



USA 2021

AUGUST 4-5, 2021

BRIEFINGS

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

Erik Rye (@gigaryte, CMAND)

Rob Beverly (@badcksum, CMAND)

6::int

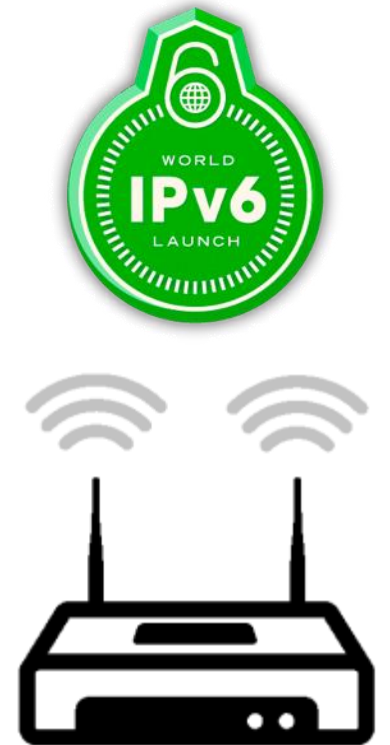
<https://sixint.io>

#BHUSA @BlackHatEvents @v6intel

- Overview
- Background
- IPvSeeYou
- Tool and Demo
- Conclusions
- Questions

- **Overview**
- Background
- IPvSeeYou
- Tool and Demo
- Conclusions
- Questions

- Got IPv6 at home? (I think...)
- Know how your router is configured? (we didn't...)
- What does your router reveal about you? (you might be surprised...)



2001:abcd:1234:fedc::/64

IPvSeeYou: In a Nutshell

- Routers deployed in the wild use legacy EUI-64 IPv6 addressing
- Anyone (able to ping6 / traceroute6) can find router's physical geolocation
 - with *street-level* precision
 - E.g., a subscriber's home



- Developed a technique to find residential routers (needle in a haystack in IPv6)
- Discovered >60M routers in the wild that reveal their hardware (MAC) address
- Gathered 450M BSSID -> Geolocations
- Developed a technique to infer the WAN MAC -> WiFi BSSID mapping
- Data fusion to geolocate IPv6 prefixes of home routers



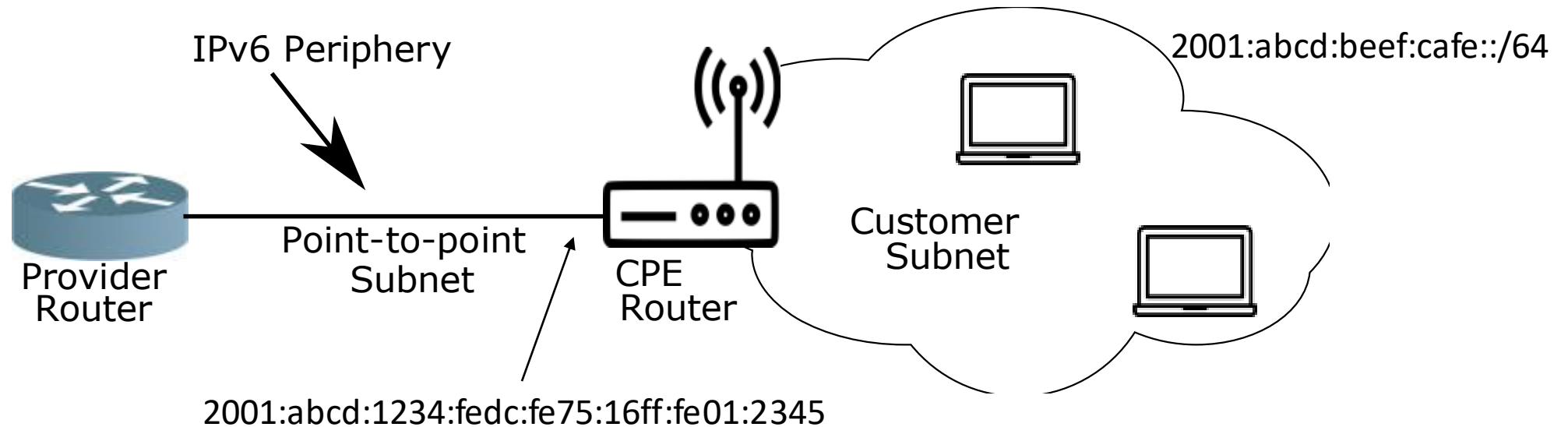
Active Measurement
EUI-64 IPv6 Address Discovery

- Overview
- **Background**
- IPvSeeYou
- Tool and Demo
- Conclusions
- Questions



- IPv6:
 - IPv6 addresses are 128 bits
 - E.g., `2001:abcd:1234:fedc:fe75:16ff:fe01:2345`
 - Huge address space + sparsity
 - No way to actively probe entire IPv6 Internet, ala zmap
 - Even residential customers allocated a /64 (=2⁶⁴ addresses)
 - No NAT
- Implication:
 - IPv6 is deployed differently than IPv4!

- Device at customer premises (CPE) is a routed hop!
- One subnet allocated to link between provider’s router and CPE
- Different subnet allocated to customer, on other side of CPE



- Smallest allocation, e.g., to a residential customer, is a /64
- What's a home to do with 2^{64} addresses?
 - Every device needs a unique IPv6 address
- How do devices choose an address within this /64?
 - Today (RFC3041/4941): “privacy extensions”, i.e., random and short-lived
 - Legacy (RFC1971/2462): “EUI-64”, encode hardware MAC address into lower 64 bits



- Recall, IEEE MAC addresses are 6 bytes, in hex:

00:11:22:33:44:55



Organizational Unique Identifier (OUI) = hardware manufacturer that owns block

- IPv6 EUI-64 address:

- Insert `ff:fe` between upper and lower 3B of MAC
- Invert 7th most significant bit

2001:1234:4567:89ab:0211:22ff:fe33:4455



EUI-64 Interface Identifier (IID)

- Advantages:

- Simple to implement
- Guarantees (in theory) unique IPv6 address
- No need for duplicate address detection (faster)

- Disadvantages:

- Exposes layer 2 (Ethernet address) in layer 3 (IP)
 - Reveals device details (hardware, vendor, etc)
- Static address doesn't change, even if device connects to new network
 - Globally unique -- permits tracking!

2001:1234:4567:89ab:0211:22ff:fe33:4455



EUI-64 Interface Identifier (IID)

- RFC3041, January 2001
 - Generate short-lived random interface identifier
 - Perform duplicate address detection
 - Regenerate address often
 - For example: `2001:558:6045:1c:8c9c:5f05:ecc0:1f49`
- Privacy implications of SLAAC / EUI-64 known for 20+ years
 - So, all devices use privacy extensions, right?

1. A remote, unprivileged attack on privacy, even when end-hosts utilize IETF standardized IPv6 “privacy extensions”
2. Tool that maps IPv6 router address to geolocation
3. Precision geolocation of ~12M residential IPv6 routers and allocated IPv6 prefixes
4. Geolocation of provider last-hop infrastructure, thereby geolocating IPv6 routers that use privacy extensions
5. Responsible disclosure and vendor remediation

- Overview
- Background
- **IPvSeeYou**
- Tool and Demo
- Conclusions
- Questions



Active Measurement
EUI-64 IPv6 Address Discovery



WiFi Geolocation
Databases



Wired-Wireless
Identifier Matching
Algorithm



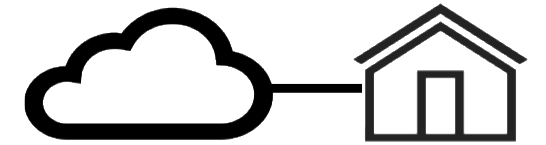
Street-Level
IPv6 Geolocation

- This work combines
 - IPv6 addresses w/embedded MAC addresses
 - BSSIDs w/fine-grained geolocation data
 - To geolocate IPv6 addresses
- Consulted with IRB
 - Follow all best practices to minimize any potential for harm
- Publish aggregate data analysis only
- Goal: ultimately *improve* privacy protections by highlighting this vulnerability

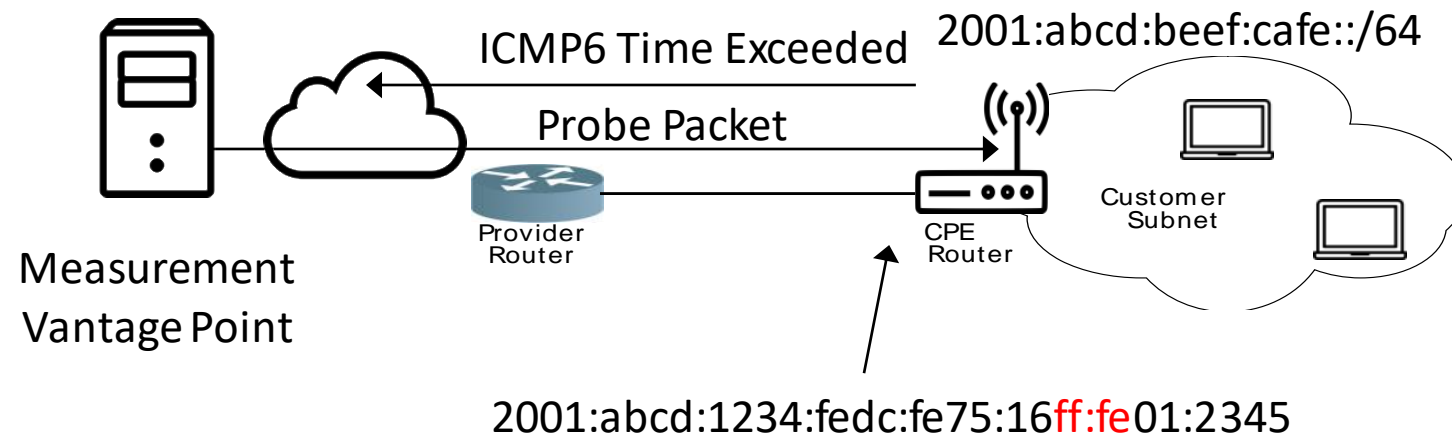
EUI-64 Address Discovery at Scale

- IPv6: no NAT, in-home devices publicly addressed
- *Smallest* IPv6 allocation a /64:
 - Traceroute to a *random* target in each /64 in a provider's network
 - (Target unlikely to exist)
 - But, typically elicits an *ICMPv6 Time Exceeded* from CPE, if /64 is allocated to a customer
- Traceroute is slow! use *yarrp**
- Found **>60M** EUI-64-derived MAC addresses

* <https://www.cmand.org/yarrp>



Active Measurement
EUI-64 IPv6 Address Discovery



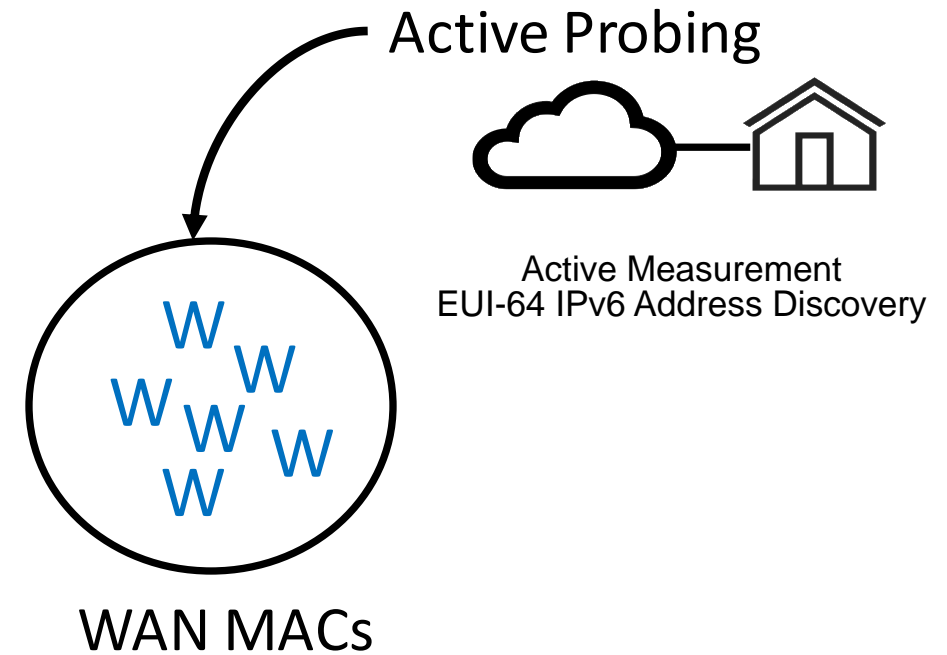
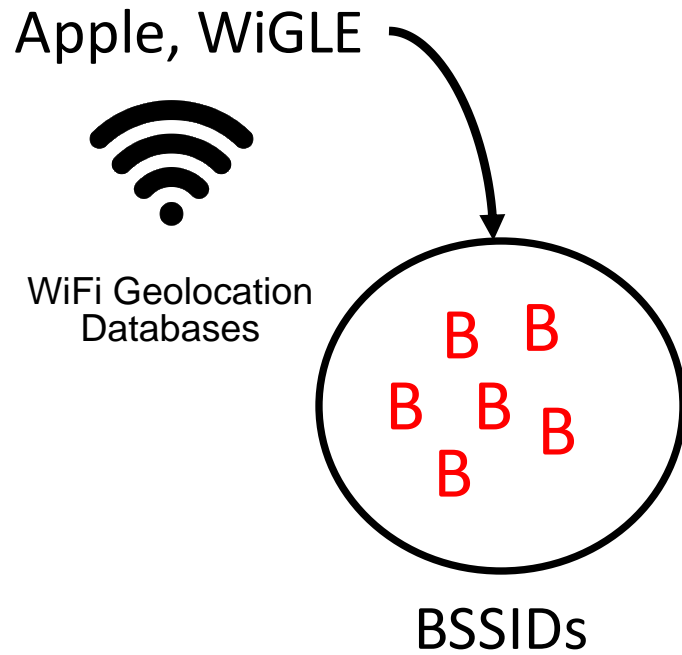


WiFi Geolocation
Databases

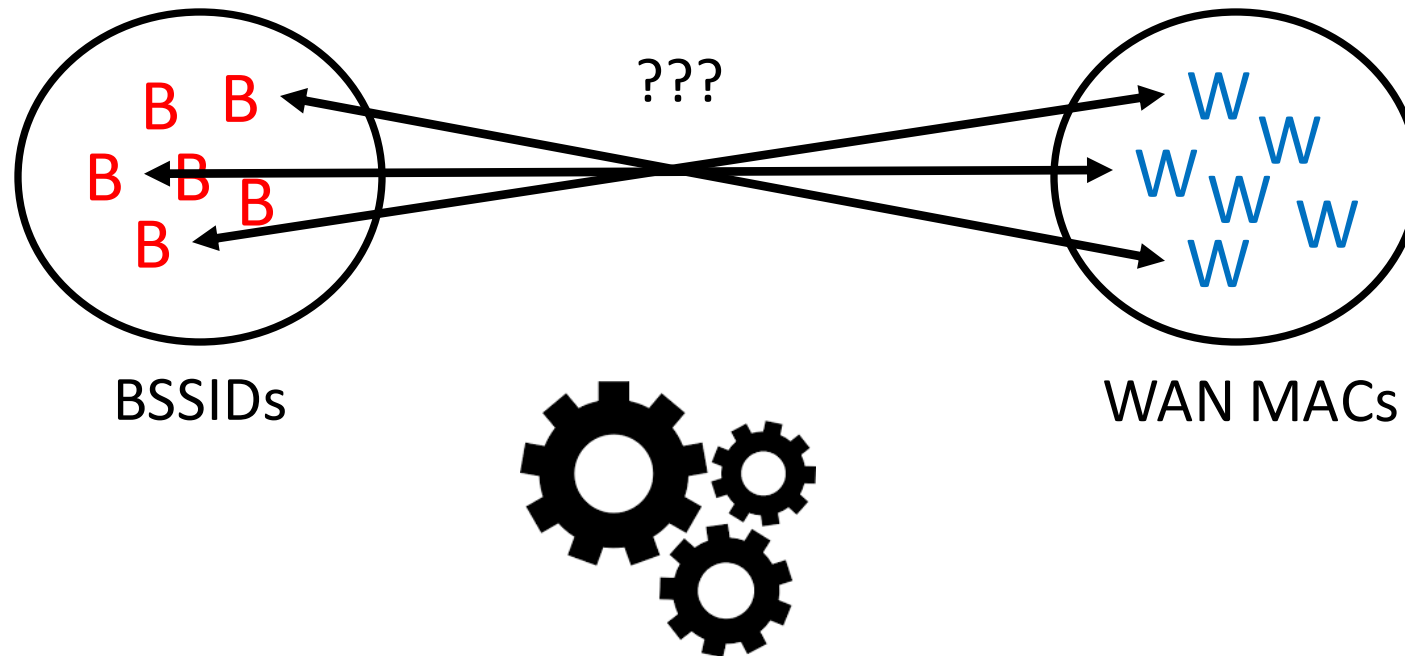
- BSSID = WiFi interface MAC address
- BSSID geolocations reported by
 - War-drivers
 - wigle.net, mylnikov.net
 - Crowd-sourced network of millions of devices
 - Provides non-GPS geolocation data for other devices in ecosystem
 - Apple Location Services*
 - Google Geolocation API
- Query databases and APIs for BSSIDs in same OUI as EUI-64-derived MAC addresses
- Amass corpus of 450M BSSID geolocations
 - Union of mylnikov.net, openBMap, and openWifi.su databases combined with querying Apple Location Services and WiGLE.net APIs

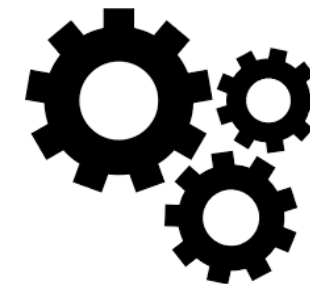
*iSniff-GPS by Hubert Seiwert (BH 2012): <https://github.com/hubert3/iSniff-GPS>

Mapping WAN MAC to WiFi BSSID

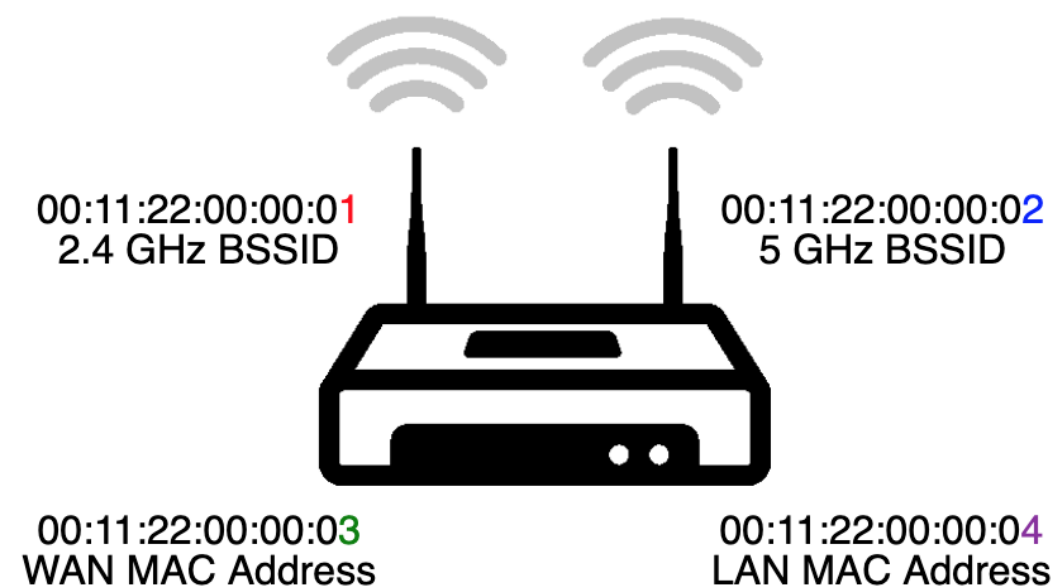


Mapping WAN MAC to WiFi BSSID





- Mental model:
 - Many all-in-one CPE devices, e.g. cable modem with built-in WiFi
 - Many System-on-a-Chip (SoC) designs where all radios made by one company
 - E.g., Broadcom BCM3349
 - Each interface gets its own MAC address
 - These MAC addresses are *related*
 - For example, +/- 1

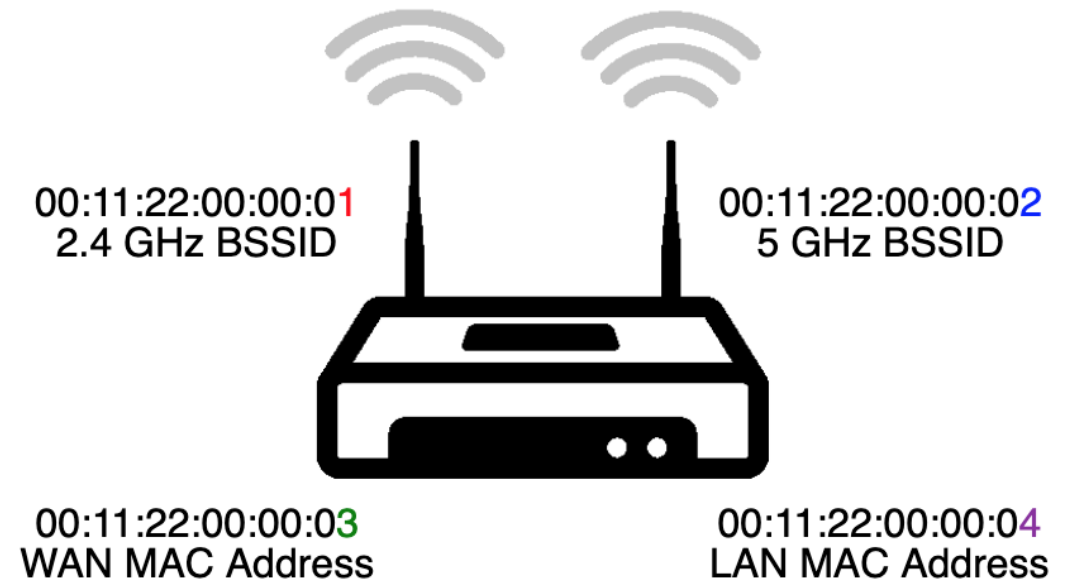


- Complications

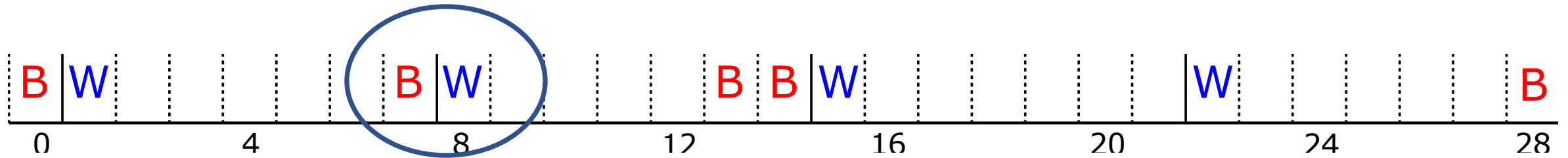
- Some devices have many interfaces (WAN, LAN, 2.4GHz, 5GHz, Guest WiFi, Bluetooth, etc)
- Different devices have different offsets
- Naïve “nearest” match does not work

- But, in the best case

- WAN MAC embedded in an EUI-64 IPv6 address:
2001:c001:d00d:0211:22ff:fe00:0003
- BSSID 00:11:22:00:00:01/2 captured in WiFi geolocation database



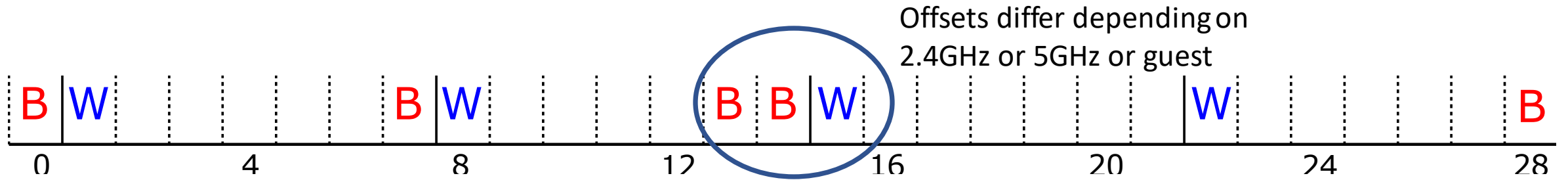
Mapping WAN MAC to WiFi BSSID



Naively, this BSSID and this WAN MAC are adjacent and belong to same device

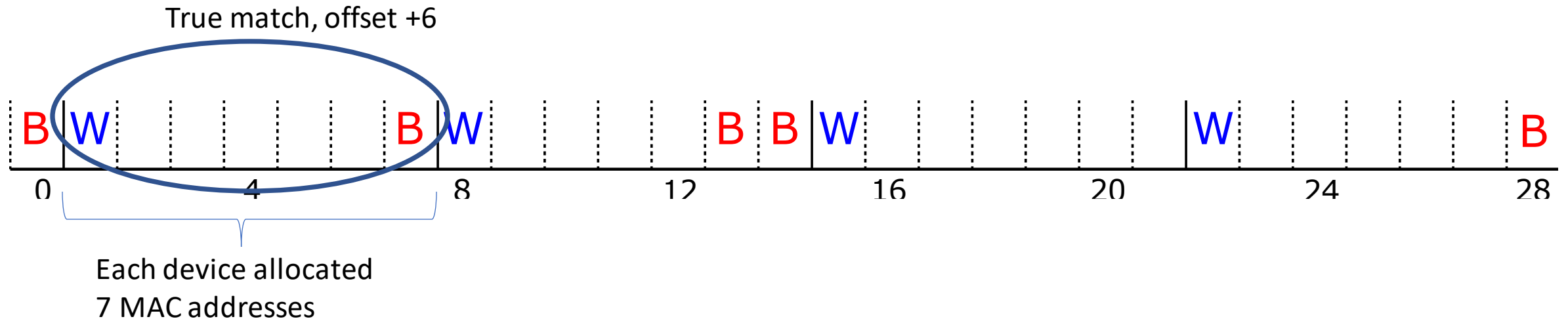
End result: produce WAN-BSSID offset inference on a per-OUI basis

Mapping WAN MAC to WiFi BSSID



End result: produce WAN-BSSID offset inference on a per-OUI basis

Mapping WAN MAC to WiFi BSSID



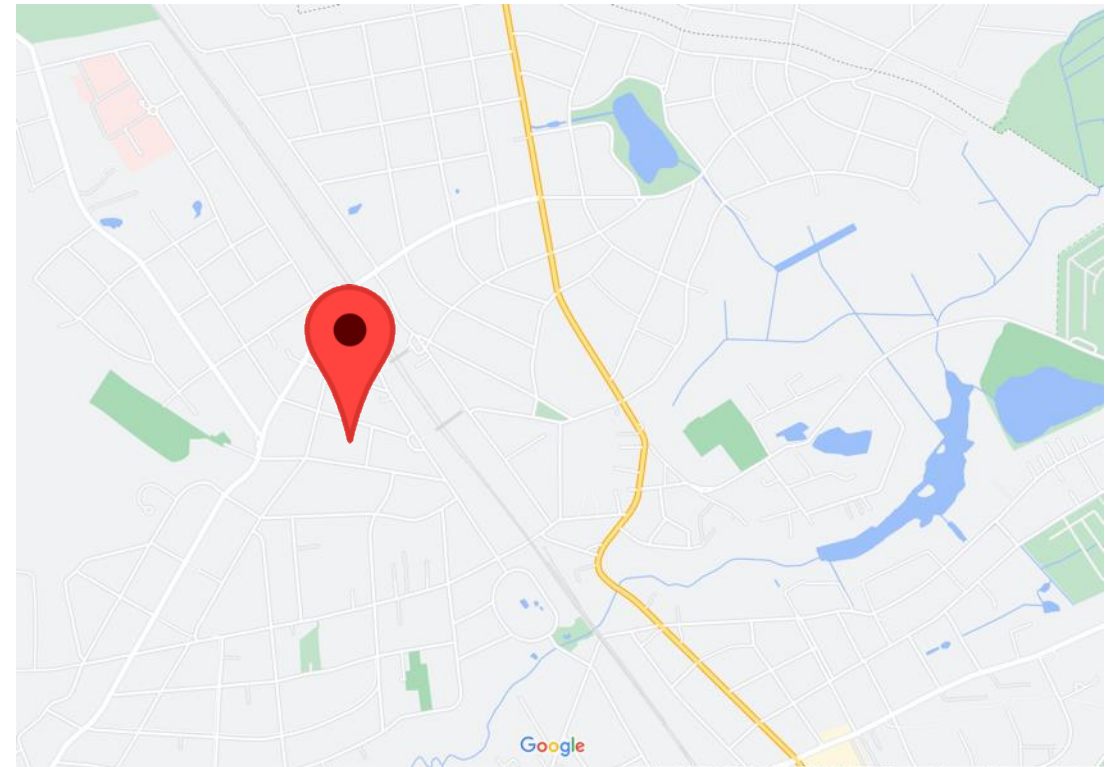
End result: produce WAN-BSSID offset inference on a per-OUI basis

- IPv6 Collection Limitations
 - Some CPE devices don't use EUI-64 IPv6 addresses
 - SLAAC w/Privacy Extensions, DHCPv6 addresses
 - Nonresponsive to ICMP6 probes
- WLAN BSSID Collection Limitations
 - Device may not have a BSSID
 - Router w/o built-in WiFi
 - IoT devices
 - Devices with BSSIDs may not be in wardriving/geolocation databases
 - Restrictions/laws regarding wardriving
- Correlation Limitations
 - MAC addresses assigned to wired and wireless interfaces non-sequential or in different OUI
 - Multiple offsets per OUI
 - 2.4/5 GHz BSSIDs complicate offset inference

- Combining our WAN MAC and BSSID data with our algorithm, we geolocated:
 - At least 12M unique devices of 60M total devices
 - In 147 countries
 - In 1000+ unique OUIs
- Widespread use of EUI-64 IPv6 addresses cause serious location privacy concerns for individuals
 - CPE routers typically in homes, businesses
- In this presentation, we examine geolocation results in the aggregate or introduce large error to preserve personal privacy

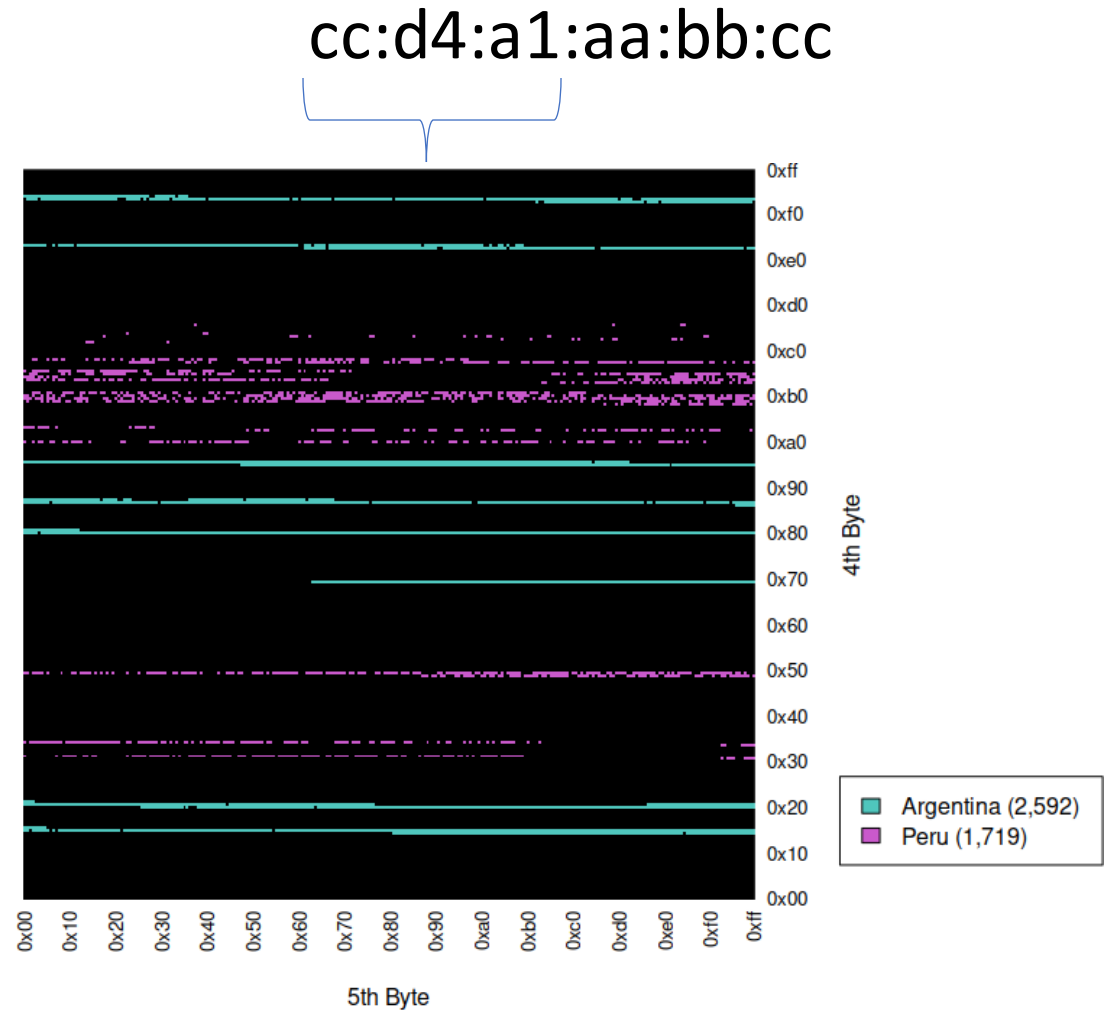
HARMFUL

- Solicited volunteers with CPE using EUI-64 IPv6 addresses
 - They divulged internal subnet
 - eg 2003:ab::/56
 - We traceroute to random address in internal network
 - Obtain WAN EUI-64 IPv6 address
 - Use IPvSeeYou to infer BSSID and geolocate IP address
- 4 of 5 volunteer devices geolocated
 - < 50m geolocation accuracy
 - 5th device used EUI-64 IPv6 addressing but non-sequential WAN/BSSID MACs

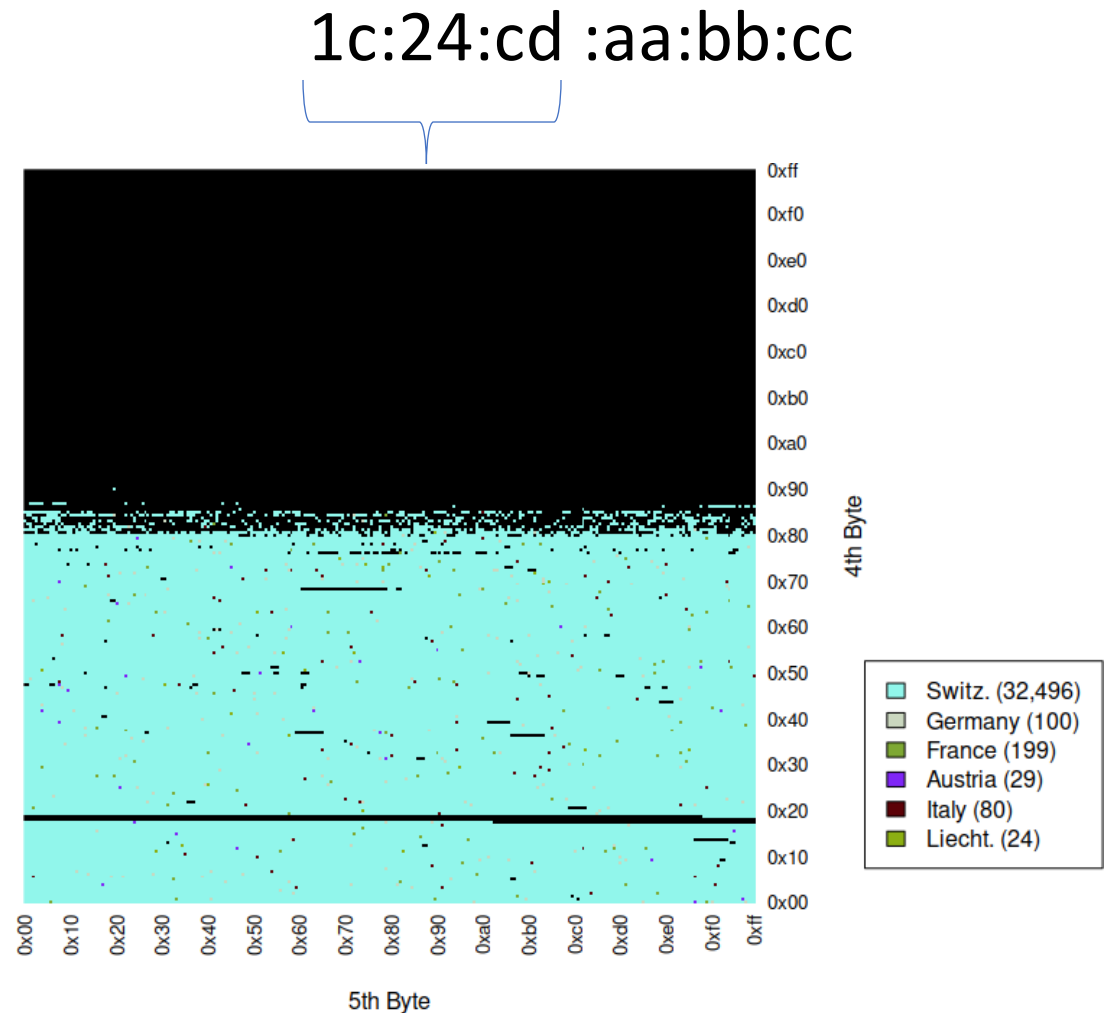


Volunteer's geolocated device
(substantial error introduced in figure)

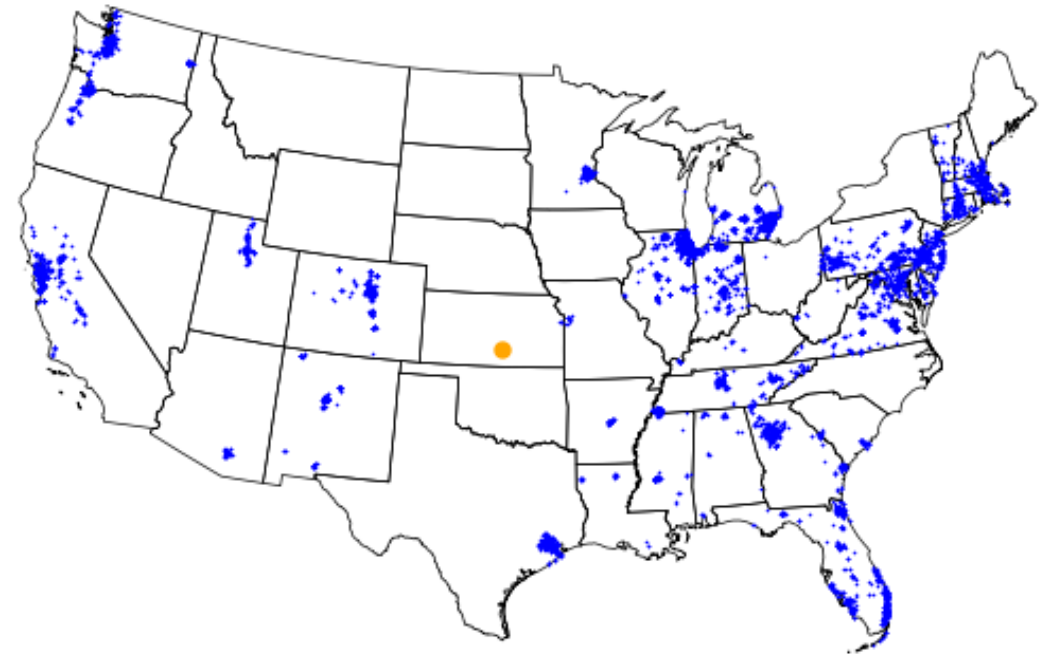
- Manufacturers frequently divide MAC address space by model*
- IPvSeeYou shows this results in geographic divisions, too
- MitraStar OUI shows clear bands of devices geolocated to Argentina and Peru



- Other OUIs show consistent country geolocations
 - Minor regional variations oftentimes exist
- Askey Corp OUI shows vast majority of geolocations in Switzerland
- Swisscom, a major Swiss ISP, provides Askey routers as its standard home WLAN device

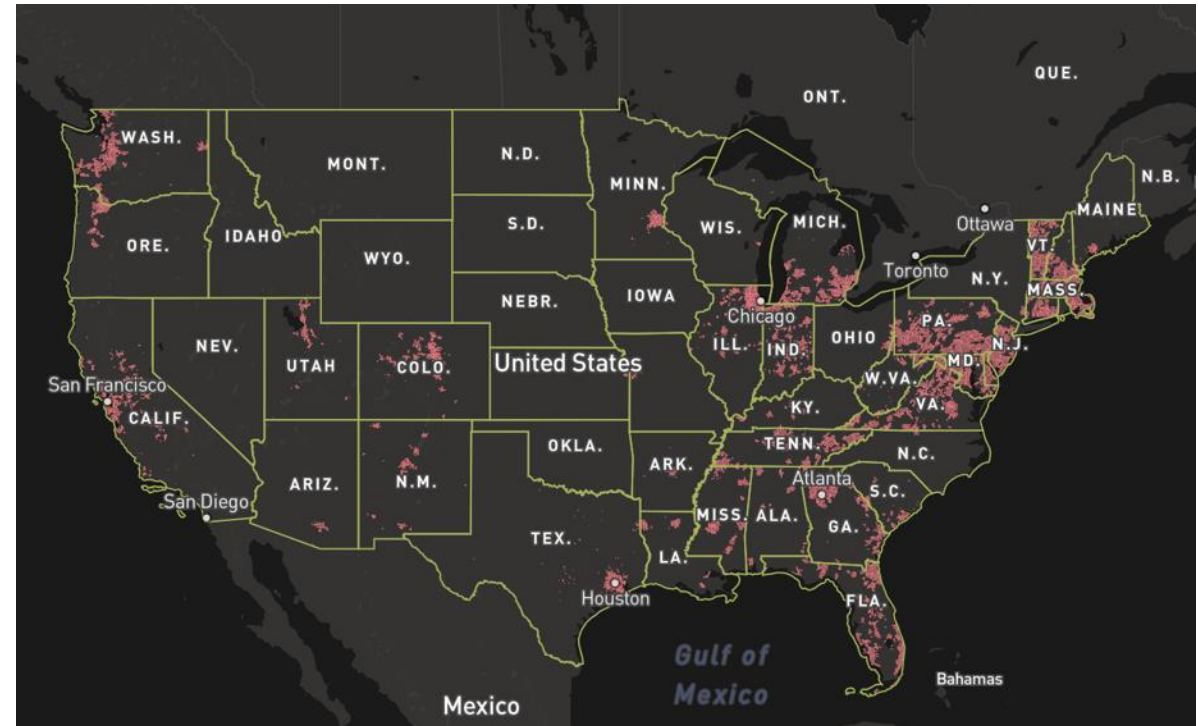


- Can infer an ISP's coverage area
- Blue
 - >1M geolocated Xfinity routers
- Orange
 - Maxmind's GeoLite database geolocation for **all** 1M IP addresses
- Far surpasses IP geolocation database performance
- IPvSeeYou geolocation matches FCC coverage map, validating methodology



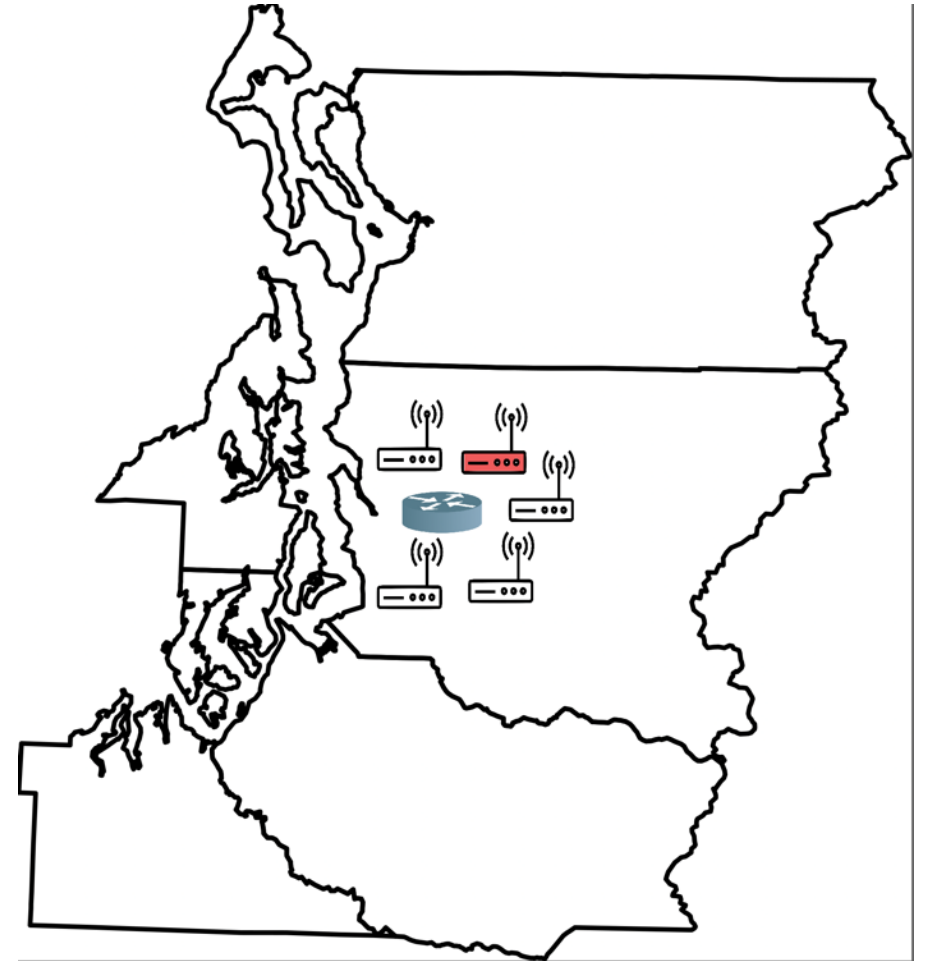
Inferred Comcast Xfinity service map in contiguous US

- Can infer an ISP's coverage area
- Blue
 - >1M geolocated Xfinity routers
- Orange
 - Maxmind's GeoLite database geolocation for **all** 1M IP addresses
- Far surpasses IP geolocation database performance
- IPvSeeYou geolocation matches FCC coverage map, validating methodology



FCC 2020 Comcast Coverage Map
<https://broadbandmap.fcc.gov/#/provider-detail>

- Assume IPv6 periphery (link from provider to customer router) has physical distance constraint
- If we can geolocate EUI-64 CPE attached to provider router
 - We can geolocate that provider router
 - We can geolocate *non-EUI-64* CPE attached to that same router!

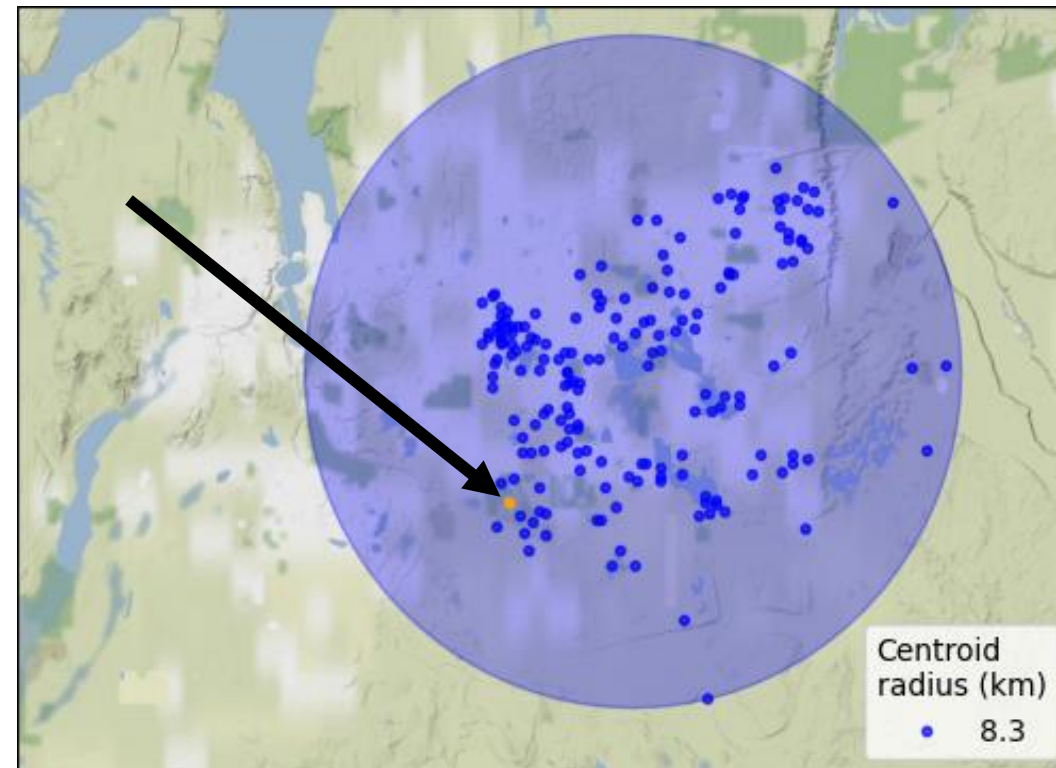


- Recall, using yarrp high-speed IPv6 traceroute
- Penultimate hop is the provider's infrastructure, e.g., cable head-end
- Group geolocated EUI-64 IPv6 addresses by penultimate hop

```
...  
18 2001:558:3:25c::2 74.284 ms  
19 2001:558:80:1b1::2 71.886 ms  
20 2001:558:82:380d::2 72.287 ms  
21 2001:558:6045:6:98cf:88bc:79ca:c366 90.986  
22 2601:642:c300:963:0211:22ff:fe33:4455 82.029
```

Intuition: last-mile connection between provider and customer (e.g., cable head-end) is relatively short. Geolocation of CPE thus can reveal geolocation of provider infrastructure and non-EUI-64 CPE!

- First, geolocate all EUI-64 CPE (blue dots) connected to same last hop as a target *non-EUI-64 CPE* (unknown location)
- Next, find centroid & EUI-64-encompassing centroid radius (large blue circle)
- Non-EUI-64 CPE inferred to within encompassing circle (orange dot known ground truth)
- Simply living near EUI-64 CPE routers is a location privacy threat



- Overview
- Background
- IPvSeeYou
- **Tool and Demo**
- Conclusions
- Questions

1. Input WAN MAC or EUI-64 IPv6 address
2. Calculates predicted BSSID value using our inferred WAN MAC – BSSID offsets
3. Queries Apple, wigle.net, or mylnikov.net for predicted BSSID value
4. Optionally outputs KML for geolocated BSSIDs

IPvSeeYou Demo

- Ideal remediation: stop using EUI-64 IPv6 addresses
- Disclosed vulnerability to multiple vendors
 - Devices account for millions of geolocated CPE
- Mixed results



- Overview
- Background
- IPvSeeYou
- Tool and Demo
- **Conclusions**
- Questions

- IPvSeeYou
 - Large scale data fusion attack
 - Combines:
 - EUI-64 IPv6 Addresses
 - Geolocated BSSIDs
 - To geolocate
 - Millions of CPE routers
 - Provider infrastructure
 - Non-EUI-64 CPE devices
- Easy to prevent (don't use EUI-64 IPv6 addresses), but:
 - Embedded / forgotten infrastructure that doesn't get updated
 - Often *can't* be updated
 - Even a single EUI-64 router can compromise privacy of non-EUI-64 devices

- Overview
- Background
- IPvSeeYou
- Tool and Demo
- Conclusions
- **Questions**

Thanks!

The logo for 6int, featuring the number '6' in black, followed by two colons in black, and the letters 'int' in blue. The logo is centered within a large, light blue circular graphic that has a textured, watercolor-like border.

- IPvSeeYou
 - Large scale data fusion attack
 - To geolocate millions of CPE routers
- Seeking volunteers to test / validate tool; contact us!
- info@sixint.io
- EUI-64 IPv6 Geolocation Tool
 - <https://github.com/6int/IPvSeeYou>

Questions?