total**	128,288	100.0

C. Methodology Results

Vulnerable ASN and Country. The scanning of all IPv6 BGP advertised prefixes brings out ∼*4M* unique last hop addresses involving *6,911* ASes and *170* countries (Table IX). ∼*128k* last hops from *3,877* ASes and *132* countries are vulnerable to the routing loop weakness, and the IID distribution results are listed in Table X. Excepting devices with randomized and EUI-64 address (64.7%, which tend to be peripheries as shown in Section IV-E), devices with low-byte, byte-pattern, and embed-IPv4 address (which are often configured manually) show the same routing loop behaviors in our measurement. We suppose that *the loops on those routers result from the manual route misconfiguration or by script*, and we have contacted the AS administrators to confirm our results. Figure 5 summarizes the Top 10 ASes and countries that produce the largest number of routing loop devices from the IPv6 BGP prefixes scanning.

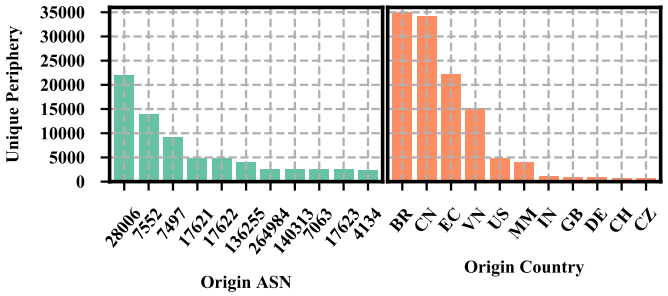


Fig. 5. Top 10 Routing Loop ASN & Country

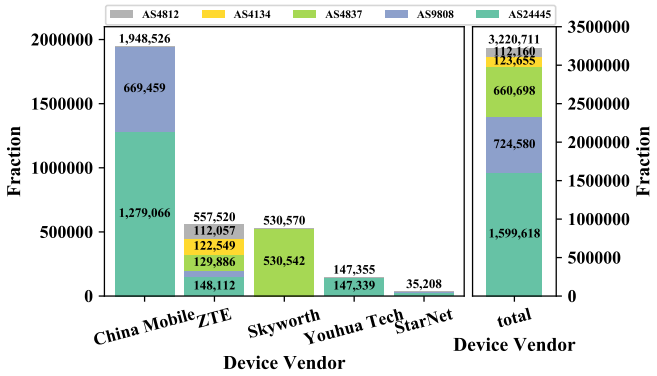


Fig. 6. Top 5 Routing Loop Periphery Device Vendors within Top 5 ASes

Vulnerable Router and Vendor. Targeting towards 15 sample IPv6 blocks, we discover *5.79M* unique peripheries with the routing loop vulnerability within *5.62M* different /64 prefixes. 95.1% of the last hops forward the loop packet due to incorrect routes of *LAN Prefix* (as seen in the "diff" column), while 4.9% of the peripheries mistake the *WAN Prefix* routes (listed in the "same" column). Among them, *3.22M* devices are identified as peripheries, such as home routers, which come from *49* router vendors affected by the loop vulnerability. The 5 most frequent vendors and ASes are shown in Figure 6, including the (total) device number within each device vendor and AS. Owing to the biased target IPv6 prefix, the primarily vulnerable vendors come from China, such as China Mobile [59] and ZTE [93]. However, several devices from Netgear [64], Linksys [52], Tenda [82], MikroTik [58], Optilink [67], Xiaomi [90], and Totolink [85] are vulnerable to the loop as well.

D. Case Study

To study the real loop behaviors and the impact, we analyze *95* sample home routers from *20* well-known router vendors and *4* open-source routing OSes installed in VMware platform, which are all updated to their up-to-date firmware by Dec 1st, 2020 and linked to a broadband home network. The WAN is assigned a /64 prefix, and the LAN is delegated a /60 prefix.

Testing Results. For each router, we send one crafted packet with Hop Limit 255 to a destination from the *Not-used Prefix* within its *WAN Prefix* and *LAN Prefix* respectively. Then we observe their routing tables and traffics to decide whether the routing loop exists or not and the loop times. Their vulnerable behaviors of partial routers and affected device numbers are listed in Table XII. Conforming with our scanning results, all

TABLE XI
RESULTS OF PERIPHERY WITH ROUTING LOOP WITHIN EACH ISP

Cty	Network	Internet Provider	Last Hops (128-bits addr) # uniq	% same	% diff
IN	Broadband	Reliance Jio	8,606	**97.9**	2.1
		BSNL	324	54.3	45.7
	Mobile	Bharti Airtel	**29,135**	**99.2**	0.8
		Vadafone	207	37.2	62.8
US	Broadband	Comcast	31	0.0	100.0
		AT&T	1,598	0.0	100.0
		Charter	373	0.0	100.0
		CenturyLink	**20,055**	0.0	**100.0**
	Mobile	AT&T	2	0.0	100.0
	Enterprise	Mediacom	7,161	0.0	100.0
CN	Broadband	Telecom	**843,375**	4.1	**95.9**
		Unicom	**1,003,635**	3.9	**96.1**
		Mobile	**3,877,512**	4.5	**95.5**
	Mobile	Unicom	190	0.0	100.0
		Mobile	353	0.0	100.0
-	-	**Total**	**5,792,237**	4.9	**95.1**

same: same /64 with probe addr's, **diff**: different /64 from probe addr's
uniq: unique num Sample IPv6 Blocks Scanning in Dec 2020

TABLE XII
ROUTING LOOP ROUTERS TESTING RESULTS AND AFFECTED NUMBER

Brand	Model	Vulnerable Prefix WAN	LAN
ASUS	GT-AC5300 3.0.0.4.384_82037	✓	✗
D-Link	COVR-3902 1.01	✓	✗
Huawei	WS5100 10.0.2.8	✓	✓
Linksys	EA8100 2.0.1.200539	✓	✓
Netgear	R6400v2 1.0.4.102_10.0.75	✓	✓
Tenda	AC23 16.03.07.35	✓	✗
TP-Link	TL-XDR3230 1.0.8	✓	✓
Xiaomi	AX5 1.0.33	✓	✗
OpenWRT	19.07.4 r11208-ce6496d796	✓	✗

ASUS (1), China Mobile (4), D-Link (2), FAST (1), Fiberhome (2), H3C (1)
Hisense (1), Huawei (4), iKuai (3), Linksys (1), Mercury (8), Mikrotik (1)
Netgear (2), Skyworthdigital (9), Tenda (1), Totolink (1), TP-Link (42)
Xiaomi (1), Youhua (1), ZTE (9), DD-Wrt (OS), Gargoyle (OS)
librecmc (OS), OpenWrt (OS) Latest Testing Date: Dec 1st 2020

the 95 routers are vulnerable to the routing loop attack. Routers with the immune prefix respond with an ICMPv6 Destination Unreachable message. Specifically, Xiaomi router, Gargoyle, librecmc, and OpenWrt OS forward such a packet *>10* times, while the other routers and OSes all forward it *(255-n)/2* times.

This section performs systematical measurements to evaluate the impact of a widespread routing loop weakness, which can be contrived to conduct DoS attacks with an amplification factor of *>200*. As a result, we discover *5.79M* routers from *49* vendors existing this loop involving *3,877* ASes and *132* countries, with real testing, which need impending protection.

VII. DISCUSSION

Mitigation. We introduce three fold of mitigation solutions to address the network security issues discovered in our work.

Firstly, we urge that the temporary and opaque IIDs should substitute for the EUI-64 IIDs as recommended by [25], [36], [39], [62]. The EUI-64 format address has been criticized for a long term since [22], [61], because of the drawbacks for hosts tracking, activities correlation, addresses scanning, and device-specific information leaking. However, there is still 7.6% of the discovered periphery using EUI-64 format addresses (Table II).

Secondly, we prompt the IPv6 ping packet should be filtered on the IPv6 periphery. Instantly, vendors should update device firmware, especially the service software, and prevent services from being open to the public by default, following [89]. RFC 4890 [28] describes it is not necessary to filter the IPv6 Echo Request messages due to the large 128-bits address space. But we show that by utilizing the ICMPv6 unreachable message in response to the ping requests, IPv6 peripheries can be exposed fast. Further, we suggest the security community, RFC groups and ISPs inspect the IPv6 packet filtering policy afresh.

Thirdly, to avoid the routing loop as shown above, we advise that "Any packet received by the CE router with a destination address in the prefix(es) delegated to the CE router but not in the set of prefixes assigned by the CE router to the LAN must be dropped", standing in line with RFC 7084 [78]. The CPE router should add an unreachable route for the unused prefix.

In conclusion, we emphasize that the IPv6 periphery is more like a provisioning system. Therefore, its security and all IPv6 network security issues should be reconsidered thoughtfully.

Responsible Disclosure. All found issues were reported to related vendors and ASes. As for the routing loop vulnerability, all *24* vendors confirmed it and patched their routers and OSes, and we received *>106* vulnerability numbers (CNVD/CVE).

VIII. Related Work

IPv6 Active Host Discovery. The state-of-the-art techniques for global IPv6 network reconnaissance mainly includes, active scanning with patterns or structures discovery [32], [38], [53], [60], [79], [86], passive collection [17], [31], [43], [71], [81], and constructing hitlists [30], [33], [34], [79].

The active IPv6 topology probing can also be used to gather IPv6 addresses. Two measurement systems (CAIDA's Ark [20] and RIPE Atlas [74]) perform active IPv6 topology mapping and traceroute ::1 or randomized addresses for each IPv6 prefix in the global BGP table. Beverly et al. adopt [15] randomized traceroute techniques to minimize the effects of rate-limiting and discovered 1.3M IPv6 router interface addresses. C. Rye et al. [77] use traceroute to discover the IPv6 network periphery.

Most recently, Padmanabhan et al. [68] show the sub-prefix assignment often comes from one same /40 block and through scanning prefixes from that /40, the search space for one EUI-64 address is reduced to 2^{64-40}. However, their IPv6 scanning perspective is still limited to the 128-bits end-host probing.

Previous techniques are mainly developed by inferring underlying address patterns and structures with an address generation algorithm, which are constrained by the seeds and time complexity. Besides, they are designed to unearth the 128-bits IPv6 end-host, whereas we aim to discover the IPv6 periphery.

IPv6 Network Security. Previous works declare that the IPv6 network security issues should be taken into account carefully, e.g., host tracking [25], [36], [39], [68], [70], host reputation [50], prefix limiting [27], fragmentation and extension headers security [16], [72], packet filtering policies [14], [28], [89].

Particularly, some research works focus on the IPv6 address security issues, including the IID generation mechanism [14], [15], [34], [71], [77], [86], the prefix agility [71], the delegated prefix rotation [71], [77], and the assignment stability [68].

Specifically, Czyz et al. [14] compared the security policies of dual-stacked servers (520k) and routers (25k) and showed that some ports are more open in IPv6 than IPv4. Besides, they showed that a 1Gbps scanner could scan and identify 90% of routers and 40% of servers from their datasets in <1h, due to the Low-byte and EUI-64 format address. In addition to plenty of EUI-64 addresses, Beverly et al. claimed that they received "Time Exceeded" messages from many addresses covered by one same /64 prefix and urged the community to consider the implications of router-addressing practices [15].

Ullrich et al. [87] discussed a number of security and privacy vulnerabilities concerning IPv6 and their current countermeasures systematically, including 36 security and 14 privacy vulnerabilities. Among them, the routing header of type 0 can form an amplification attack by setting two routers' addresses alternately multiple times in the routing header, deprecated in RFC 5095 [1]. The automatic tunneling mechanisms could also force the routing loops. At a tunnel ingress point, a native IPv6 packet with a spoofed source address is encapsulated into an IPv4 packet and forwarded, while the egress point decapsulates the packet and forwards it back to the ingress point.

Our work serves as a complement to the existing IPv6 security researches. With the ability of fast IPv6 network periphery discovery, we explore the periphery's network security issues.

IX. Conclusion

In this paper, we present the first systematic and large-scale measurement study on the IPv6 network periphery, in order to understand the unintended exposed IPv6 security services and the IPv6 routing strategy implementation flaws. We highlight that, although it is widely recognized that scanning the entire 128-bits IPv6 address space is inefficient, discovering the IPv6 periphery under the small sub-prefix space can be impressively gainful. Moreover, we show that the scope of the unintended exposed IPv6 services is excessive in practice, facing potential security threats. Furthermore, our work reveals the vulnerable implementations on the IPv6 protocol stack. We demonstrate a widespread IPv6 routing loop vulnerability through systematical measurements, which can be used to conduct DoS attacks. Additionally, we release XMap to help the security community carry out IPv6 network measurement studies and responsibly disclose all security issues to related vendors and ASes. Our research results also call for a review of current IPv6 network security strategies and the protocol stack's implementations.

Acknowledgement

Special thanks are sincerely expressed to our shepherd Jia Wang and the anonymous reviewers for their insightful comments, and everyone for giving brilliant assistance. This work is supported in part by the National Natural Science Foundation of China (U1836213, U19B2034, and 61572278) and the BNRist Network and Software Security Research Program (Grant No. BNR2019TD01004). Baojun Liu is partially supported by the Shuimu Tsinghua Scholar Program.

References

[1] J. Abley, P. Savola, and G. V. Neville-Neil, *Deprecation of Type 0 Routing Headers in IPv6*, https://tools.ietf.org/html/rfc5095, RFC 5095 (Proposed Standard), 2007.

[2] AFRINIC, "IPv6 Address Allocation and Assignment Policy," https://www.afrinic.net/library/policies/current/122-afpub-2013-v6-001, 2013.

[3] R. Al-Dalky, M. Rabinovich, and K. Schomp, "A Look at the ECS Behavior of DNS Resolvers," in *Proceedings of the Internet Measurement Conference (IMC '19)*, 2019.

[4] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proceedings of the 26th USENIX Security Symposium (USENIX Security '17)*, 2017.

[5] APNIC, "APNIC guidelines for IPv6 allocation and assignment requests," https://www.apnic.net/about-apnic/corporate-documents/documents/resource-guidelines/ipv6-guidelines, 2013.

[6] APNIC, "APNIC Whois Database," https://ftp.apnic.net/apnic/whois, 2020.

[7] APNIC Labs, "Customer per AS Measurements," https://stats.labs.apnic.net/aspop, 2020.

[8] APNIC Labs, "IPv6 Users by Country," https://labs.apnic.net/dists/v6dcc.html, 2020.

[9] ARIN, "ARIN Whois Database," https://www.arin.net/reference/research/bulkwhois, 2020.

[10] ARIN, "Number Resource Policy Manual," https://www.arin.net/participate/policy/nrpm, 2020.

[11] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Kasper, S. Cohney, S. Engels, C. Paar, and Y. Shavitt, "DROWN: Breaking TLS Using SSLv2," in *Proceedings of 25th USENIX Security Symposium (USENIX Security '16)*, 2016.

[12] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan, "The Menlo Report," *IEEE Security & Privacy*, vol. 10, no. 2, pp. 71–75, 2012.

[13] S. M. Bellovin, B. Cheswick, and A. D. Keromytis, "Worm Propagation Strategies in an IPv6 Internet," *The USENIX Magazine*, vol. 31, no. 1, 2006.

[14] R. Beverly, R. Durairajan, D. Plonka, and J. P. Rohrer, "Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy," in *Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS '16)*, 2016.

[15] R. Beverly, R. Durairajan, D. Plonka, and J. P. Rohrer, "In the IP of the beholder: Strategies for active IPv6 topology discovery," in *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*, 2018.

[16] R. Bonica, F. Baker, G. Huston, R. M. Hinden, O. Troan, and F. Gont, *IP Fragmentation Considered Fragile*, https://tools.ietf.org/html/rfc8900, RFC 8900 (Best Current Practice), 2020.

[17] K. Borgolte, S. Hao, T. Fiebig, and G. Vigna, "Enumerating Active IPv6 Hosts for Large-Scale Security Scans via DNSSEC-Signed Reverse Zones," in *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP '18)*, 2018.

[18] J. J. Brzozowski and G. V. de Velde, *Unique IPv6 Prefix per Host*, https://tools.ietf.org/html/rfc8273, RFC 8273 (Informational), 2015.

[19] C. Byrne, D. Drown, and A. Vizdal, *Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link*, https://tools.ietf.org/html/rfc7278, RFC 7278 (Informational), 2014.

[20] CAIDA, "The CAIDA UCSD IPv6 Topology Dataset," https://www.caida.org/data/active/ipv6_allpref_topology_dataset.xml, 2020.

[21] B. E. Carpenter, T. Chown, F. Gont, S. Jiang, A. Petrescu, and A. Yourtchenko, *Analysis of the 64-bit Boundary in IPv6 Addressing*, https://tools.ietf.org/html/rfc7421, RFC 7421 (Informational), 2015.

[22] T. Chown, *IPv6 Implications for Network Scanning*, https://tools.ietf.org/html/rfc5157, RFC 5157 (Informational), 2008.

[23] T. Chown, J. Arkko, A. Brandt, O. Troan, and J. Weil, *IPv6 Home Networking Architecture Principles*, https://tools.ietf.org/html/rfc7368, RFC 7368 (Informational), 2014.

[24] A. Conta, S. E. Deering, and M. Gupta, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol version 6 (IPv6) Specification*, https://tools.ietf.org/html/rfc4443, RFC 4443 (Internet Standard), 2006.

[25] A. Cooper, F. Gont, and D. Thaler, *Security and Privacy Considerations for IPv6 Address Generation Mechanisms*, https://tools.ietf.org/html/rfc7721, RFC 7721 (Informational), 2016.

[26] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, "Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks," in *Proceedings of the 2014 Internet Measurement Conference (IMC '14)*, 2014.

[27] Dave Plonka, "IPv6 Prefix Intelligence," https://www.ietf.org/proceedings/95/slides/slides-95-maprg-5.pdf, IETF 95 meeting, 2016.

[28] E. B. Davies and J. Mohácsi, *Recommendations for Filtering ICMPv6 Messages in Firewalls*, https://tools.ietf.org/html/rfc4890, RFC 4890 (Informational), 2007.

[29] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: fast internet-wide scanning and its security applications," in *Proceedings of the 22nd USENIX Security Symposium (USENIX Security '13)*, 2013.

[30] X. Fan and J. S. Heidemann, "Selecting representative IP addresses for internet topology studies," in *Proceedings of the 10th ACM SIGCOMM Internet Measurement Conference (IMC '10)*, 2010.

[31] T. Fiebig, K. Borgolte, S. Hao, C. Kruegel, and G. Vigna, "Something from Nothing (There): Collecting Global IPv6 Datasets from DNS," in *Proceedings of the 18th International Conference on Passive and Active Measurement (PAM '17)*, 2017.

[32] P. Foremski, D. Plonka, and A. W. Berger, "Entropy/IP: Uncovering Structure in IPv6 Addresses," in *Proceedings of the 2016 ACM on Internet Measurement Conference (IMC '16)*, 2016.

[33] O. Gasser, Q. Scheitle, P. Foremski, Q. Lone, M. Korczynski, S. D. Strowes, L. Hendriks, and G. Carle, "Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists," in *Proceedings of the Internet Measurement Conference 2018 (IMC '18)*, 2018.

[34] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle, "Scanning the IPv6 Internet: Towards a Comprehensive Hitlist," in *Proceedings of the 8th International Workshop on Traffic Monitoring and Analysis (TMA '16)*, 2016.

[35] GMP, "The GNU Multiple Precision Arithmetic Library," https://gmplib.org, 2020.

[36] F. Gont, *A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)*, https://tools.ietf.org/html/rfc7217, RFC 7217 (Standards Track), 2014.

[37] F. Gont, "IPv6 Toolkit," https://www.si6networks.com/research/tools/ipv6toolkit, 2020.

[38] F. Gont and T. Chown, *Network Reconnaissance in IPv6 Networks*, https://tools.ietf.org/html/rfc7707, RFC 7707 (Informational), 2016.

[39] F. Gont, A. Cooper, D. Thaler, and W. Liu, *Recommendation on Stable IPv6 Interface Identifiers*, https://tools.ietf.org/html/rfc8064, RFC 8064 (Standards Track), 2017.

[40] Google, "IPv6 Adoption Statistics," https://www.google.com/intl/en/ipv6/statistics, 2020.

[41] M. Hastings, J. Fried, and N. Heninger, "Weak Keys Remain Widespread in Network Devices," in *Proceedings of the 2016 Internet Measurement Conference (IMC '16)*, 2016.

[42] L. Hendriks, R. de Oliveira Schmidt, R. van Rijswijk-Deij, and A. Pras, "On the Potential of IPv6 Open Resolvers for DDoS Attacks," in *Proceedings of the 18th International Conference on Passive and Active Measurement (PAM' 17)*, 2017.

[43] Q. Hu, M. R. Asghar, and N. Brownlee, "Measuring IPv6 DNS Reconnaissance Attacks and Preventing Them Using DNS Guard," in *Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '18)*, 2018.

[44] G. Huston, "AS131072 IPv6 BGP Table Data," https://bgp.potaroo.net/v6/as2.0/index.html, 2020.

[45] IEEE Registration Authority, "IEEE Standard OUI data," http://standards-oui.ieee.org/oui.txt, 2020.

[46] ITU/UNESCO Broadband Commission for Sustainable Development, "The State of Broadband: Broadband as a Foundation for Sustainable Development," https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf, 2019.

[47] J. Korhonen, J. Arkko, T. Savolainen, and S. Krishnan, *IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts*, https://tools.ietf.org/html/rfc7066, RFC 7066 (Informational), 2013.

[48] J. Korhonen, J. Soininen, B. Patil, T. Savolainen, G. Bajko, and K. Iisakkila, *IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)*, https://tools.ietf.org/html/rfc6459, RFC 6459 (Informational), 2012.

[49] LACNIC, "IPv6 Address Allocation and Assignment Policies," https://www.lacnic.net/684/2/lacnic/4-ipv6-address-allocation-and-assignment-policies, 2020.

[50] F. Li and D. Freeman, "Towards A User-Level Understanding of IPv6 Behavior," in *Proceedings of the ACM Internet Measurement Conference (IMC '20)*, 2020.

[51] F. Li and V. Paxson, "A Large-Scale Empirical Study of Security Patches," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*, 2017.

[52] Linksys, "Linksys Product Website," https://www.linksys.com, 2020.

[53] Z. Liu, Y. Xiong, X. Liu, W. Xie, and P. Zhu, "6Tree: Efficient dynamic discovery of active addresses in the IPv6 address space," *Computer Networks*, vol. 155, pp. 31–46, 2019.

[54] C. Lu, B. Liu, Z. Li, S. Hao, H. Duan, M. Zhang, C. Leng, Y. Liu, Z. Zhang, and J. Wu, "An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?" in *Proceedings of the Internet Measurement Conference (IMC '19)*, 2019.

[55] M. Luckie, R. Beverly, R. Koga, K. Keys, J. A. Kroll, and k. claffy, "Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, 2019.

[56] Masscan, "MASSCAN: Mass IP port scanner," https://github.com/robertdavidgraham/masscan, 2021.

[57] MaxMind, "GeoIP2 Database," https://www.maxmind.com, 2020.

[58] MikroTik, "MikroTik Product Website," https://mikrotik.com, 2020.

[59] C. Mobile, "China Mobile Product Website," http://products.chinamobiledevice.com, 2020.

[60] A. Murdock, F. Li, P. Bramsen, Z. Durumeric, and V. Paxson, "Target generation for internet-wide IPv6 scanning," in *Proceedings of the 2017 Internet Measurement Conference (IMC '17)*, 2017.

[61] T. Narten and R. Draves, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, https://tools.ietf.org/html/rfc3041, RFC 3041 (Standards Track), 2001.

[62] T. Narten, R. Draves, and S. Krishnan, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, https://tools.ietf.org/html/rfc4941, RFC 4941 (Standards Track), 2007.

[63] T. Narten, G. Huston, and R. G. Roberts, *IPv6 Address Assignment to End Sites*, https://tools.ietf.org/html/rfc6177, RFC 6177 (Best Current Practice), 2011.

[64] Netgear, "Netgear Product Website," https://www.netgear.com, 2020.

[65] newzoo, "Global Mobile Market Report 2020," https://newzoo.com/insights/trend-reports/newzoo-global-mobile-market-report-2020-free-version, 2020.

[66] Nmap, "Nmap Free Security Scanner," https://nmap.org, 2020.

[67] Optilink, "Optilink Official Website," https://optilinknetwork.com, 2020.

[68] R. Padmanabhan, J. P. Rula, P. Richter, S. D. Strowes, and A. Dainotti, "DynamIPs: analyzing address assignment practices in IPv4 and IPv6," in *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '20)*, 2020.

[69] J. Park, A. Khormali, M. Mohaisen, and A. Mohaisen, "Where Are You Taking Me? Behavioral Analysis of Open DNS Resolvers," in *Proceedings of the 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN '19)*, 2019.

[70] D. Plonka and A. Berger, "KIP: A Measured Approach to IPv6 Address Anonymization," *arXiv preprint arXiv:1707.03900*, 2017.

[71] D. Plonka and D. Berger, "Temporal and Spatial Classification of Active IPv6 Addresses," in *Proceedings of the 2015 ACM Internet Measurement Conference (IMC '15)*, 2015.

[72] S. Povolny and M. Bereza, "CVE-2020-16898: "Bad Neighbor"," https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-16898-bad-neighbor, 2020.

[73] RIPE, "Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose," https://www.ripe.net/publications/docs/ripe-690, 2017.

[74] RIPE NCC, "RIPE Atlas," https://atlas.ripe.net, 2020.

[75] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," in *Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS '14)*, 2014.

[76] Routeview, "Routeview 6477," http://www.routeviews.org/routeviews, 2020.

[77] E. Rye and R. Beverly, "Discovering the IPv6 Network Periphery," in *Proceedings of the 21st International Conference on Passive and Active Network Measurement (PAM '20)*, 2020.

[78] H. Singh, W. Beebee, C. Donley, and B. Stark, *Basic Requirements for IPv6 Customer Edge Routers*, https://tools.ietf.org/html/rfc7084, RFC 7084 (Informational), 2013.

[79] G. Song, L. He, Z. Wang, J. Yang, T. Jin, J. Liu, and G. Li, "Towards the Construction of Global IPv6 Hitlist and Efficient Probing of IPv6 Address Space," in *Proceedings of the 28th IEEE/ACM International Symposium on Quality of Service (IWQoS '20)*, 2020.

[80] P. Srisuresh and M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, https://tools.ietf.org/html/rfc2663, RFC 2663 (Informational), 1999.

[81] S. D. Strowes, "Bootstrapping Active IPv6 Measurement with IPv4 and Public DNS," *CoRR*, vol. abs/1710.08536, 2017.

[82] Tenda, "Tenda Product Website," https://www.tendacn.com, 2020.

[83] The MITRE Corporation, "Common Vulnerabilities and Exposures (CVE)," https://cve.mitre.org, 2020.

[84] S. Thomson, T. Narten, T. Jinmei *et al.*, *IPv6 stateless address autoconfiguration*, https://tools.ietf.org/html/rfc4862, RFC 4862 (Standards Track), 2007.

[85] Totolink, "Totolink Product Website," http://totolink.net, 2020.

[86] J. Ullrich, P. Kieseberg, K. Krombholz, and E. R. Weippl, "On Reconnaissance with IPv6: A Pattern-Based Scanning Approach," in *Proceedings of the 10th International Conference on Availability, Reliability and Security (ARES '15)*, 2015.

[87] J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, and E. R. Weippl, "IPv6 Security: Attacks and Countermeasures in a Nutshell," in *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT '14)*, 2014.

[88] W3Techs, "Usage statistics of IPv6 for websites," https://w3techs.com/technologies/details/ce-ipv6, 2020.

[89] J. Woodyatt, *ecommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*, https://tools.ietf.org/html/rfc6092, RFC 6092 (Informational), 2011.

[90] Xiaomi, "Xiaomi Official Website," https://www.mi.com, 2020.

[91] L. Yu, B. Luo, J. Ma, Z. Zhou, and Q. Liu, "You Are What You Broadcast: Identification of Mobile and IoT Devices from (Public) WiFi," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security '20)*, 2020.

[92] ZGrab2, "Fast Go Application Scanner," https://github.com/zmap/zgrab2, 2020.

[93] ZTE, "ZTE Official Website," https://www.zte.com.cn, 2020.