



UK IPv6 Council  
November 18, 2025

Large-Scale IPv6 Internet Reconnaissance



Scott Hogg

Founder Hogg Networking, Chair Emeritus RMv6TF

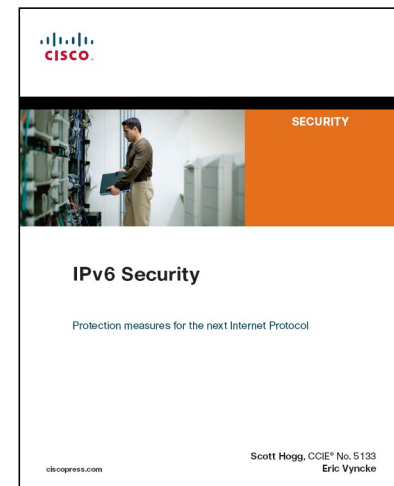
CCIE #5133 (Emeritus), CISSP #4610, CCSP, CCSK, AWS Certified

# IPv6 Reconnaissance



- Targeted attacks begin with reconnaissance.
  - Enumeration, checking registries (whois), DNS (nslookup, dig, etc.), Google hacking, ping sweeps, port scans.
- We presume that IPv6 makes ping sweeps problematic.
  - The address space is immense and seemingly too large to scan.
  - Brute-force scanning a /64 doesn't seem practical.
- Let's do the math, shall we?

$$\frac{18,446,744,073,709,551,616 \text{ addresses}}{\frac{1,000,000 \text{ probes/second}}{\frac{60 \text{ seconds/minutes}}{\frac{60 \text{ minutes/hour}}{\frac{24 \text{ hours/day}}{365 \text{ days/year}}}}} \sim = 584,942 \text{ years}$$





## Network Reconnaissance in IPv6 Nets (RFC 7707, March 2016)

- This RFC covers the recon methods and how IPv6 changes the process.
- IPv6 Address Scanning
  - Address Configuration in IPv6: SLAAC, DHCPv6, manual, transition/coexistence
- IPv6 Address Scanning of Remote and Local Networks
- Existing IPv6 Address-Scanning Tools
- Alternative Methods to Glean IPv6 Addresses
  - DNS, Local Name Resolution and Service Discovery Services
  - Public Archives
  - Application Participation
  - Neighbor Cache and Routing Table
  - System Configuration and Log Files
  - Routing Protocols, IPFIX, SNMP, Traffic Snooping, traceroute6

## Remote Reconnaissance

- We assume that IPv6 prefixes themselves are sparsely allocated.
- Finding an IPv6 prefix may be difficult and communicating with an internal IPv6 network from the Internet perspective may be nearly impossible.
- If an organization is allocated a /32, they have  $2^{32} / 64$  prefixes (4,294,967,296 prefixes).
- However, these are not randomly assigned to networks.
- Over the recent decade, we have developed innovative approaches to finding IPv6 networks and nodes.
- It is now possible to find IPv6 networks and probe them remotely.





## Remote Internet Reconnaissance of IPv6 Nodes

- Many mobile devices do not have host-based firewalls on them, many broadband routers don't have a stateful firewall (no simple security) and may use EUI-64 IIDs (Linux kernel routers, IoT devices, etc.).
- Devices may respond when pinging non-existent IIDs on their /64 networks or respond to the all-zeros subnet anycast address "::".
  - Scanning the IPv6 Internet Using Subnet-Router Anycast Probing, 11/7/25
  - <https://arxiv.org/abs/2511.05423>
- Incrementally increasing the hop-limit value in the scanning traffic may reveal that a device is using a /64 prefix and respond with ICMPv6 Time Exceeded (Hop Limit Exceeded) sourced from its GUA.
- Mobile phones with hotspot/tethering enabled will have shorter IID that can be easily found by scanning.

## Remote Internet Reconnaissance of IPv6 Nodes

- New Ways of IPv6 Scanning Video, By Shupeng Gao, Jie Gao, Xingru Wu (Baidu), Blackhat Europe 2021.
  - <https://www.youtube.com/watch?v=QAnqgZAXpRo>
  - <http://i.blackhat.com/EU-21/Wednesday/EU-21-Shupeng-New-Ways-of-IPV6-Scanning.pdf>

	Risk	Scan world-wide	Android	IOS	Linux	Windows
<b>Risk 1</b>	ICMP unreadable error return the full addr	Y	✓			✓ Hotspot
<b>Risk 2</b>	In some cases the IPv6 addr will become shorter	Y	✓ Hotspot			
<b>Risk 3</b>	IPv6 addr can be sniffed and calculated form radio nearby	N	✓			
<b>Risk 4</b>	ICMP time exceeded error returned the full addr (all Linux kernel based devices)	Y	✓ Hotspot	✓ Hotspot	✓ Hotspot or Forward	✓ Hotspot or Forward
<b>Risk 5</b>	All zero address returned the full addr (all Linux kernel based devices)	Y	✓ Hotspot		✓ Hotspot or Forward	

Hotspot = need hotspot function enable. Hotspot will enable IPv4/6 forward

11/19/25 Forward = need net.ipv6.conf.all.forwarding = 1. In the routing device, it is a default configuration



## NATting Else Matters

- NATting Else Matters: Evaluating IPv6 Access Control Policies in Residential Networks, Passive and Active Network Measurement Conference (PAM) 2022, by Karl Olson, Jack Wampler, Fan Shen, and Nolen Scaife (CU Boulder) [https://dl.acm.org/doi/10.1007/978-3-030-72582-2\\_22](https://dl.acm.org/doi/10.1007/978-3-030-72582-2_22)
- They tested 10 popular CPE devices (25% of market share) and found they had IPv6 weaknesses.
- TP-Link AC1750 v2

Device	Default FW	FW Enabled	FW Disabled
Amazon Eero	●	–	No Disable Option
AmpliFi Gamer's Edition	●	–	–
Cisco DPC3941T XB3	●	–	–
Google Nest (2nd Gen)	●	–	No Disable Option
Linksys EA3500	●	–	25, 53, <b>80</b> , 135, 139, 443, 445, <b>2601</b> , 1080, <b>10000</b>
Linksys EA6350 AC1200	●	–	25, 53, <b>80</b> , 135, 139, <b>443</b> , 445, <b>2601</b> , 1080, <b>10000</b>
Motorola MR2600	○	25, 135, 139, 445, 1080	25, 135, 139, 445, 1080
Nighthawk X4 R7000	●	–	25, 43, 80, 135, 139, 443, 445, 548, 1080, <b>2601</b>
Surfboard SBG10 DOCSIS 3.0	●	–	25, 80, 135, 139, 443, 445, 1080
TP-Link AC1750 v2	○	No Enable Option	<b>22</b> , 25, 135, 139, 445, 1080



## IPv6 Tunneling Vulnerabilities

- Haunted by Legacy: Discovering and Exploiting Vulnerable Tunnelling Hosts, USENIX Security '25, August 2025.
  - <https://papers.mathyvanhoef.com/usenix2025-tunnels.pdf>
  - <https://www.youtube.com/watch?v=eFZsM3khrSk>
  - <https://www.top10vpn.com/research/tunneling-protocol-vulnerability/>
- Discovered numerous Internet devices susceptible to discovery and forwarded tunneled packets.
- They created various encapsulated probes to discovery private hosts behind vulnerable CPE devices.
  - GRE, GRE6: CVE-2024-7595
  - 4in6, 6in4: CVE-2025-23018/23019
- Their code is available: <https://github.com/vanhoefm/tunneltester>



# IPv6 Tunneling Vulnerabilities

Table 2: Scan results for IPv4 and IPv6 hosts. The total vulnerable hosts are shown followed by the results of each scan type.

Protocol	Total	Standard Scan		Subnet Spoof Scan		Spoofing Scan		Echo/Reply Scan		TTL Expired Scan	
		Replied	Unique	Replied	Unique	Replied	Unique	Replied	Unique	Replied	Unique
IPIP	530,100	88,123	8282	182,668	36,180	66,288	2068	411,565	256,225	105,833	21,820
GRE	1,548,251	612,479	159,673	517,331	394,932	219,213	219,213	509,433	95,735	193,629	145,641
IP6IP6	217,641	860	319	846	846	333	333	216,080	208,894	224	16
GRE6	1806	286	3	900	366	360	4	1219	238	167	20

Table 3: Mixed IPv4/6 scans. The total number of vulnerable hosts is shown followed by the results of each individual scan.

Proto.	Total	Scan Type	Replied	Unique
4in6	130,217	Spoofing	4113	1158
		TTL Expired	127,810	122,531
6in4	2,126,018	Spoofing	1,650,846	464,155
		TTL Expired	465,304	405,252
		IPv4-Mapped src	664,532	22,498
		6to4 src	1,048,559	85,178

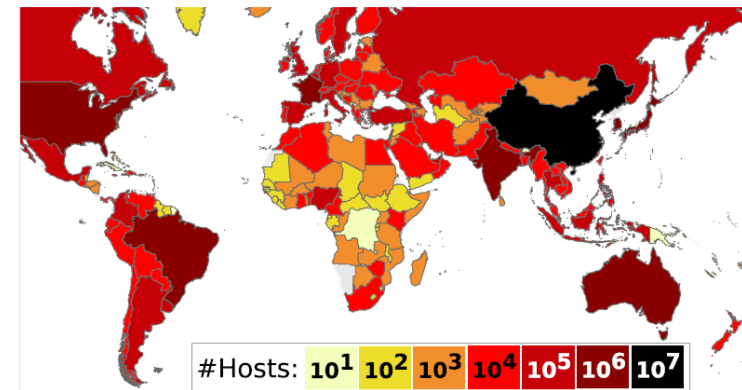
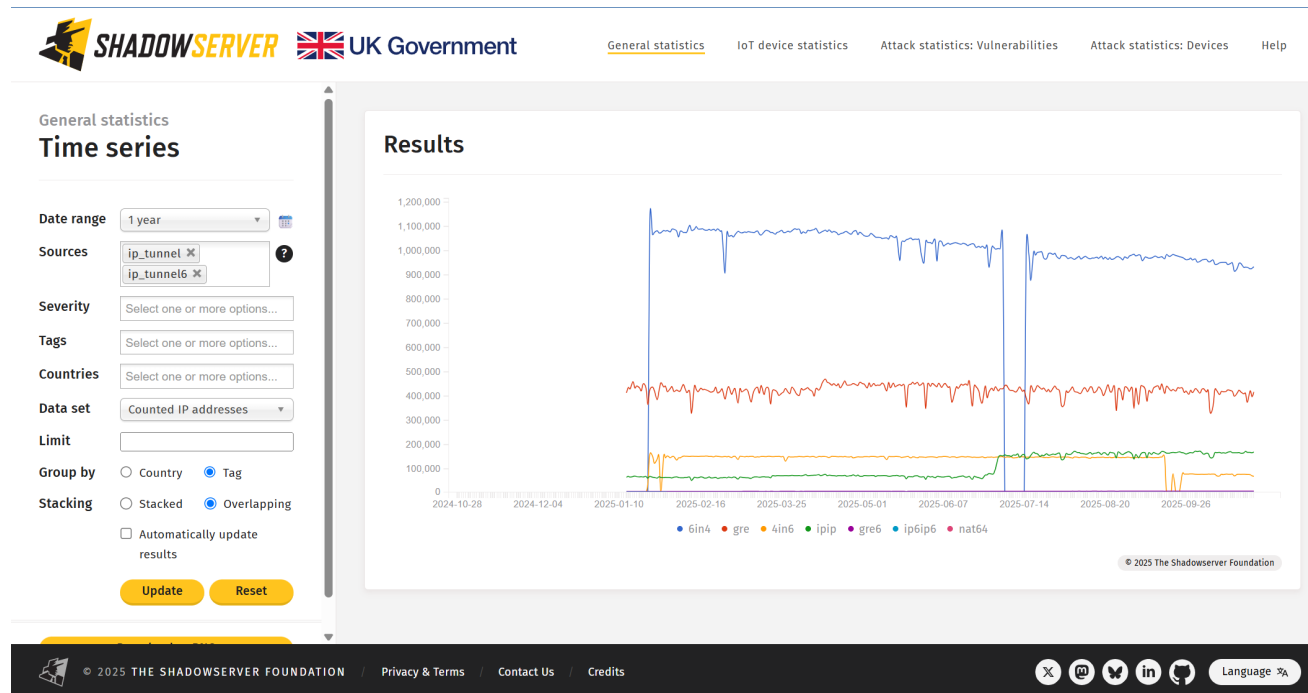


Figure 3: The number of vulnerable IPv4/6 hosts per territory, where colours represent numbers from 10 to 10 million.

# IPv6 Tunneling Vulnerabilities

- They collaborated with Shadowserver to plot the IPv6 tunneling issues.
- [https://dashboard.shadowserver.org/statistics/combined/time-series/?date\\_range=365&source=ip\\_tunnel&source=ip\\_tunnel6&dataset=unique\\_ips&group\\_by=tag&stacking=overlap](https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=365&source=ip_tunnel&source=ip_tunnel6&dataset=unique_ips&group_by=tag&stacking=overlap)

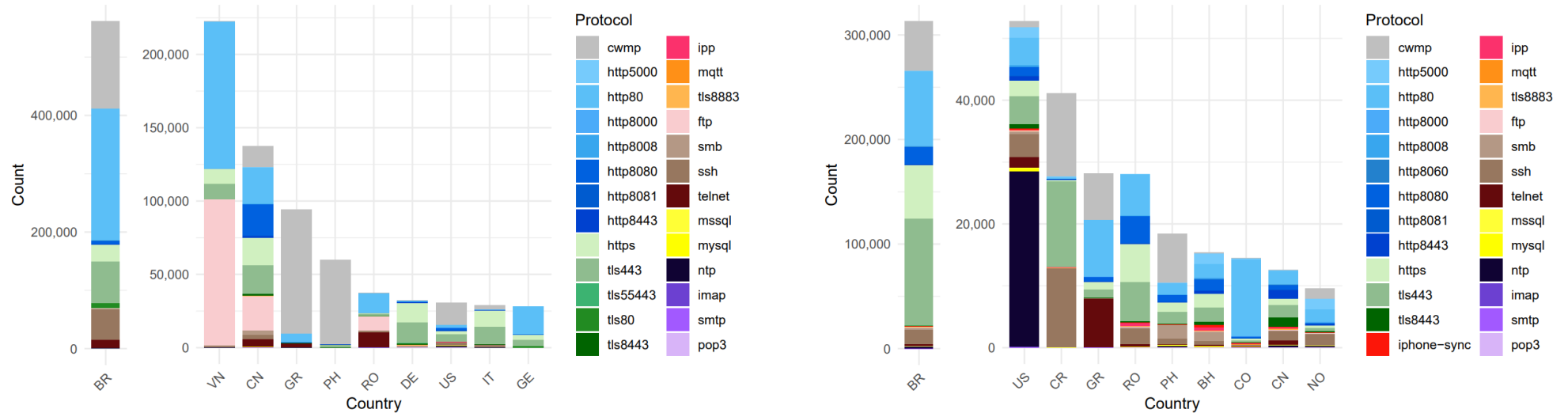


## Where Have All the Firewalls Gone?

- Where Have All the Firewalls Gone? Security Consequences of Residential IPv6 Transition, by Erik Rye, Dave Levin, Robert Beverly, Sept. 5, 2025  
– <https://arxiv.org/abs/2509.04792>
- IPv6-enabled CPE devices do not need to perform IPv6 NAT but some CPE devices to unfortunately allow unsolicited inbound IPv6 connections.
- Their IoT botnet style remote reconnaissance method received responses from 14 million distinct IPv6 addresses inside of residential networks (i.e., not the external-facing gateway), in 2,436 ASs across 118 countries.
- They found many Apple devices (iPhones, Apple TV), HP Printers, and other IoT devices like cameras and lights.

HP Printer Model	# IPv6 Addresses	%
HP DeskJet 2700 series	6,630	24.8
HP Ink Tank Wireless 410 series	4,133	15.4
HP Smart Tank 580	3,253	12.2
HP DeskJet 2600	1,728	6.5
HP DeskJet 2800	1,314	4.9
92 other models	9,712	36.3
<b>Total</b>	26,770	100

## Where Have All the Firewalls Gone?



(a) Network services reachable on *external* addresses.

(b) Network services reachable on *internal* addresses.

Figure 4: The network services that are reachable on external IPv6 addresses differ significantly from those reachable on internal addresses. Not shown in Figure 4(b) is the most responsive country, GB, which had 893,704 internal responding addresses, 99.6% of which responded to CWMP.

Source: <https://arxiv.org/pdf/2509.04792>

11/19/25

© 2025 Scott Hogg

12

## IPv6 Hitlist Collection

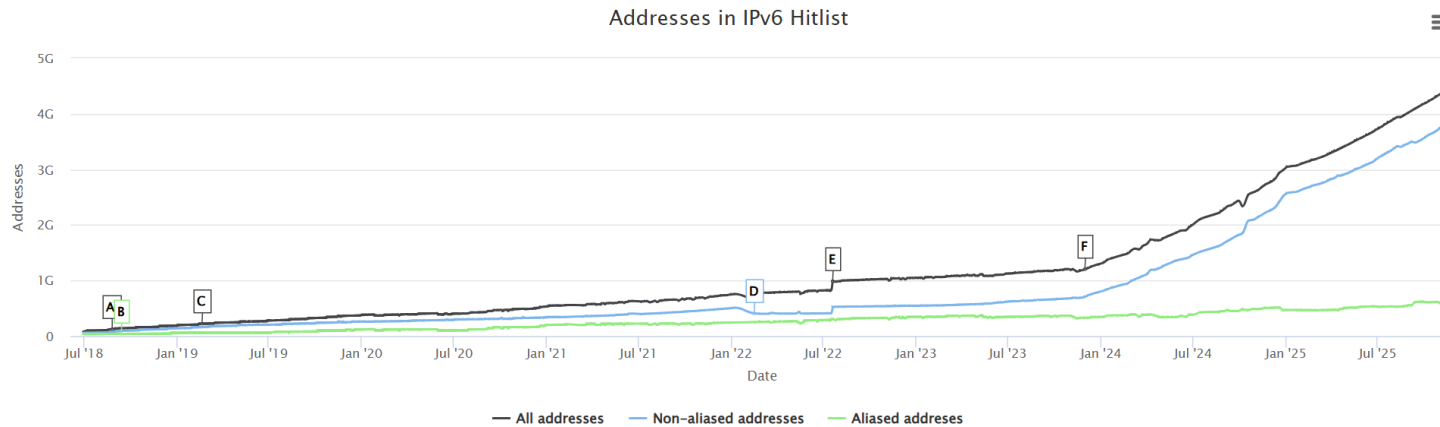
- Scanning the IPv6 Internet: Towards a Comprehensive Hitlist
  - <http://tma.ifip.org/2016/papers/tma2016-final51.pdf>
- Daily updated list of the Alexa Top 1M and Cisco Umbrella hosts. Also gets data from ipinfo.io.
  - <https://ipv6hitlist.github.io/>
- Useful for remote reconnaissance.
  - <https://www.net.in.tum.de/projects/gino/ipv6-hitlist.html>
  - Download link (Technical University of Munich (TUM))
  - <https://alcatraz.net.in.tum.de/i8-ipv6-hitlist/open/>
- Send registration e-mail to obtain the larger data set.



# IPv6 Hitlist Service

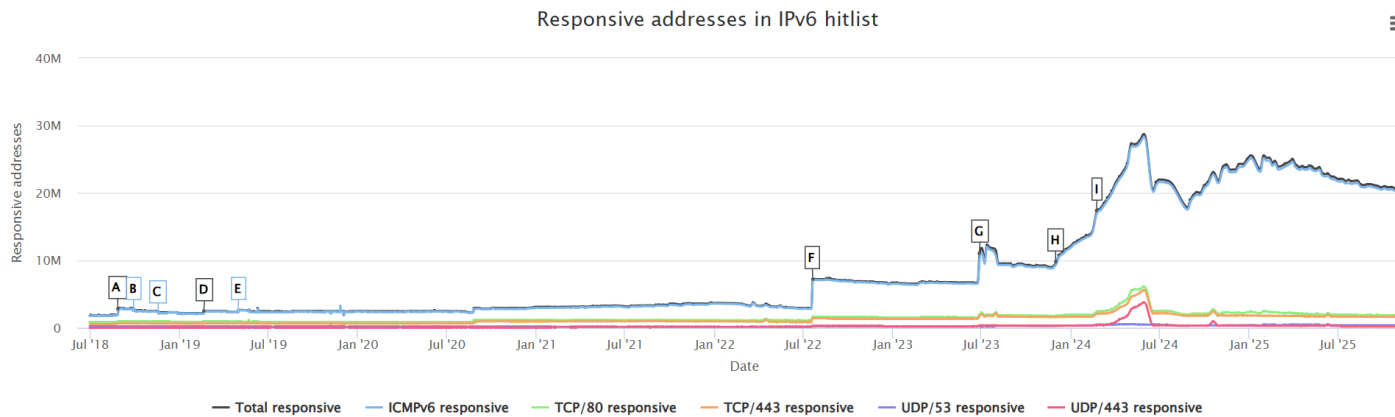
## Hitlist addresses

This graph shows the development of the **full, aliased and non-aliased** hitlist over time.





## Responsive addresses

Here, the development of the **different protocol responses** over time is shown. We scan five different protocols, an additional graph shows the amount of IP addresses which respond to at least one of the protocols.



## IPv6 Scanning Tools

- ZMapv6 now supports IPv6 scanning. (version 4.3.1) 
  - <https://github.com/tumi8/zmap>
- Masscan is a “TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.” 
  - <https://github.com/robertdavidgraham/masscan>
- fi6s is an IPv6 port scanner designed to be fast by sending and processing raw packets asynchronously.
  - <https://github.com/sfan5/fi6s>
- Yarrp is an open-source tool developed by Robert Beverly (Naval Postgraduate School (NPS)) that statelessly and randomly chosen destination and hop-limit. This utility facilitates fast active large-scale Internet remote reconnaissance.
  - <https://www.cmand.org/yarrp/>





## 6Trace

- 6Trace: An Effective Method for Active IPv6 Topology Discovery, by Zhaobin Shen, Pan Chen, Yi Xie, Chiyu Chen, Yongheng Zhang, Guozheng Yang, January 17, 2025
  - <https://www.mdpi.com/2079-9292/14/2/343>
- 6Trace is a stateless asynchronous IPv6 scanning method.
- A core feature of 6Trace is its feedback-based, bisection-like probing strategy, which dynamically optimizes TTL value adjustments, achieves high-speed probing, minimizes redundancy, and reduces local network load.
- 6Trace organizes its scanning process into iterative rounds, refining strategies based on real-time network routing information.
- 6Trace aims to minimize probing redundancy and time while maximizing scanning efficiency: defined as the ratio of discovered active interface addresses to the total number of probes sent.

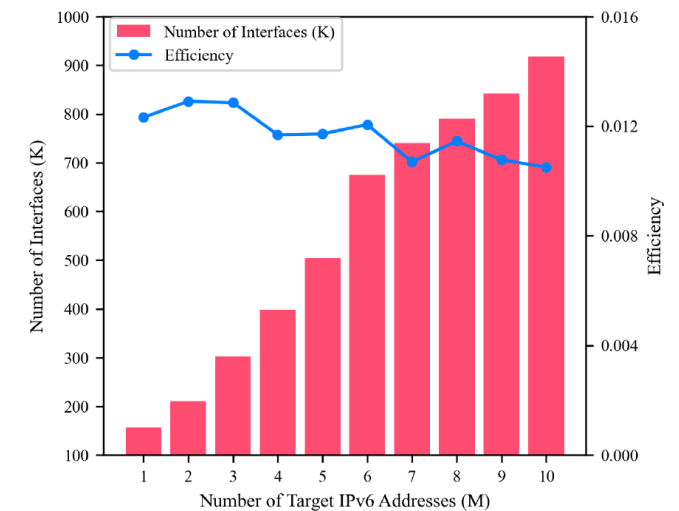
## 6Trace

- 6Trace achieves a 70% improvement in scanning efficiency on average which enables faster, more comprehensive, and resource-efficient topology discovery compared to existing state-of-the-art methods for IPv6 network measurement.

**Table 2.** Performance comparison of 6Trace, Flashroute, and Yarrp6 (bold values represent the best results).

Experimental Setup	Interfaces	Probes	Scan Time	• Scanning Efficiency
Flashroute-16 (gaplimit 8)	106.23 k	12.14 M	496 s	0.0088
Flashroute-32	109.18 k	21.45 M	895 s	0.0051
Yarrp-16 (Fill Mode)	157.81 k	16.94 M	684 s	0.0093
Yarrp-32	167.72 k	32 M	1278 s	0.0052
6Trace-24	162.93 k	9.98 M	469 s	<b>0.0163</b>
6Trace-32	164.75 k	12.48 M	519 s	<b>0.0132</b>

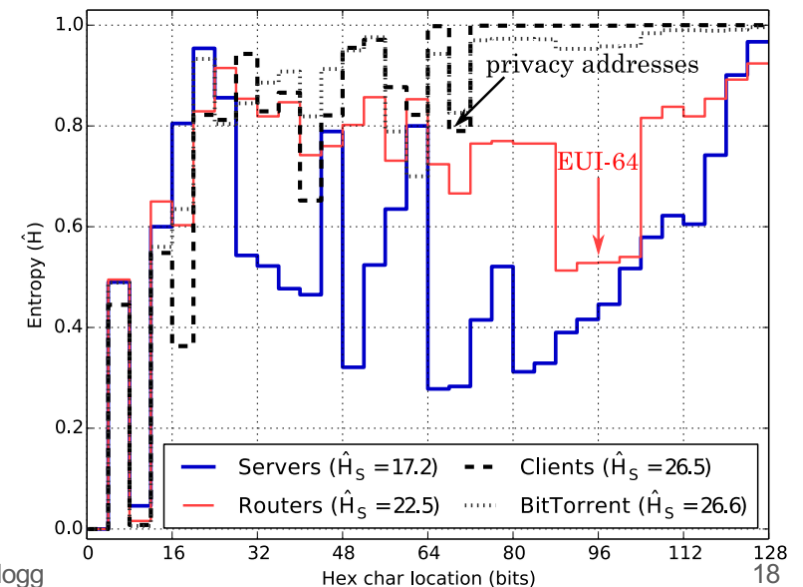
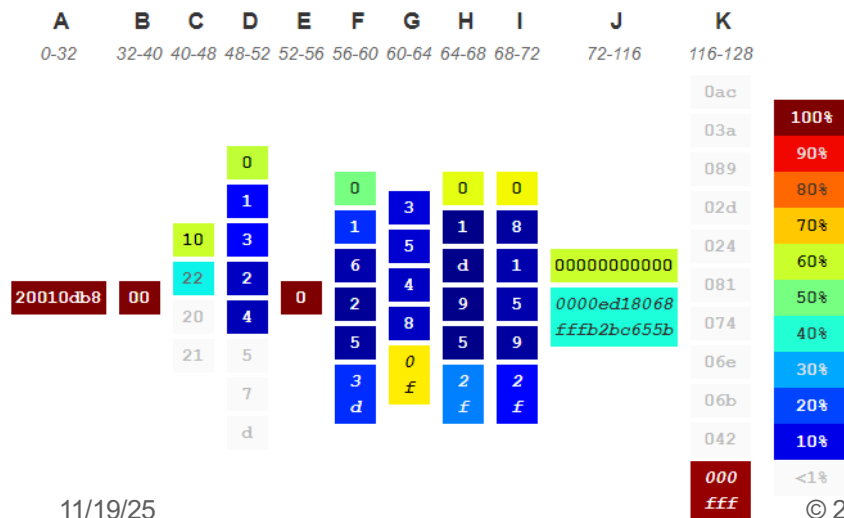
• Scanning efficiency is defined as the ratio of newly discovered interfaces to the total number of probe packets sent.



**Figure 8.** 6Trace scalability: interface discovery and efficiency trends.

# Entropy Analysis of IPv6 Addresses

- Entropy/IP: Uncovering Structure in IPv6 Addresses, by Paweł Foremski, David Plonka, Authur Berger (Akamai Technologies), 2016.
  - <https://arxiv.org/pdf/1606.04327.pdf>
  - <http://www.entropy-ip.com/> <https://github.com/akamai/entropy-ip>
- System analyzes and visualizes IPv6 addresses and creates candidate addresses for active scanning.



© 2025 Scott Hogg



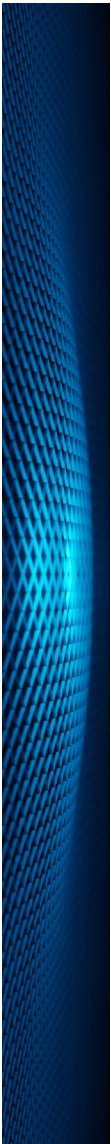
## 6Gen

- Target Generation for Internet-wide IPv6 Scanning, 2017 by Austin Murdock, Frank Li, Paul Bramsen, Zakir Durumeric, Vern Paxson.
  - <https://austinmurdock.com/6Gen.pdf>
  - <https://pdfs.semanticscholar.org/dd67/5c78db80f311165b0bc91c0a2da4402bb8c2.pdf>
- Paper details a Target Generation Algorithm (TGA), starting from a set of known seeds, with iterations as it performs probes, finding more seeds, organizing them into clusters, growing the cluster until it reaches the probe budget. “Bottom up, expand from seeds to ranges.”
- 6Gen written in C++ uses OpenMP for multi-threading.
- 6Gen uses dealiasing to remove nodes that respond to multiple IPv6 addresses (e.g. CDNs).
- 6Gen can find between 1-8 times more addresses than Entropy/IP.



## Target Generation Algorithms (TGAs)

- Many other TGAs have been created for finding IPv6 address targets.
  - 6Tree: Efficient dynamic discovery of active addresses in the IPv6 address space, 2019
  - 6GCVAE: Gated Convolutional Variational Autoencoder for IPv6 Target Generation, 2020
  - 6Hit: A Reinforcement Learning-based Approach to Target Generation for Internet-wide IPv6 Scanning, 2020
  - 6GAN: IPv6 Multi-Pattern Target Generation via Generative Adversarial Nets with Reinforcement Learning, 2021
  - 6VecLM: Language Modeling in Vector Space for IPv6 Target Generation, 2021
  - 6Graph: A graph-theoretic approach to address pattern mining for Internet-wide IPv6 scanning, 2022
  - 6Forest: An Ensemble Learning-based Approach to Target Generation for Internet-wide IPv6 Scanning, 2022



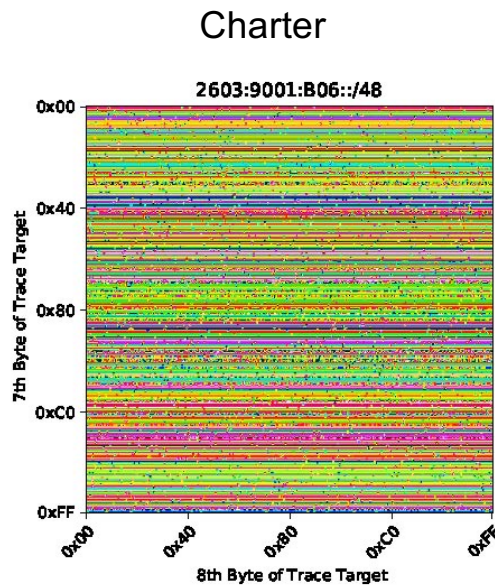
## TGAs (Cont.)

- Many other TGAs have been created for finding IPv6 address targets.
  - AddrMiner: A Comprehensive Global Active IPv6 Address Discovery System, 2022
  - DET: Enabling Efficient Probing of IPv6 Active Addresses, 2022
  - 6Scan: A High Efficiency Dynamic Internet-Wide IPv6 Scanner With Regional Encoding, 2023
  - 6Rover: Leveraging Reinforcement Learning-based Address Pattern Mining Approach for Discovering Active Targets in IPv6 Unseeded Space, 2024
  - 6Diffusion: IPv6 Target Generation Using a Diffusion Model with Global-Local Attention Mechanisms for Internet-wide IPv6 Scanning, 2024
  - 6Loda: Pattern Filtering and Ensemble Learning for IPv6 Target Generation and Scanning, 2025

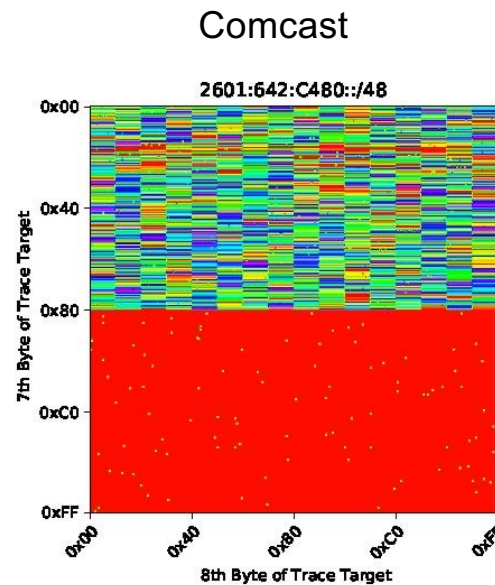


# IPv6 Network Discovery

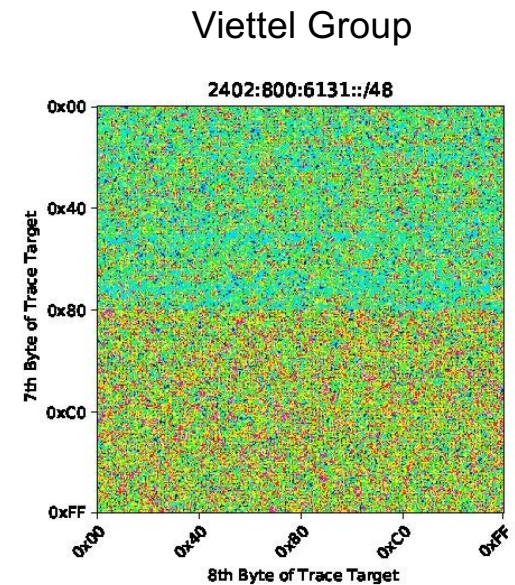
- Measuring the IPv6 network periphery, by Erik Rye, May 6, 2020.
  - <https://blog.apnic.net/2020/05/06/measuring-the-ipv6-network-periphery/>
- Discovering the IPv6 Network Periphery, by Erik C. Rye, Robert Beverly
  - <https://rbeverly.net/research/papers/edgy-pam20.pdf>



11/19/25

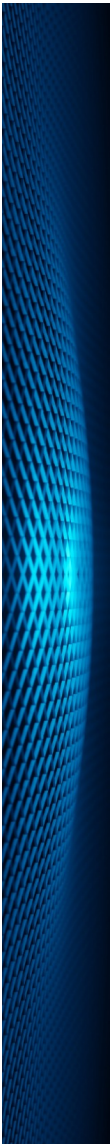


© 2025 Scott Hogg



22

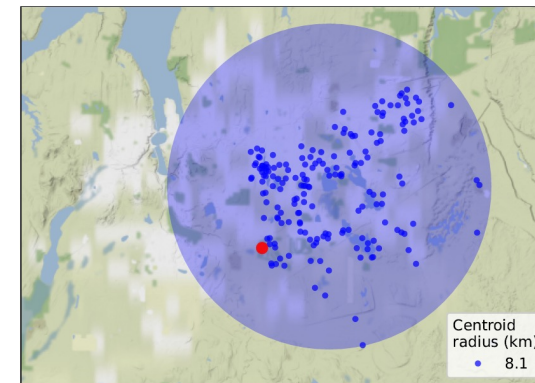
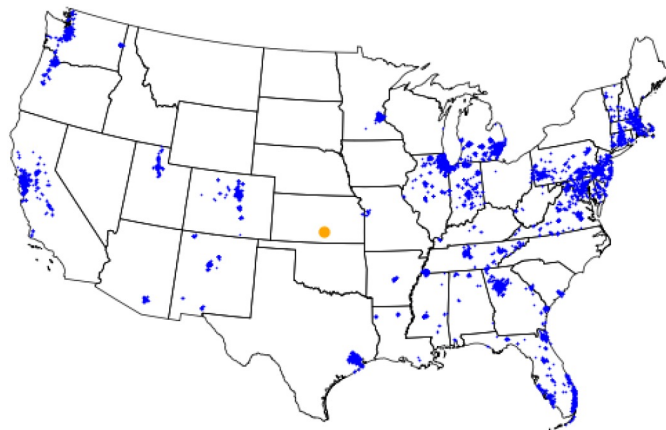
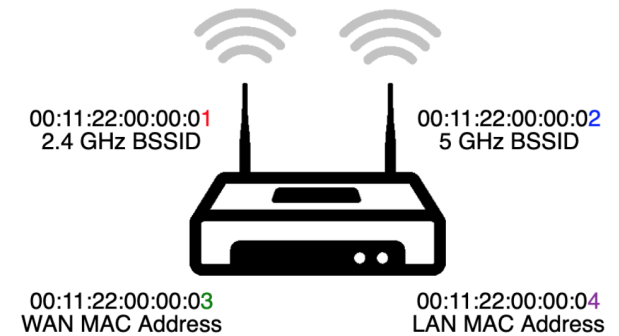
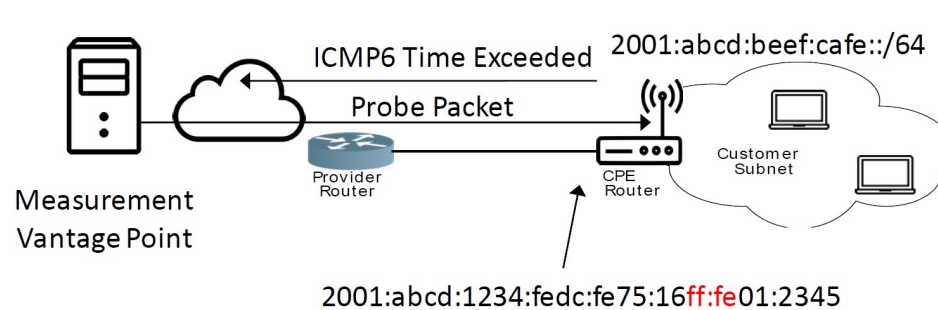




## IPvSeeYou: Exploiting Leaked Identifiers in IPv6 for Street-Level Geolocation

- Paper and Black Hat 2021 presentation by Robert Beverly and Erik C. Rye, Center for Measurement and Analysis of Network Data (CMAND), the Naval Postgraduate School and CAIDA.
  - <https://arxiv.org/pdf/2208.06767.pdf>
  - <https://i.blackhat.com/USA21/Wednesday-Handouts/US-21-Rye-IPvSeeYou.pdf>
  - <https://www.youtube.com/watch?v=KG4LF49hLM4>
- Using yarrp, they found 60M CPE devices using EUI-64, determined offset of WAN interface MAC and internal/Wi-Fi MACs.
- Cross-referenced BSSIDs with geolocation data (war-drivers, Apple, Google, others), thus, mapping IPv6 addresses to latitude & longitude.
- Only works for CPE that uses EUI-64, responsive to probes, and use predictable MACs & Wi-Fi, which unfortunately is many devices. (12M)
- Penultimate hop shows IPv6 (e.g. /48) prefix of nearby CPEs, even if those are using privacy addresses.

# IPvSeeYou: Exploiting Leaked Identifiers in IPv6 for Street-Level Geolocation



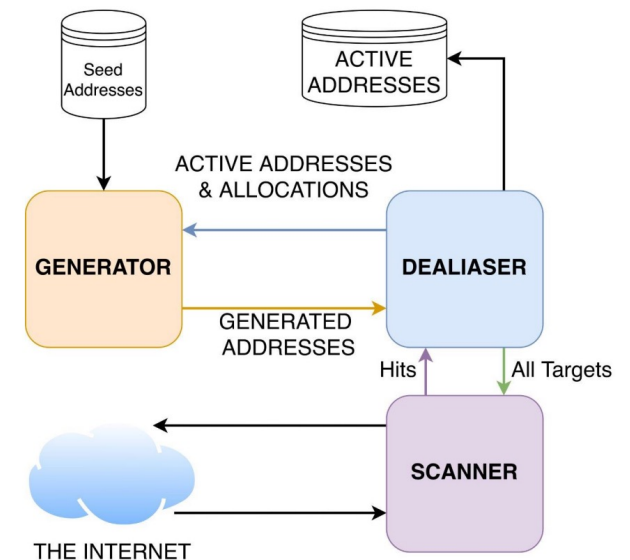
Source: <https://i.blackhat.com/USA21/Wednesday-Handouts/US-21-Rye-IPvSeeYou.pdf>

# 6Sense

- 6Sense: Internet-Wide IPv6 Scanning and its Security Applications, USENIX Security Symposium, by Grant Williams, Mert Erdemir, Amanda Hsu, Shraddha Bhat, Abhishek Bhaskar, Frank Li, and Paul Pearce, 2024.

- <https://www.usenix.org/conference/usenixsecurity24/presentation/williams>
- <https://www.usenix.org/system/files/usenixsecurity24-williams.pdf>
- <https://www.youtube.com/watch?v=ICTpBT20qHU>
- <https://github.com/IPv6-Security/6Sense>

Dataset Name	Pop.	Unique	De-Aliased	Active
Censys Certs	Servers	320,328	128,497	75,253
IPv6 Hitlist	All	6,763,519	6,746,480	5,866,234
CAIDA DNS Names	Servers	345,776	268,233	141,019
Cisco Umbrella	Servers	130,742	44,808	35,157
Rapid7 FDNS	Servers	15,015,809	5,154,197	1,651,805
Scamper	Routers	333,811	325,559	25,169
Majestic Million	Servers	135,290	24,134	18,446
Alexa Top 1 Million	Servers	95,375	9,028	7,196
Tranco	Servers	292,090	84,268	64,181
SecRank	Servers	109,686	59,744	35,688
Over All Sources	All	21,278,453	11,104,852	6,349,455



# 6Sense

Port/Protocol	Hits	New Active Upper-64s
ICMP	11,118,330 (11.11%)	5,776,637
TCP80	1,113,150 (1.11%)	203,948
TCP443	1,162,222 (1.16%)	316,372
UDP53	526,606 (0.52%)	166,573
<b>Total</b>	<b>11,882,633</b>	<b>6,128,152</b>

Category	Example	Count
Consumer Routers/Modems	DLink	78,532
	Fritz	978
	Hitron	626
	Ubiquiti	90
	Zyxel	73
Security Tools	OPNsense	23
	Fortinet	19
	Sangfor	14
	HillStone	4
Virtualization Tools	Kubernetes	52
	VMWare	19
Enterprise Switches	Brocade	64
	Cisco	60
	Lenovo	1
Printers	HP	351
	Lexmark	5

Device Category	Device Name	CVEs
Switches	Cisco WS-C3650	10
	Brocade ICX 7450	7
	Lenovo EN4093R	1
Routers	D-Link DIR-853/ET	12
	D-Link M15/R15	1
	EdgeMax (various)	1
	ZyXEL VMG3925	7
	ZyXEL VMG8825	2
	ZyXEL EX3301-T0	3
Printers	AVM Fritz!Box	12
	HP M479	3
	HP Officejet 3830	5
	HP Officejet 4650	2
	HP Officejet Pro 8600	2
	HP LaserJet M15w	6
Total	HP Deskjet 5730	1
	-	70

Source: <https://www.youtube.com/watch?v=ICTpBT20qHU>

© 2025 Scott Hogg

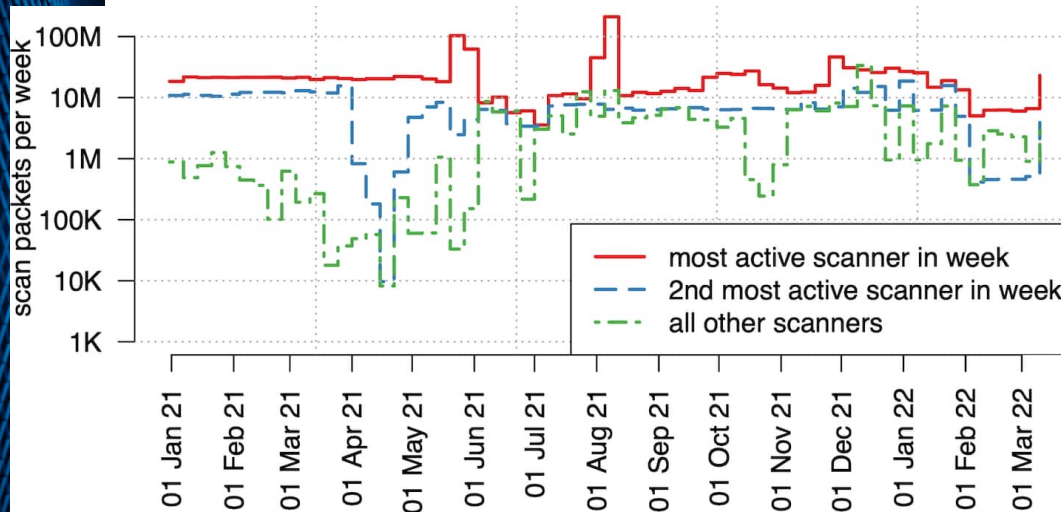
## Akamai's IPv6 Scanning Observations

- Who's Scanning the IPv6 Space? And, Frankly, Why Do We Even Care?, Philipp Richter, October 19, 2022.
  - <https://www.akamai.com/blog/security-research/vulnerability-scanning-IPv6-why-should-we-care>
  - Observed 15 months of IPv6 scanning traffic destined for their servers (on hitlists), analyzing the source addresses, the ASs, and the volume of scanning traffic.
  - Found that the top scanner source traffic from a single 128-bit address, but another source used entire /32 for the source addresses.
  - They discovered that 93% of the scanning traffic came from just 5 scanners. (2 scanners account for 70% of the traffic).
- Paper presented at the ACM Internet Measurement Conference 2022 titled “Illuminating Large-Scale IPv6 Scanning in the Internet”.
  - <https://www.akamai.com/content/dam/site/en/documents/research-paper/large-scale-IPv6-scanning-2022.pdf>





# Akamai's IPv6 Scanning Observations



rank	AS type	packets	scan sources		
			/48s	/64s	/128s
#1	Datacenter (CN)	839M (39.2%)	1	1	1
#2	Datacenter (CN)	744M (34.8%)	1	1	5
#3	Cybersecurity (US)	275M (12.9%)	1	1	12
#4	Cloud (US/global)	78M (3.7%)	2	2	512
#5	Cloud (DE)	48M (2.3%)	3	59	59
#6	Cloud (US/global)	45M (2.1%)	10	15	205
#7	Cloud (US/global)	39M (1.8%)	9	9	123
#8	Cloud (CN)	30M (1.4%)	5	5	53
#9	Transit (global)	11M (0.5%)	1	2	956
#10	Cloud (CN)	10M (0.5%)	1	1	7
#11	Cloud (US/global)	4.7M (0.2%)	1	1	353
#12	Datacenter (CN)	3.1M (0.1%)	9	12	19
#13	ISP (VN)	2.5M (0.1%)	1	1	1
#14	Datacenter (CN)	1.6M ( $\leq 0.1\%$ )	1	1	2
#15	Research (DE)	1.1M ( $\leq 0.1\%$ )	1	1	1
#16	ISP (RU)	0.9M ( $\leq 0.1\%$ )	1	1	2
#17	University (DE)	0.8M ( $\leq 0.1\%$ )	1	1	2
#18	Cloud/Transit (DE)	0.6M ( $\leq 0.1\%$ )	1,092	1,057	1,057
#19	ISP (RU)	0.6M ( $\leq 0.1\%$ )	1	1	1
#20	University (DE)	0.5M ( $\leq 0.1\%$ )	1	1	1

Source: <https://www.akamai.com/blog/security-research/vulnerability-scanning-IPv6-why-should-we-care>

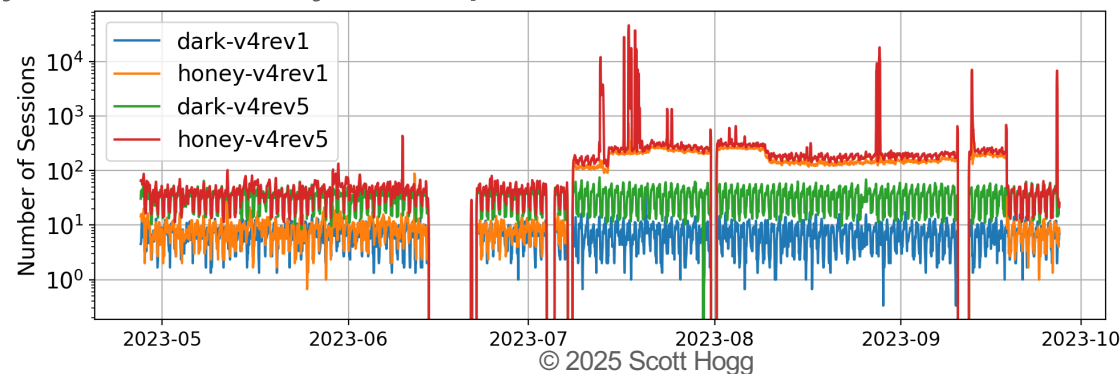
11/19/25

© 2025 Scott Hogg

28

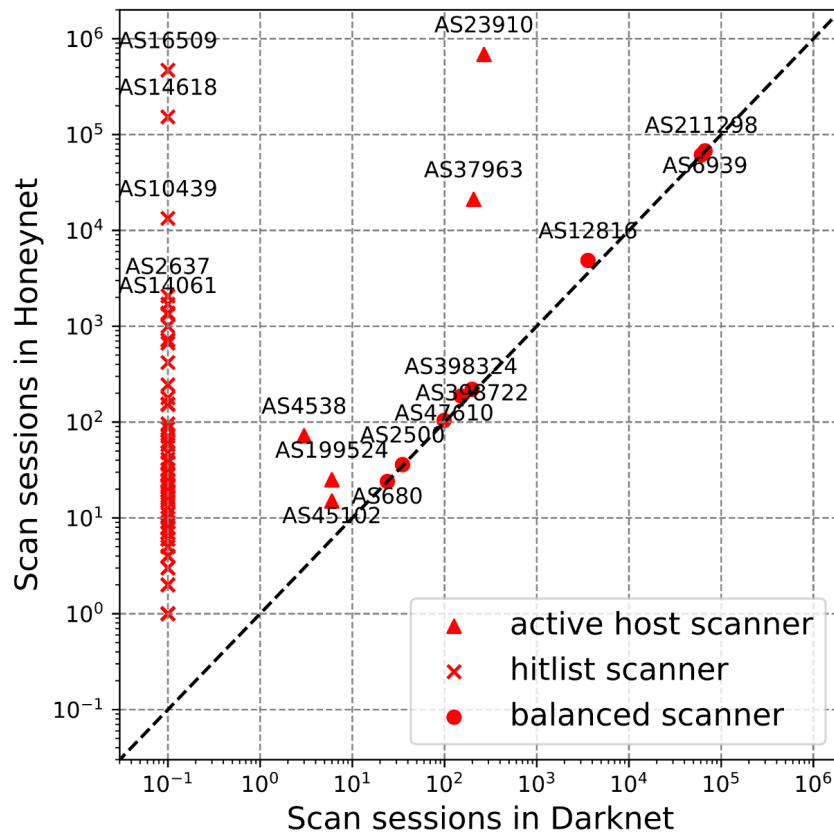
## Exploring IPv6 Scanning Activities & Prefix Discovery

- Exploring IPv6 scanning activities and prefix discovery, By Liang Zhao, June 25, 2024.
  - <https://blog.apnic.net/2024/06/25/exploring-ipv6-scanning-activities-and-prefix-discovery/>
  - Exploring the Discovery Process of Fresh IPv6 Prefixes: An Analysis of Scanning Behavior in Darknet and Honeynet, by Liang Zhao, Satoru Kobayashi & Kensuke Fukuda, 3/20/24.
- They used passive darknets and responsive honeynets to attract IPv6 scanning activity with DNS reverse zones, findable AAAA and PTR records. Addresses were then discovered after 2 weeks and added to IPv6 Hitlist, then actively scanned July to September 2023.





# Exploring IPv6 Scanning Activities & Prefix Discovery



AS211298 Constantine Cybersecurity Ltd.  
AS6939 Hurricane Electric LLC  
AS12816 Leibniz-Rechenzentrum  
AS23910 China Next Generation Internet CERNET2  
AS37963 Hangzhou Alibaba Advertising Co.,Ltd.  
AS398324 Censys, Inc.  
AS398722 Censys, Inc.  
AS47610 RWTH Aachen University  
AS2500 WIDE Project  
AS4538 China Education and Research Network Center  
AS199524 G-Core Labs S.A.  
AS680 Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.  
AS45102 Alibaba (US) Technology Co., Ltd.  
AS16509 Amazon.com, Inc.  
AS14618 Amazon.com, Inc.  
AS10439 CariNet, Inc. (Fiberalley??)  
AS2637 Georgia Institute of Technology  
AS14061 DigitalOcean, LLC

Source: <https://blog.apnic.net/2024/06/25/exploring-ipv6-scanning-activities-and-prefix-discovery/>  
11/19/25 © 2025 Scott Hogg



## IPv6 Scanners and BGP Adaptation

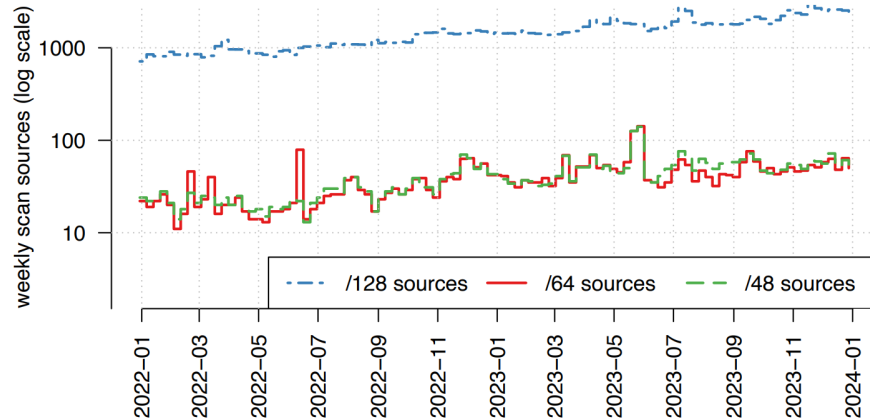
- A Detailed Measurement View on IPv6 Scanners and Their Adaption to BGP Signals, by Isabell Egloff, Raphael Hiesgen, Maynard Koch, Thomas C. Schmidt, Matthias Wählisch, June 25, 2025.
  - <https://arxiv.org/abs/2506.20383>
- After an initial baseline observation phase (week 1-13), we recursively split one prefix into two more specific prefixes every two weeks (dotted vertical lines) until we announce 17 prefixes, our most-specific prefix is /48. 11 months of observations from 4 network telescopes using 17 IPv6 prefixes. 8 months of changing BGP signals found strong correlation with packet arrival.
- 70% of all scanners were observed only once, 9% target uniformly all announced prefixes and account for 63% of all packet.
- Addresses receive significantly more attention by scanners when more specific prefixes are announced in BGP.



## Unveiling IPv6 Scanning Dynamics

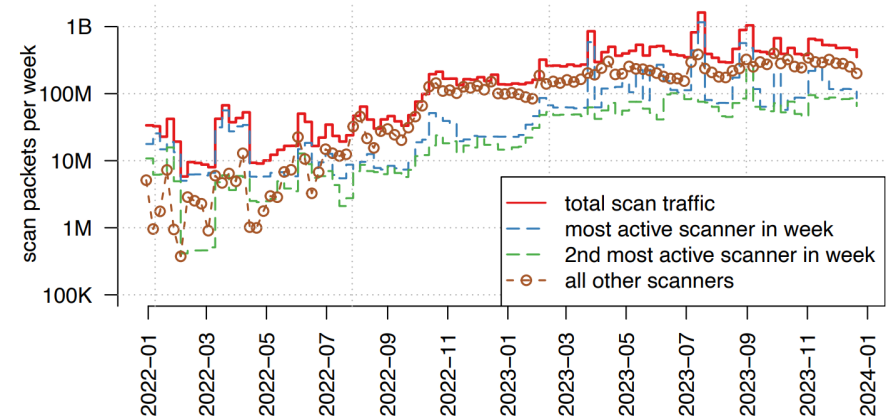
- Unveiling IPv6 Scanning Dynamics: A Longitudinal Study Using Large Scale Proactive and Passive IPv6 Telescopes, August 10, 2025.
  - <https://arxiv.org/abs/2508.07506>
- Techniques to attract IPv6 scan traffic, thus enabling its analysis. By deploying the largest-ever IPv6 proactive telescope in a production ISP network, they collected over 600M packets of unsolicited traffic from 1.9k Autonomous Systems in 10 months.
- They defined a scan as a source hitting at least 100 IPv6 addresses of the CDN, with a maximum packet inter-arrival time of 3,600 seconds (1 hr).
- Over 90% of observed scanning traffic used ICMP ping, even though their telescopes were responsive to TCP/UDP traffic.
- They used a /32 and /48s with BGP, DNS with subdomains, TLS certs, seeded hitlists, and used passive and proactive methods of observation.

# Unveiling IPv6 Scanning Dynamics



Steady increase in IPv6 scan sources per week hitting the CDN. Number of IPv6 addresses (/128s) more than doubled over the two-year window. When aggregated into /64, and /48 subnets, the weekly rate tripled, from  $\approx 20$  to  $\approx 50-70$ .

Weekly scan packets (/64 aggregation), grew 100X, from 10-60M to 1B. In early 2022, scan traffic was often dominated by the most active source(s) (dashed lines), by late 2023 scanning traffic comes from a broad range of sources.



Source: <https://arxiv.org/pdf/2508.07506>



## Large-Scale IPv6 Internet Reconnaissance Summary

- There are tools that can perform Internet-wide IPv6 scanning.
- There are research papers describing how to use Target Generation Algorithms (TGAs) along with hitlists to iterate through and find targets.
- Active IPv6 probing is taking place on the Internet today.
- Large-Scale IPv6 Internet Reconnaissance - Part 1 of 2, Dec. 12, 2023
  - <https://hoggnet.com/blogs/news/large-scale-ipv6-internet-reconnaissance-part-1-of-2>
- Large-Scale IPv6 Internet Reconnaissance - Part 2 of 2, Dec. 13, 2023
  - <https://hoggnet.com/blogs/news/large-scale-ipv6-internet-reconnaissance-part-2-of-2>



## Take Steps to Proactively Secure IPv6

- You should be aware of where you are using IPv6 and how extensively it is used on the Internet. Your end-users are already using IPv6 on their mobile phones, at their homes, as they travel, and elsewhere.
- You should develop an IPv6 security strategy NOW since you are already using IPv6.
- You want to use these same scanning techniques to proactively assess your IPv6 Internet risk.
- You want to use security tools and products that give you visibility to IPv6 activity (on your local networks, across your private networks, and over the Internet) and control IPv6 communications.
- You should use a risk-based approach to IPv6 security by mitigating the biggest risks as soon as possible.
  - <https://hoggnet.com/pages/ipv6-security>



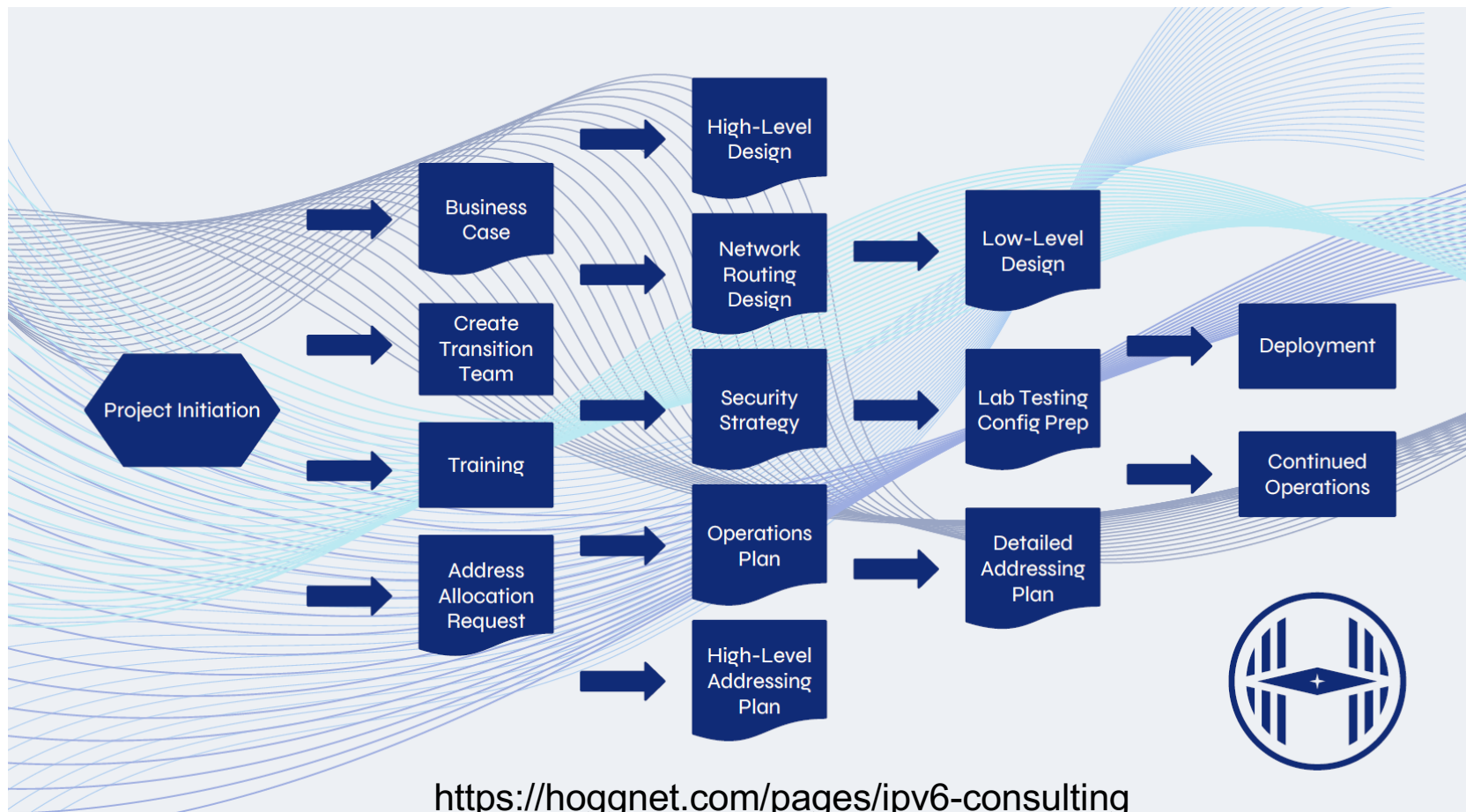


## FREE IPv6 Certifications

- Hogg Networking also offers 3 free IPv6 certification exams.
- <https://hoggnet.com/pages/ipv6-certifications>
- They are free, online, and open-book exams.
- These are the industry's most current exams that validate your knowledge of IPv6.
- Confirm your comprehension after taking an IPv6 training class.
- Show others that you have a solid understanding of IPv6.
- See if you can pass all the exams and try to get a higher passing score than your colleagues.
- These exams are meant to be fun and challenging.



# IPv6 Transition Phases





## Questions and Answers

Q:

&

A:

Scott@HoggNet.com      Mobile: +1-303-949-4865  
<https://www.linkedin.com/in/scottrhogg/>  
<https://bsky.app/profile/scotthogg.bsky.social>  
X/Twitter: @scotthogg