

Fast IPv6 Network Periphery Discovery and Security Implication

Xiang Li, Baojun Liu, Xiaofeng Zheng,
Haixin Duan, Qi Li, Youjun Huang



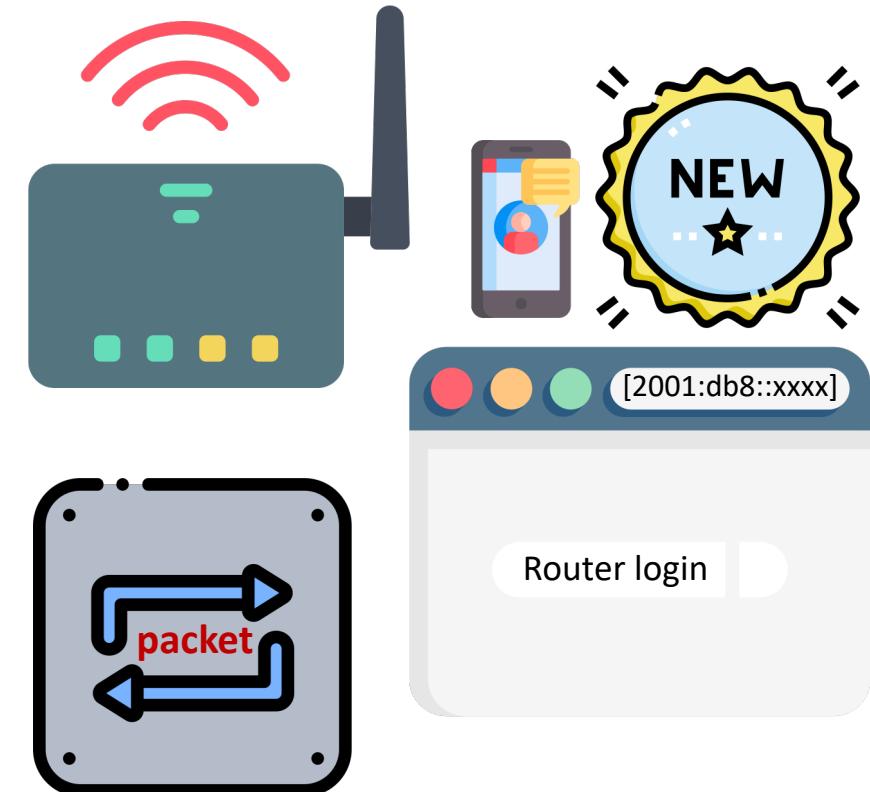
What did we do?



- **New Approach**
 - IPv6 network periphery discovery

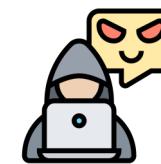


- **New Findings**
 - 52M IPv6 peripheries
 - Unintended exposed services
 - Routing loop attack, **20** vendors, **4** OSes



What did we find?

131 CVE/CNVD



ASUS

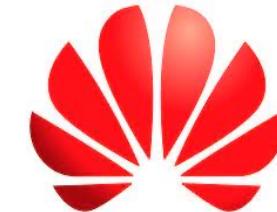
LINKSYS™

NETGEAR®

D-Link®

tp-link

MERCURY



MikroTik

ZTE

mi

Tenda

HUAWEI

Skyworth

中国移动
China Mobile

H3C

TOTO LINK
The Smartest Network Device

FiberHome

FAST

Hisense

友华通信
YOUHUA TECHNOLOGY

OpenWrt®
WIRELESS FREEDOM

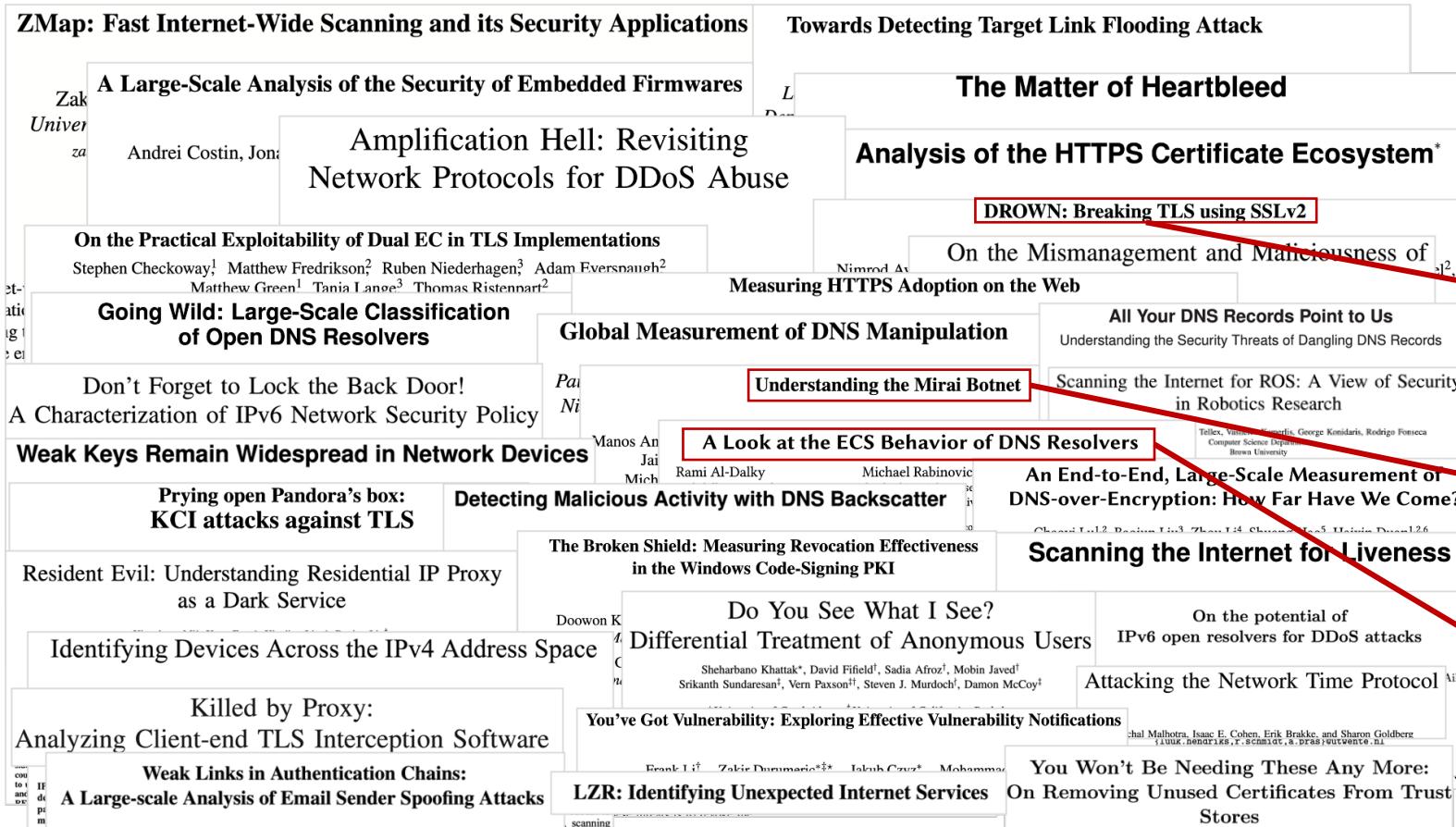
Gargoyle
Router
Management
Utility

DD-WRT

DD-WRT

How to find devices in IPv4?

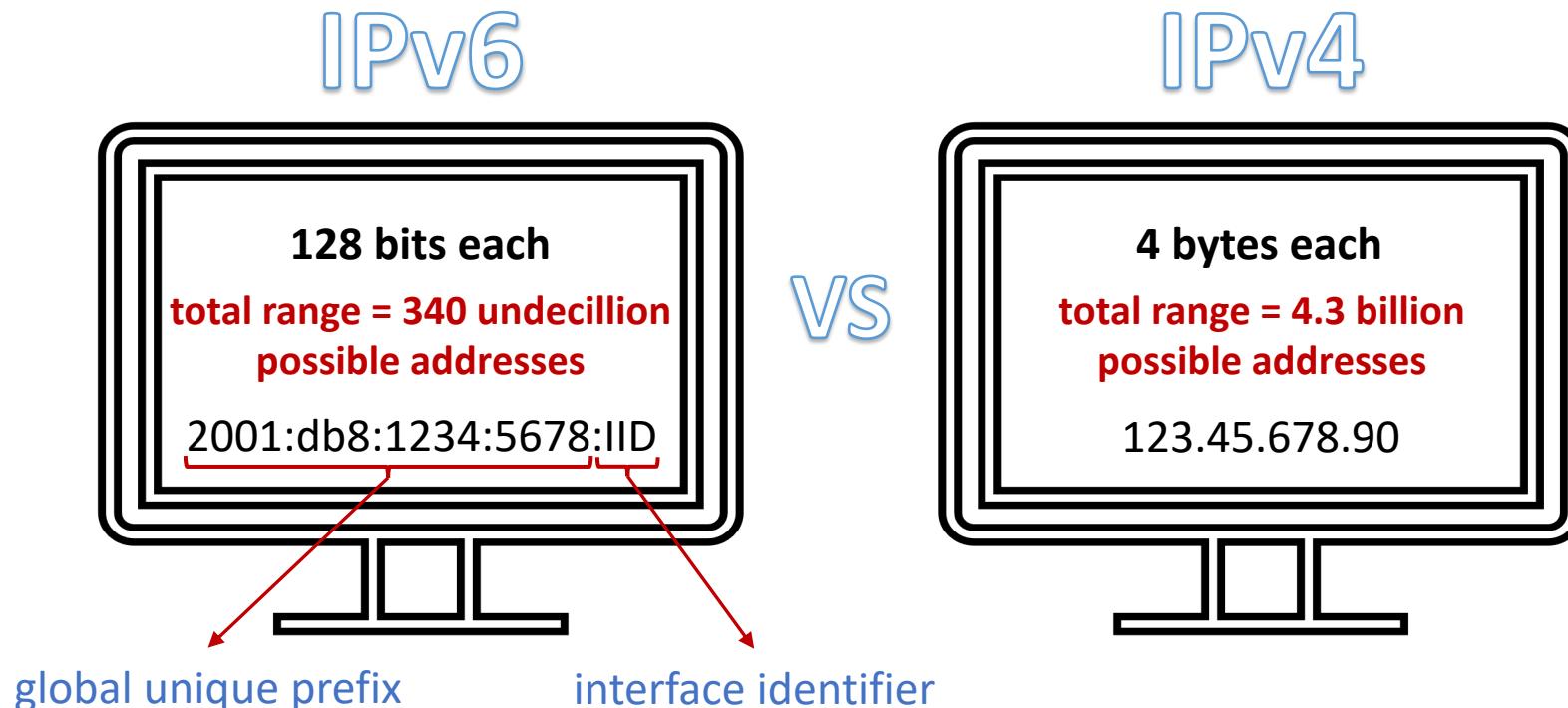
• Network Scanning



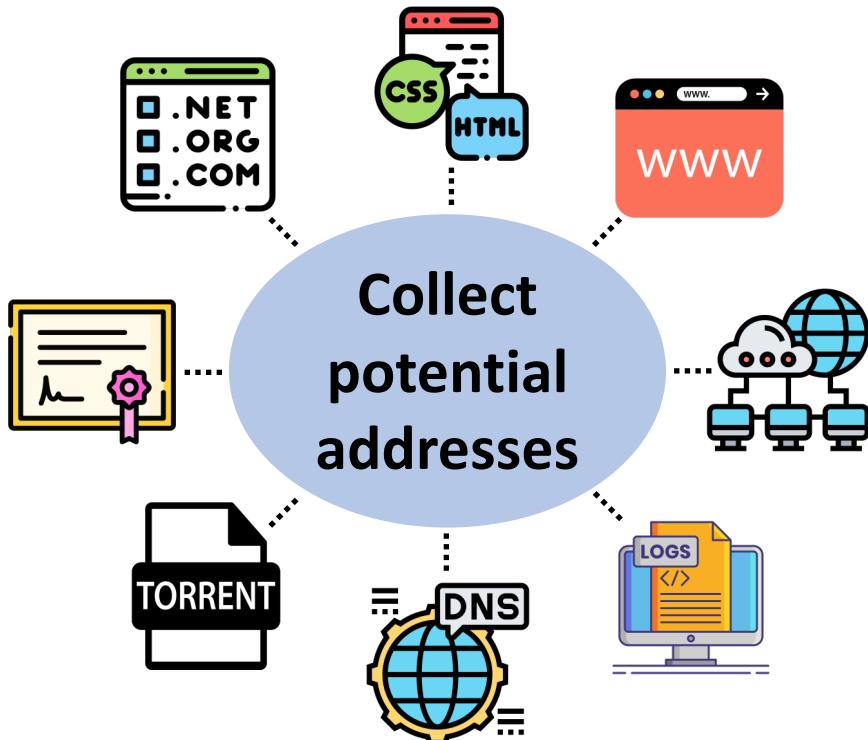
- Uncover vulnerabilities
→ USENIX Security '16
- Track botnets' behaviors
→ CCS '17
- Measure protocol adoption
→ USENIX Security '17
- IMC '19

IPv6 Address Space

- A lot lot lot of addresses
 - 340 trillion trillion trillion addresses
 - IPv4-style brute force won't work

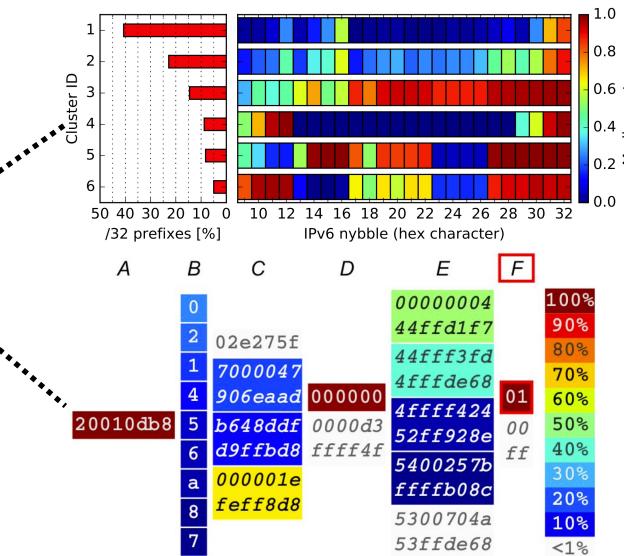


Active IPv6 Host Discovery

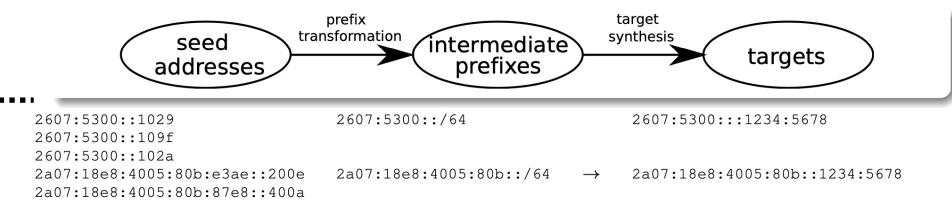


Identify address patterns

Generate candidate addresses



Pawel Foremski, David Plonka, and Arthur Berger. Entropy/IP: Uncovering Structure in IPv6 Addresses. (IMC '16)

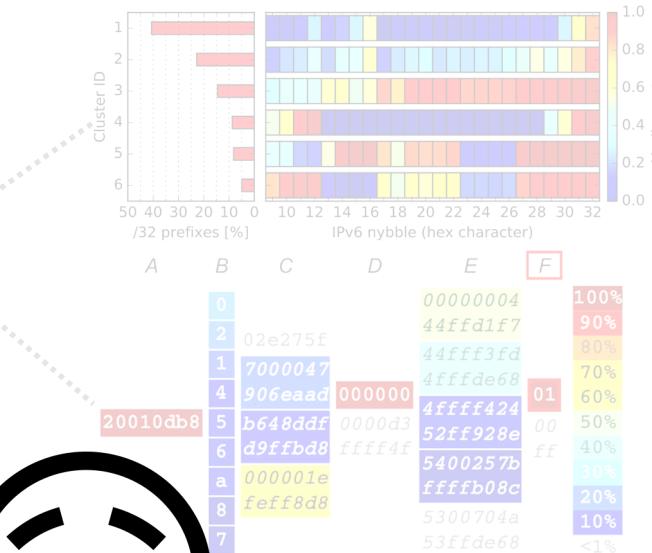


Robert Beverly, Ramakrishnan Durairajan, David Plonka, and Justin P. Rohrer. In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery. (IMC '18)

Active IPv6 Host Discovery



**Not real-time
Not large-scale**



Pawel Foremski, David Plonka, and Arthur Berger. Entropy/IP: Uncovering Structure in IPv6 Addresses. (IMC '16)



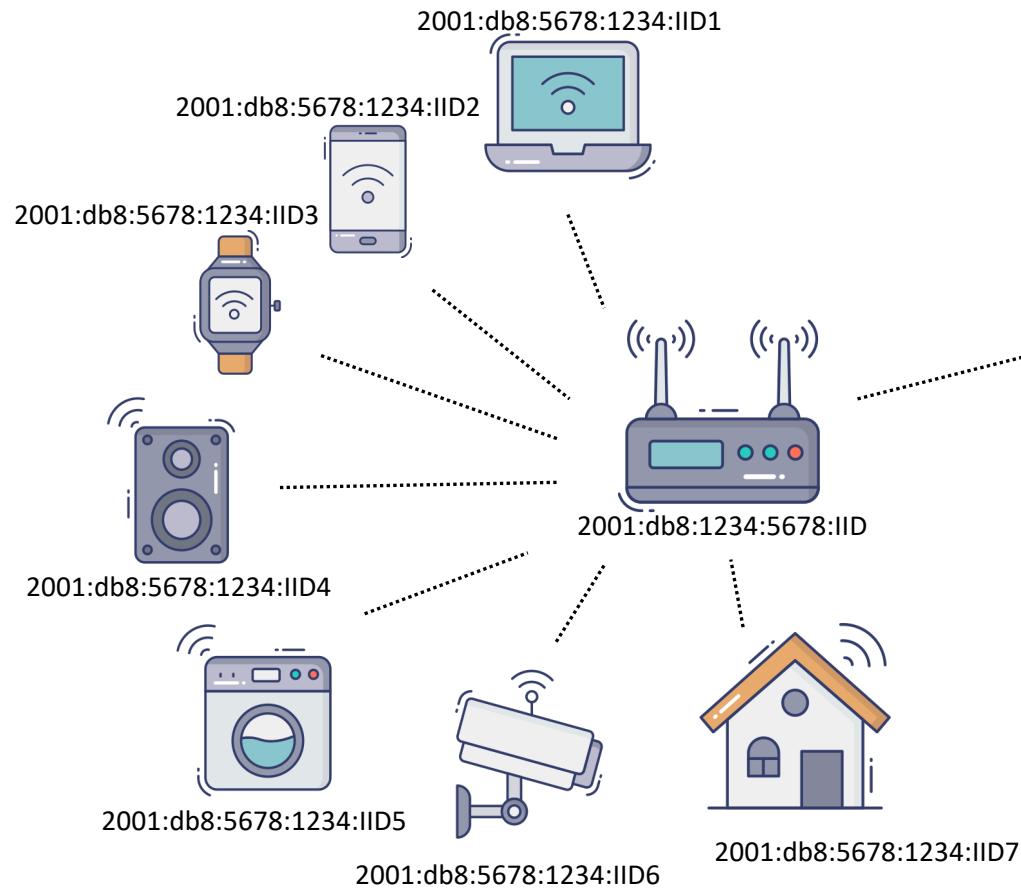
Robert Beverly, Ramakrishnan Durairajan, David Plonka, and Justin P. Rohrer. In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery. (IMC '18)

Our Scanning Perspective

To find the IPv6 network periphery

IPv6 Internet

Home



ISP



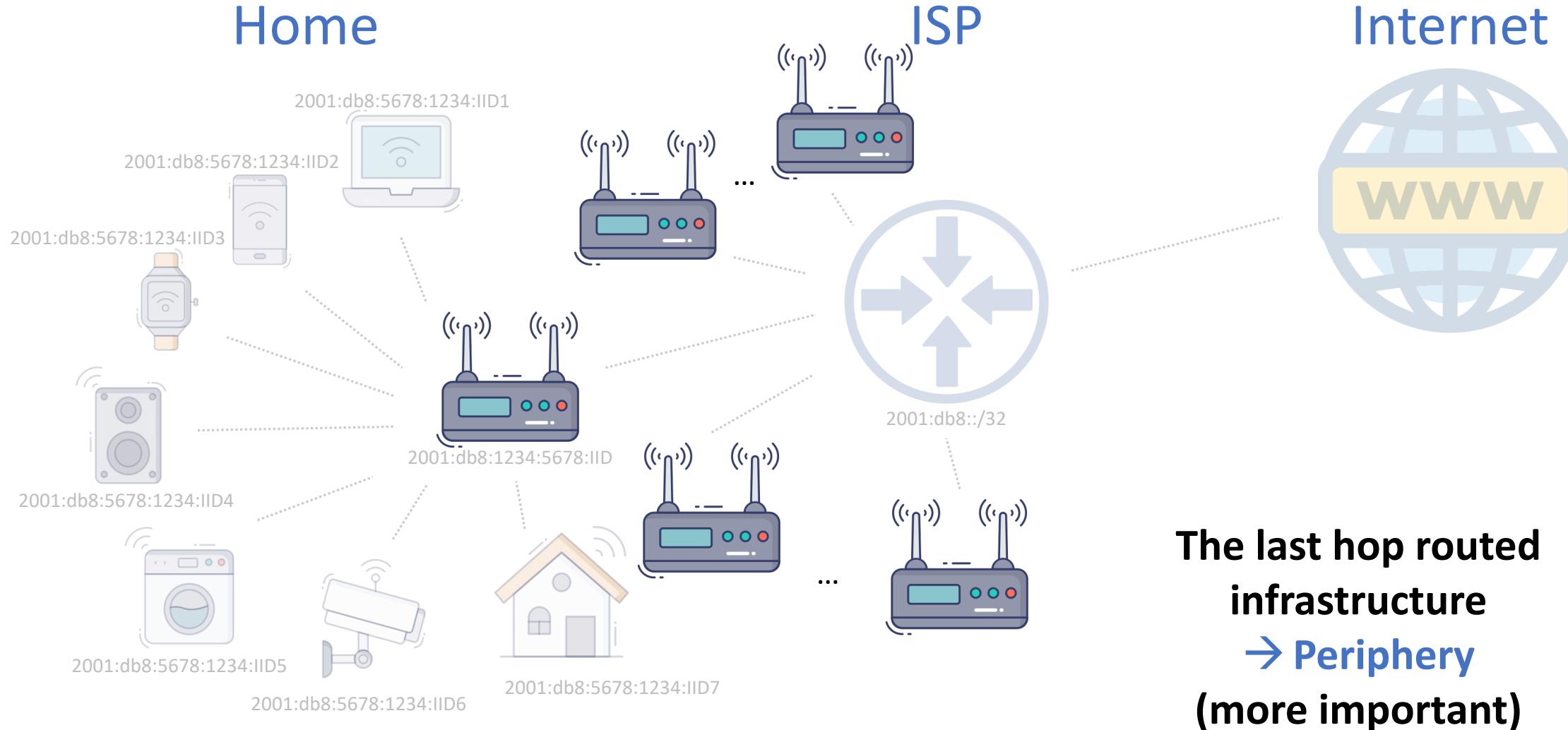
Internet



End User

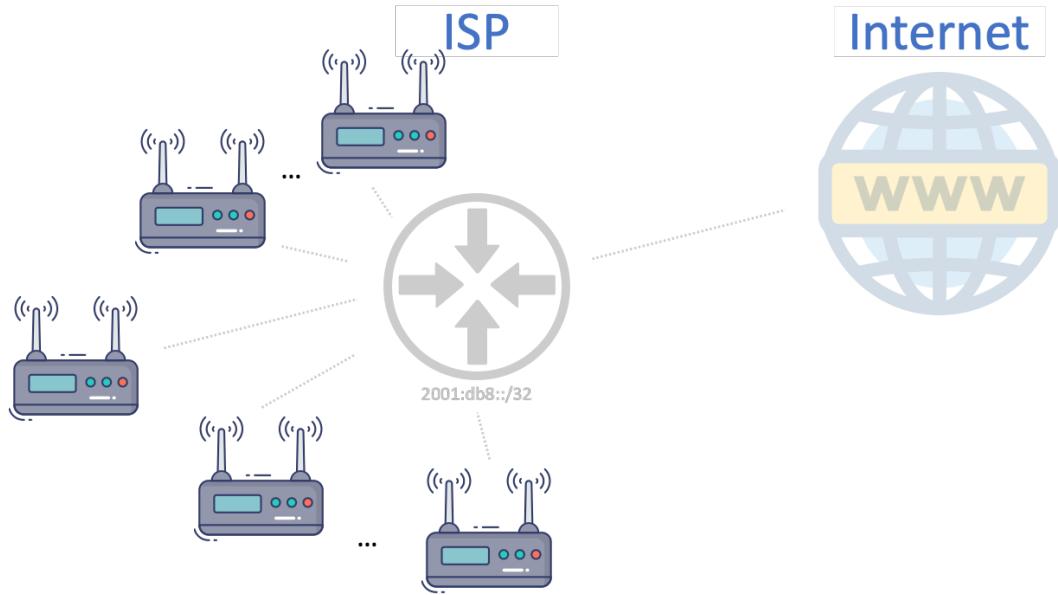
- 1 public IPv6 network
- Public addresses at home

What's IPv6 Network Periphery

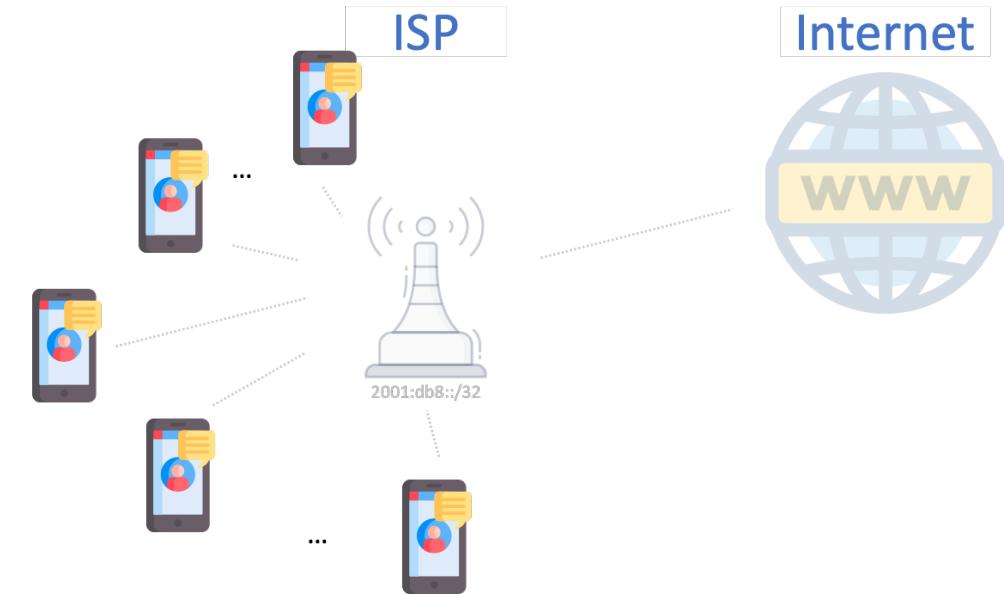


What's IPv6 Network Periphery

Broadband Network

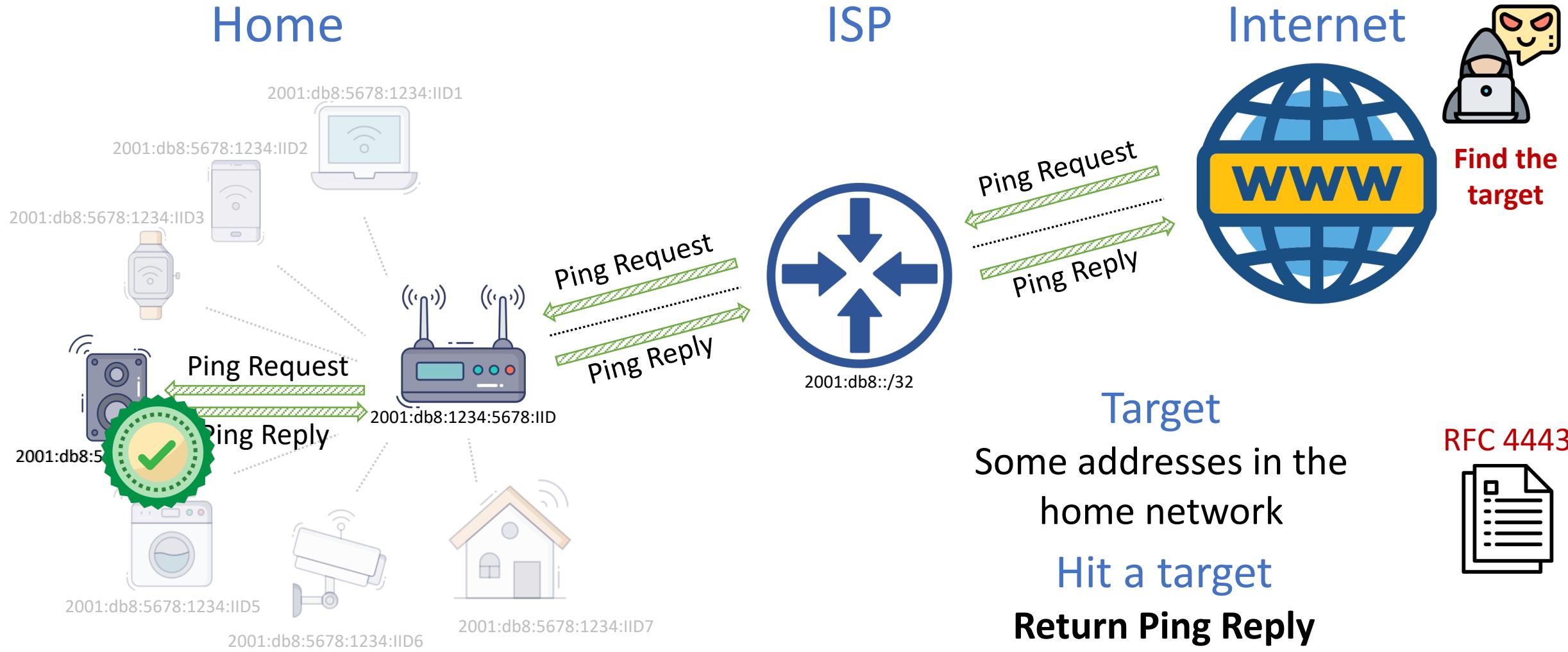


Mobile Network

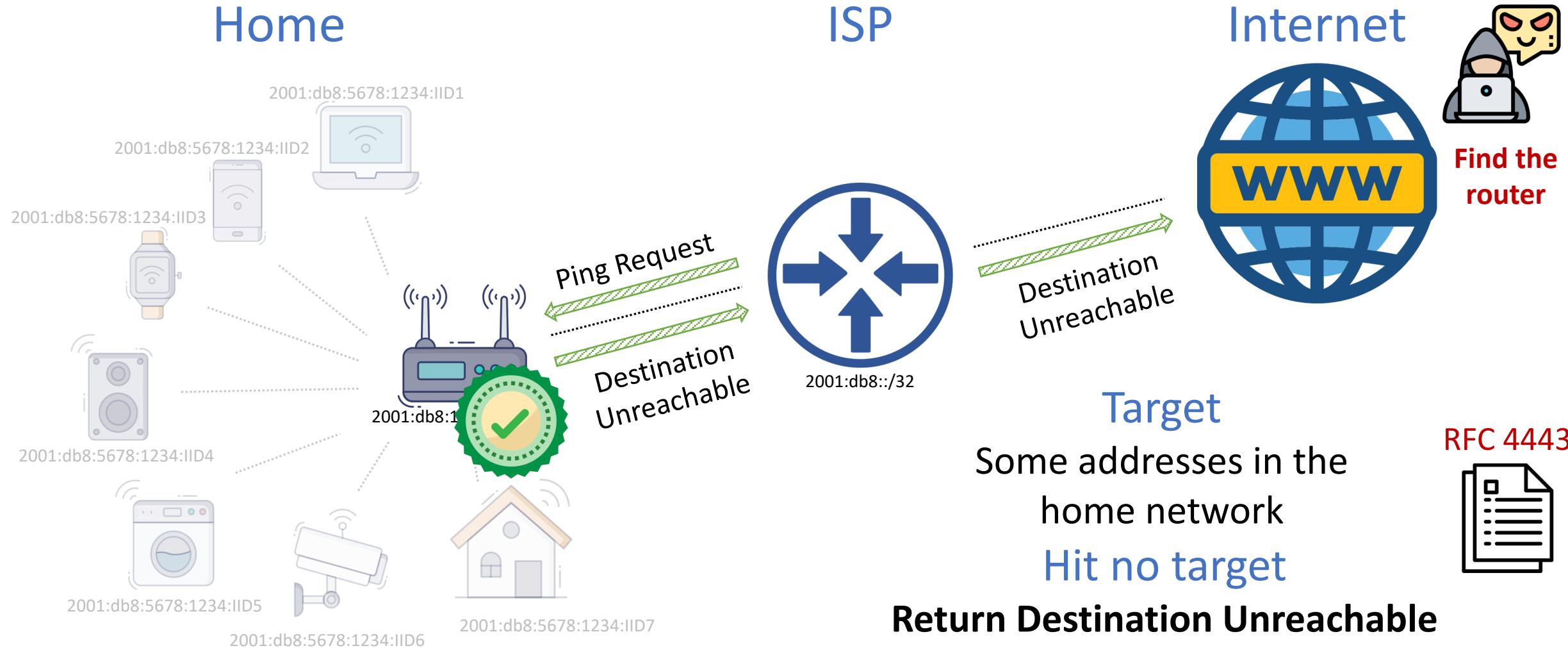


**The last hop routed
infrastructure
→ Periphery**

How to find?

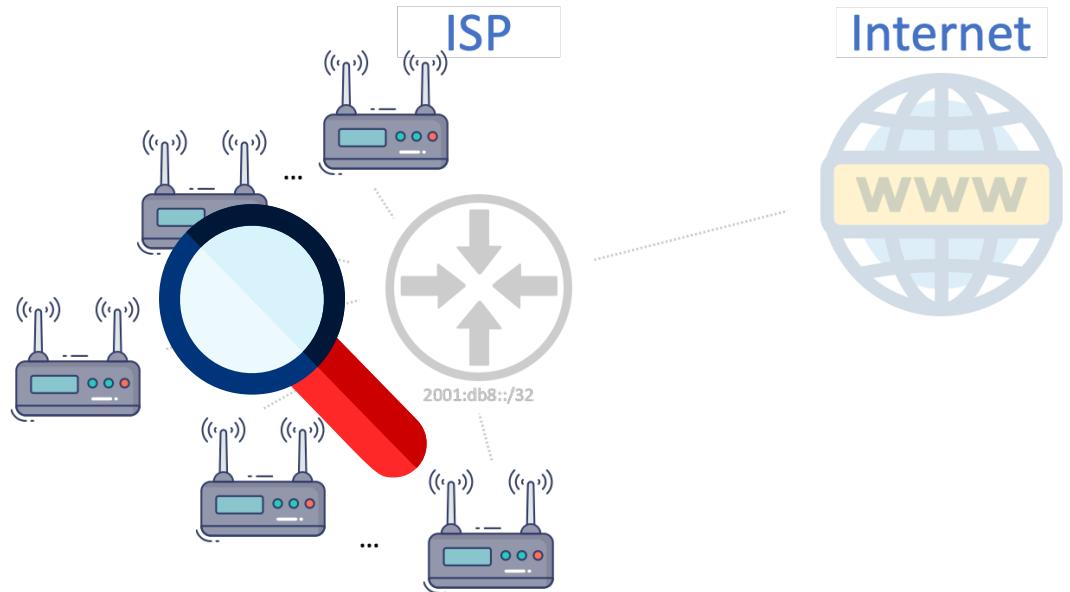


How to find?

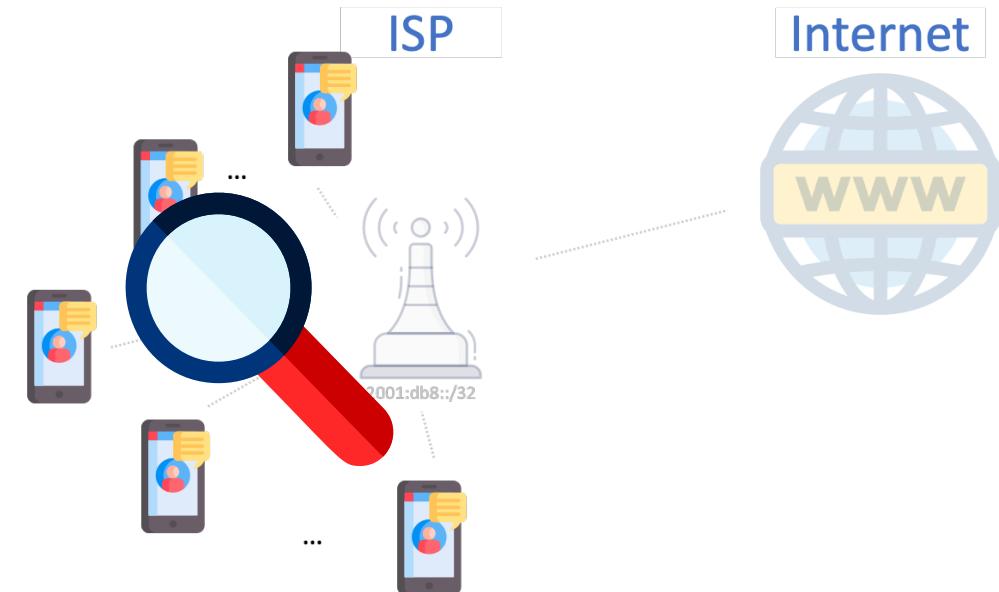


How to find?

Broadband Network



Mobile Network



Scan the IPv6 prefix space

Probe each sub-prefix once for any address under it

How many devices did we find?

- Scanning targets
 - 12 ISPs' 15 IPv6 blocks, sample 32-bit prefix space
 - <15Mbps, 48h for each sample, 52M devices

Country	Network	ISP	# Periphery
Total	3	12	52,478,703
IN	Broadband	Reliance Jio	3,365,175
	Mobile	Bharti Airtel	22,542,690
US	Broadband	AT&T	740,141
	Mobile	AT&T	1,734,506
	Enterprise	Mediacom	38,399
...
CN	Broadband	Telecom	2,122,292
		Mobile	7,316,861
	Mobile	Unicom	3,696,275

Security Implications

- Q1: IPv6 Address Privacy
- Q2: IPv6 Application Services
- Q3: Routing Loop Attack

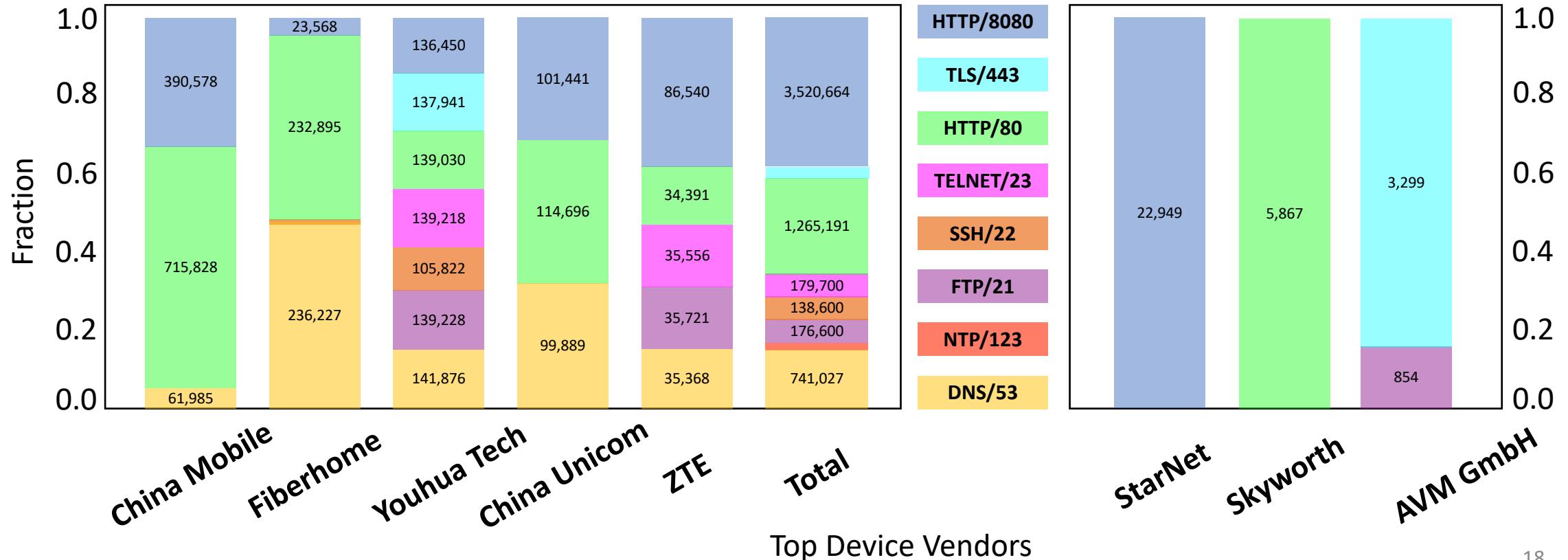
IPv6 Address Privacy

- EUI-64 format IPv6 address
 - Device MAC addresses are embedded into IPv6 addresses
- Still, lots of EUI-64 format addresses
 - Customer premise edge devices, e.g., home routers
 - User equipment devices, e.g., smartphones
 - >62 vendors

Pattern	# device
EUI-64	3.97M
Randomized	39.60M
Low-byte	511.18k
Byte-pattern	5.46M
Embed-IPv4	2.91M
Total	52.48M

IPv6 Application Services: Devices

- Invisible services through IPv4
- Exposed to the Internet via IPv6
 - 4.7M, e.g., DNS, NTP, FTP, SSH, TELNET, HTTP, TLS



IPv6 Application Services: Software

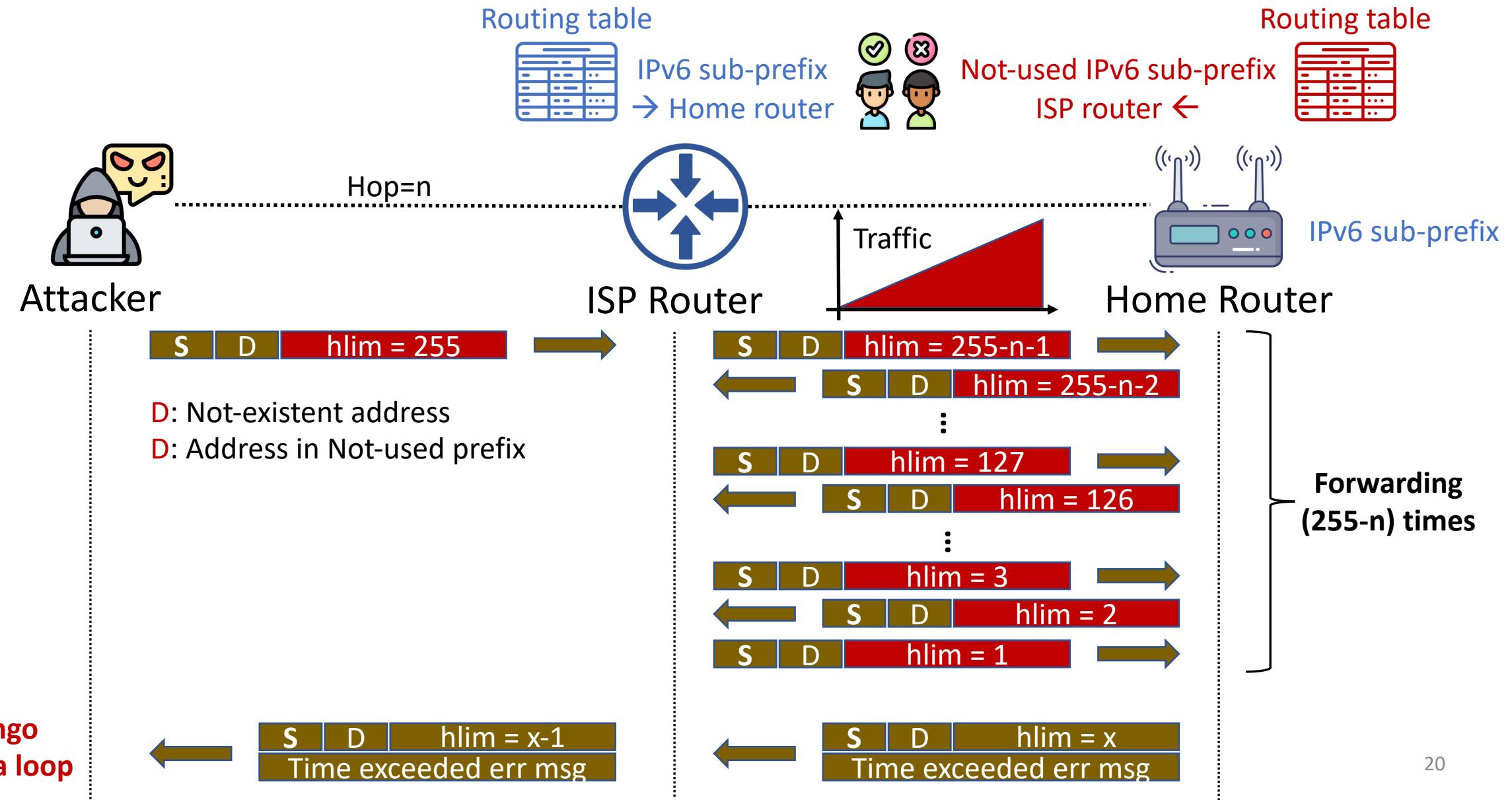
- Most software is released 8-10 years ago
 - e.g., [DNS](#) and [SSH](#)
- Affected by many CVEs

Released ~8 years ago

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
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

Released before 2006

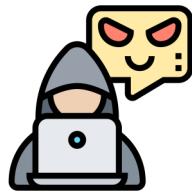
Routing Loop Attack: Threat Model



Routing Loop Attack: Measurement

- How wide is the vulnerability
 - IPv6 BGP prefix probing
- How many devices are under the attack
 - 12 ISPs' 15 IPv6 blocks probing
- Method
 - Use the Time-exceeded msg
- Results
 - 5.8M vulnerable devices
 - 3,877 ASes, 132 countries

Routing Loop Attack: Vulnerable Routers



- 20 router vendors (95 devices), 4 OSes
- All vendors confirm and are fixing

131 CVE/CNVD

ASUS

LINKSYS™

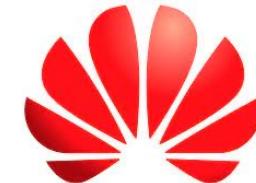
NETGEAR®

D-Link®



tp-link

MERCURY



HUAWEI

MikroTik

ZTE



Tenda

Skyworth



中国移动
China Mobile

H3C

TOTO LINK
The Smartest Network Device

FiberHome

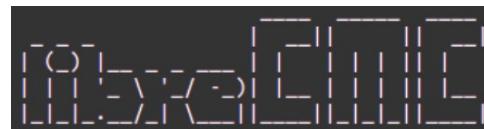
FAST

Hisense

友华通信
YOUHUA TECHNOLOGY

iKuai

OpenWrt®
WIRELESS FREEDOM



DD-WRT

Community Contribution: XMap

- **Open source tool**
 - Rewritten thoroughly from ZMap
 - **Support IPv6 & IPv4**
 - Fast periphery discovery
 - Discovering routing loop vulnerability
 - Multiple ports probing
 - ...
- <https://github.com/idealeer/xmap>
- Everyone can join!!! Maybe star it



Discussion

- **Mitigation**
 - Avoid/Block ICMPv6 ‘reply’ msgs
 - Strengthen access control policies
 - Add unreachable routes for not-used prefixes
- **IPv6 Network Security**
 - IPv6 network peripheries should be focused
 - IPv6 strategies need to be revisited

Questions?

Thank you

x-l19@mails.tsinghua.edu.cn